Серия NXC

Контроллеры беспроводной локальной сети

Версия 4.10
Издание 1-е, 02/2014

Руководство пользователя

Параметры входа по умолчанию	
IP-адрес	https://192.168.1.1
Имя пользователя	admin
Пароль	1234

ВАЖНО!

ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ ПЕРЕД ИСПОЛЬЗОВАНИЕМ.

СОХРАНИТЕ ЭТО РУКОВОДСТВО ДЛЯ БУДУЩИХ СПРАВОК.

Снимки экрана и графические изображения в этом руководстве могут отличаться от реального вида продукта из-за различий во встроенном программном обеспечении или в операционной системе, установленной на компьютере пользователя. Нами сделано все возможное для того, чтобы информация, приведенная в настоящем руководстве, была точной.

Дополнительная документация

- Краткое руководство по началу работы

  Краткое руководство по началу работы рассказывает о том, как выполнить аппаратные подключения для устройства NXC и получить доступ к Web-конфигуратору.

- Справочное руководство по интерфейсу командной строки

  Справочное руководство по интерфейсу командной строки описывает интерфейс командной строки и рассказывает, как с помощью его команд выполнять настройку устройства NXC.

Примечание: Для настройки NXC предпочтительнее использовать Web-конфигуратор.

- Интерактивная справка Web-конфигуратора

  Чтобы получить информацию о настройках на каждом экране, а также дополнительную информацию по параметрам, нажмите на значок помощи на любом из экранов.

Обзорное оглавление

Оглавление

Часть I
Руководство пользователя

1

Введение

1.1 Обзор

В данном руководстве пользователя рассматриваются следующие модели: NXC2500 и NXC5500.

Таблица 1 Сравнительная таблица устройств серии NXC

ХАРАКТЕРИСТИКИ	NXC2500	NXC5500
Два порта USB	Да	Да
Консольный (последовательный) порт	Разъем DB-9	Разъем RJ-45

Устройство NXC представляет собой полнофункциональный контроллер беспроводной локальной сети. Гибкие возможности настройки помогают сетевым администраторам конфигурировать беспроводные локальные сети и эффективно применять в них политики безопасности. Кроме того, устройство NXC обладает высочайшей пропускной способностью, которая делает его идеальным решением для предоставления надежных, защищенных услуг.

К числу функций безопасности устройства NXC относятся межсетевой экран и сертификаты. Кроме того, данное устройство предлагает такие возможности, как настройка непокидаемого портала, трансляция сетевых адресов (NAT), перенаправление портов, маршрутизация на основе политик, сервер DHCP, расширенные функции управления беспроводными точками доступа и многие другие мощные функции. Гибкие возможности настройки помогают создать рабочую сеть и эффективно применять в ней политики безопасности.

Физические порты Gigabit Ethernet, расположенные на передней панели (обозначенные как **P1**, **P2**, **P3** и т.д.) ассоциированы с интерфейсами Gigabit Ethernet (ge). По умолчанию порт **P1** ассоциирован с интерфейсом **ge1**, порт **P2** – с интерфейсом **ge2** и т.д.

- По умолчанию IP-адрес устройства в локальной сети – 192.168.1.1.
- Имя и пароль администратора по умолчанию – «admin» и «1234» соответственно.

1.2 Зоны, интерфейсы и физические порты

Ниже приведены обзорные сведения о зонах, интерфейсах и физических портах устройства NXC.

Таблица 2 Зоны, интерфейсы и физические порты Ethernet

Зоны (локальная сеть)	Зона – это группа интерфейсов. Используйте зоны для применения настроек безопасности, таких, как межсетевые экраны.
Интерфейсы (Ethernet, виртуальные локальные сети)	Интерфейсы – это логические сущности, через которые проходят пакеты (третьего уровня). Используйте интерфейсы при настройке зон, маршрутов на основе политик, статических маршрутов и трансляции сетевых адресов. Физические порты объединяются в интерфейсы.
Физические порты Ethernet (P1, P2, P3 и т.д.)	Физический порт – это разъем, к которому подключается кабель.

1.2.1 Типы интерфейсов

На устройстве NXC существуют два типа интерфейсов. Помимо того, что интерфейсы используются различными функциями, они еще и описывают сеть, которая непосредственно к ним подключена.

- **Интерфейсы Ethernet** служат основой для определения других интерфейсов и сетевых политик.
- **Интерфейсы VLAN** распознают кадры с тегами. Устройство NXC автоматически добавляет или удаляет теги по мере необходимости. Каждая сеть VLAN может быть ассоциирована только с одним интерфейсом Ethernet.

Примечание: По умолчанию все интерфейсы Ethernet принадлежат сети vlan0, благодаря чему устройство NXC может выступать в качестве моста.

1.2.2 Настройка интерфейсов и зон

В этом разделе описывается процесс настройки физических интерфейсов, входящих в зону по умолчанию устройства NXC, и значения параметров этих интерфейсов по умолчанию. Для примера в этом разделе приведены чертежи NXC500.

Рисунок 1 Сетевая топология по умолчанию

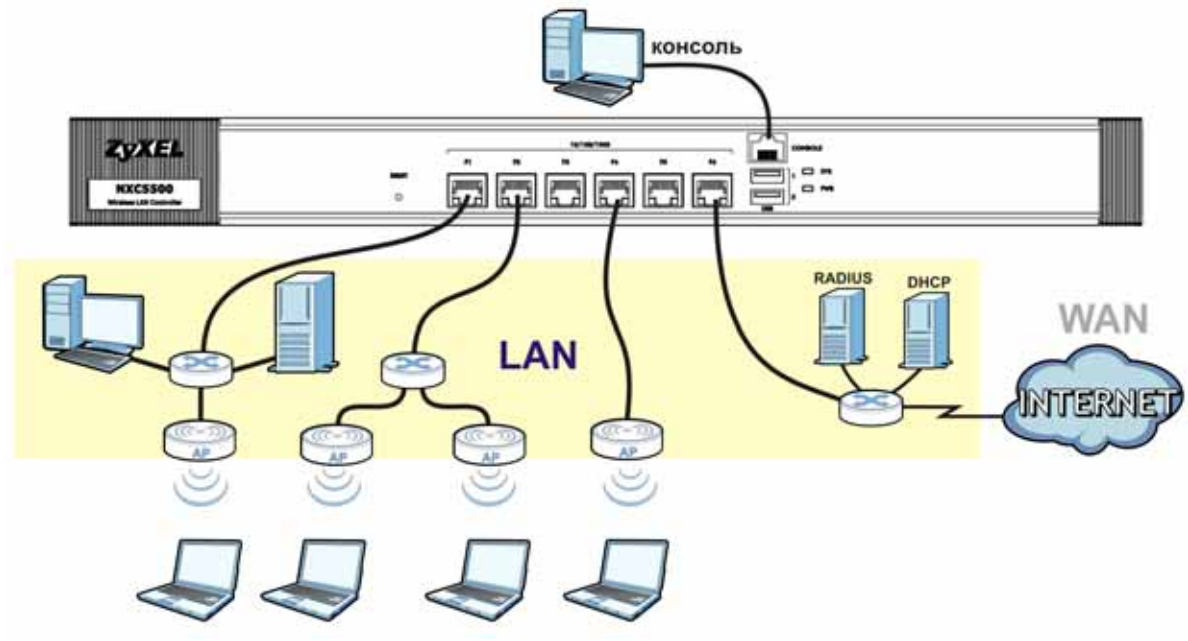


Таблица 3 Настройки интерфейсов по умолчанию

ПОРТ	ИНТЕРФЕЙС	ЗОНА	IP-АДРЕС И ПАРАМЕТРЫ DHCP	РЕКОМЕНДУЕМЫЙ ВАРИАНТ ИСПОЛЬЗОВАНИЯ С ПАРАМЕТРАМИ ПО УМОЛЧАНИЮ
P1~P6	ge1~ge6	LAN (vlan0)	192.168.1.1, сервер DHCP отключен	Выделенное подключение к локальной сети
CONSOLE	н/п	Нет	Нет	Локальное управление

- В зону **LAN** входят интерфейсы **ge1~ ge6** (физические порты P1~P6). По умолчанию все интерфейсы LAN принадлежат сети vlan0.
- Консольный порт (**console**) не входит ни в какие зоны – доступ к нему может осуществляться напрямую с компьютера, подключенного с помощью специального переходника «консоль-Ethernet».

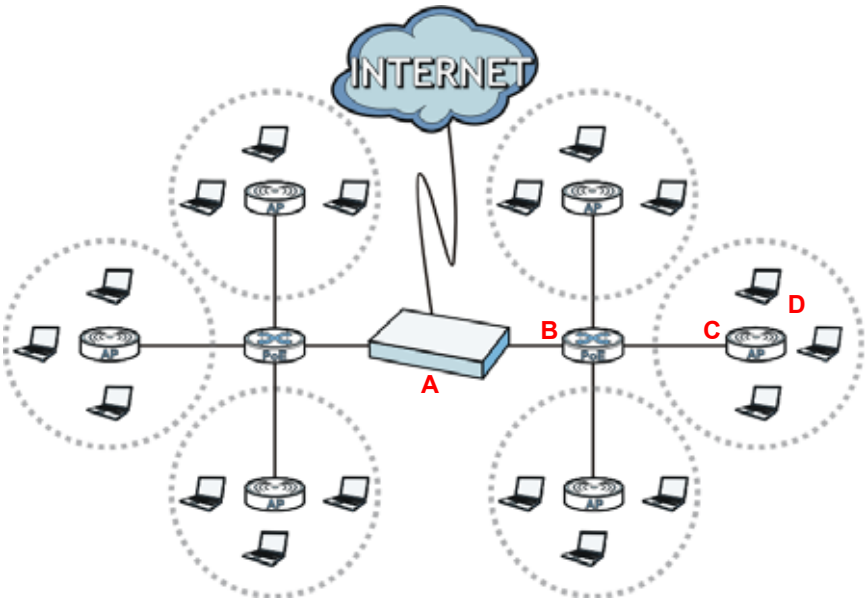
1.3 Варианты применения

Существует несколько вариантов использования устройства NXC.

1.3.1 Управление точками доступа

Управление несколькими точками доступа из одного места. Настройки точек доступа позволяют отслеживать появление мошеннических точек доступа.

Рисунок 2 Пример управления точками доступа



В данном случае устройство NXC (**A**) подключается к нескольким устройствам, поддерживающим питание устройств по витой паре (**PoE**) (**B**). Они подключаются к управляемым точкам доступа (**C**), таким, как NWA5123-NI, которые в свою очередь обеспечивают доступ к сети беспроводным клиентам (**D**) в пределах радиуса действия.

1.3.2 Обеспечение безопасности беспроводных каналов

Обеспечение безопасности соединений между беспроводными клиентами и точками доступа с помощью мощных инструментов защиты, предлагаемых устройством NXC. В настройках точек доступа можно потребовать обязательного шифрования WEP и WPA для всех беспроводных клиентов, пытающихся подключиться к данной точке доступа. Кроме того, можно обеспечить дополнительную защиту сети путем отслеживания мошеннических точек доступа. Мошенническими называют точки доступа, которые действуют в зоне покрытия сети и при этом не контролируются администраторами сети. Потенциально они представляют собой бреши в политике безопасности сети.

1.3.3 Непокидаемый портал

На устройстве NXC может быть включена функция непокидаемого портала, который перехватывает весь сетевой трафик, независимо от адреса или порта, до тех пор, пока пользователь, пытающийся установить соединение, не пройдет аутентификацию на специальной веб-странице для ввода имени и пароля.

Рисунок 3 Варианты применения: непокидаемый портал

Страница непокидаемого портала появляется только один раз во время сессии аутентификации. Обычно пользователь больше не видит этого окна в пределах одной сессии, за исключением случаев, когда сессия разрывается по тайм-ауту или пользователь закрывает соединение.

1.3.4 Балансировка нагрузки

Благодаря функции балансировки нагрузки можно легко организовать распределение беспроводного трафика между разными точками доступа, чтобы облегчить нагрузку на сеть. При перегрузке станция может автоматически отложить установку соединения, пока клиент не «уйдет» в другую сеть, или отключить клиентов, находящихся в неактивном состоянии, или клиентов с нестабильным подключением.

1.3.5 Динамический выбор каналов

Устройство NXC может автоматически выбирать радиоканал, по которому его точки доступа будут вести передачу. Для этого устройство сканирует зоны вокруг точек доступа и определяет, какие каналы используют в настоящее время другие устройства, не подключенные к сети.

1.3.6 Контроль доступа на уровне пользователей

Установка политик доступа, ограничивающих доступ к важной информации и общим ресурсам в зависимости от того, какой пользователь пытается к ним обратиться.

1.4 Обзор способов управления

Существуют следующие способы управления устройством NXC.

Web-конфигуратор

Web-конфигуратор представляет собой удобный интерфейс настройки и администрирования устройства NXC с помощью браузера. Описание Web-конфигуратора приводится в настоящем руководстве пользователя.

Интерфейс командной строки (CLI)

Интерфейс командной строки позволяет использовать для настройки устройства NXC текстовые команды. Получить доступ к интерфейсу командной строки можно с помощью средств удаленного доступа (например, по протоколам SSH или Telnet), через физический порт или консольный порт Web-конфигуратора. Подробное описание интерфейса командной строки можно найти в Справочном руководстве по интерфейсу командной строки. По умолчанию консольный порт имеет следующие параметры:

Таблица 4 Параметры консольного порта по умолчанию

ПАРАМЕТР	ЗНАЧЕНИЕ
Скорость	115200 бод
Битов данных	8
Четность	Нет
Стоп-бит	1
Управление потоком	Нет

1.5 Конфигурирование с использованием объектов

Устройство NXC хранит информацию или настройки в виде объектов. Эти объекты можно использовать для настройки множества функций и параметров устройства NXC. После настройки объект можно повторно использовать для конфигурирования других функций.

При изменении параметров объекта устройство NXC автоматически обновляет все параметры и правила, которые используют данный объект.

Объекты адресов можно создавать на основе IP-адреса подсети или шлюза интерфейса. Устройство NXC автоматически обновляет любое правило или параметр, которые используют эти объекты, при каждом изменении параметров IP-адреса данного интерфейса. Например, если изменить IP-адрес интерфейса Ethernet, устройство NXC автоматически поменяет правила или настройки, которые используют объект адреса подсети LAN на основе интерфейса.

Для создания объектов перед тем, как настроить использующие их функции, можно воспользоваться экранами **Configuration > Object**. При нахождении на экране, который использует объекты, для настройки параметров нового объекта можно также выбрать в меню пункт **Create new Object**.

Чтобы посмотреть, параметры каких объектов уже заданы, и какие настройки конфигурации ссылаются на определенные объекты, можно воспользоваться экраном **Object Reference**.

1.6 Запуск и остановка устройства NXC

Существует несколько способов запуска и остановки устройства NXC.

> Перед тем, как выключить устройство **NXC** или отключить его от источника питания, необходимо обязательно выбрать в меню пункт **Maintenance > Shutdown** или воспользоваться командой **`shutdown`**. **Невыполнение этого требования может привести к повреждению встроенного программного обеспечения.**

Таблица 5 Запуск и остановка устройства NXC

МЕТОД	ОПИСАНИЕ
Отключение питания	При включении питания устройства NXC происходит холодный запуск. Устройство NXC включается, выполняет проверку аппаратного обеспечения и запускает системные процессы.
Перезагрузка устройства NXC	Горячий запуск (без отключения и последующего включения питания) происходит в том случае, если нажать кнопку **Reboot** на экране **Reboot** или воспользоваться командой `reboot`. Устройство NXC записывает все кэшируемые данные в локальное хранилище, останавливает системные процессы, а затем выполняет горячий запуск.
Использование кнопки RESET	При нажатии кнопки **RESET** устройство NXC сбрасывает параметры до значений по умолчанию, а затем выполняет перезагрузку.
Выбор пункта меню **Maintenance > Shutdown > Shutdown** или использование команды `shutdown`	Если выбрать в меню пункт **Maintenance > Shutdown > Shutdown** или воспользоваться командой `shutdown`, то устройство запишет все кэшируемые данные в локальное хранилище и остановит системные процессы. Дождитесь завершения работы устройства, а затем вручную выключите его или отключите от источника питания. Завершение работы устройства не приводит к его выключению.
Отключение от источника питания	Отключение питания происходит в том случае, если выключить питание устройства NXC. Устройство NXC просто выключается. Оно не останавливает системные процессы и не записывает кэшируемые данные в локальное хранилище.

При применении файлов конфигурации и при запуске сценариев командной строки устройство NXC не останавливает и не запускает системные процессы, хотя некоторое время сетевые ресурсы могут быть недоступны.

2

Установка и подключение аппаратного обеспечения

2.1 Установка в стойке

Примечание: ZyXEL предлагает специальные выдвижные направляющие для устройства. Для получения дополнительной информации свяжитесь с местным поставщиком.

Устройство NXC может быть установлено в стандартную 19-дюймовую стойку или в шкаф вместе с другим оборудованием. Для установки устройства NXC в стандартную стойку с использованием комплекта для монтажа в стойку выполните следующие действия. Удостоверьтесь, что стойка способна уверенно выдержать совокупный вес всего оборудования, которое должно быть в нее установлено, и что положение устройства NXC не приводит к неустойчивости стойки и перегруженности ее верхней части. Перед установкой примите все необходимые меры предосторожности для надежного закрепления стойки.

Примечание: Необходимо, чтобы по 10 см по бокам и 20 см позади устройства были свободны.

Для винтовых креплений потребуется крестовая отвертка #2.

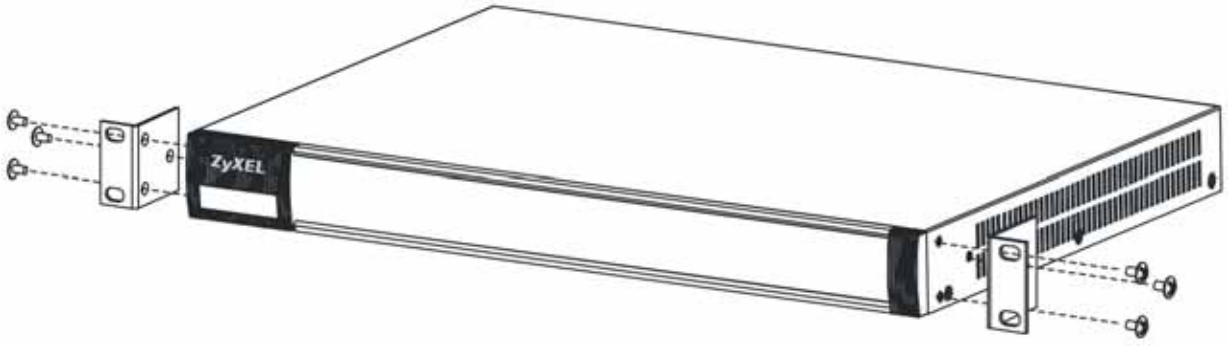
Примечание: Использование винтов неправильного типа может повредить устройство.

2.1.1 Процедура установки в стойку

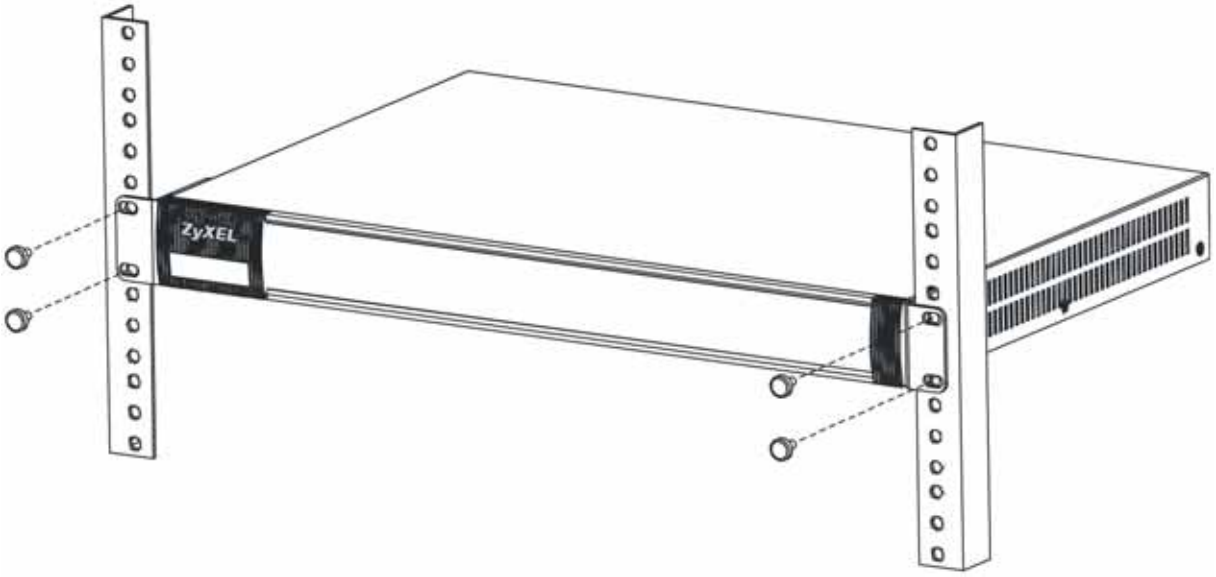
Для примера в этом разделе приведены чертежи NXC5500.

1 Совместите кронштейн с отверстиями на боковой панели устройства NXC и закрепите его винтами для кронштейна из комплекта поставки (они меньше по размеру, чем винты для крепления к стойке).

2 Аналогичным образом закрепите другой кронштейн.



3 После прикрепления обоих кронштейнов расположите устройство NXC в стойке таким образом, чтобы отверстия кронштейна совпали с крепежными позициями в стойке. Закрепите устройство NXC в стойке с использованием соответствующих винтов.



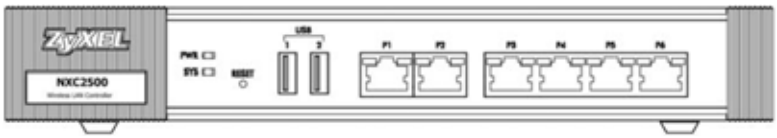
2.2 Передняя панель

В этом разделе приведено общее описание передней панели.

2.2.1 NXC2500

На передней панели устройства NXC2500 расположены индикаторы, одна кнопка сброса, два USB-порта и шесть портов Ethernet.

Рисунок 4 Передняя панель: NXC2500



2.2.2 NXC5500

На передней панели устройства NXC5500 расположены одна кнопка сброса, шесть портов Ethernet, один консольный порт, два USB-порта и индикаторы.

Рисунок 5 Передняя панель: NXC5500

Порты Ethernet

Порты Ethernet с автосогласованием и автоматическим определением типа кабеля поддерживают подключения Gigabit Ethernet 10/100/1000 Мбит/с, то есть они могут работать со скоростью 10, 100 или 1000 Мбит/с. Работа на скорости 10/100 Мбит/с возможна в полудуплексном или дуплексном режимах, а на скорости 1000 Мбит/с – только в дуплексном режиме. Порт с функцией автосогласования может определять и настраивать оптимальную скорость и режим дуплекса в канале Ethernet для подключенного устройства.

Порт с функцией автоматического определения типа кабеля (автоматического выбора режима MDI/MDI-X) позволяет использовать для подключения как стандартный (прямой), так и кроссоверный (перекрещенный) кабели Ethernet.

Настройки Ethernet по умолчанию

По умолчанию для портов Ethernet устройства NXC установлены следующие заводские настройки:

- Скорость: Автосогласование
- Режим дуплекса: Автосогласование
- Управление потоком: Включено (изменить настройки управления потоком нельзя, однако устройство NXC может согласовать с подключенным устройством и при необходимости отключить этот режим)

Консольный порт (только для NXC5500)

Соедините этот порт с компьютером (с помощью консольного кабеля с разъемами RJ-45 и DB-9), если необходимо настроить параметры устройства NXC с помощью интерфейса командной строки (CLI) через консольный порт.

Для локального управления можно использовать компьютер с установленной на нем программой-эмулятором терминала, настроенной со следующими параметрами:

- Эмуляция терминала VT100
- 115200 бод
- Четность – нет, 8 бит данных, 1 стоп-бит
- Управление потоком – нет

Подключите разъем RJ-45 консольного кабеля к консольному порту устройства NXC. Подключите другой конец консольного кабеля с разъемом типа «мама» к последовательному порту (COM1, COM2 или другому COM-порту) компьютера.

В таблице ниже описаны правила цветового кодирования проводов и назначение контактов консольного кабеля.

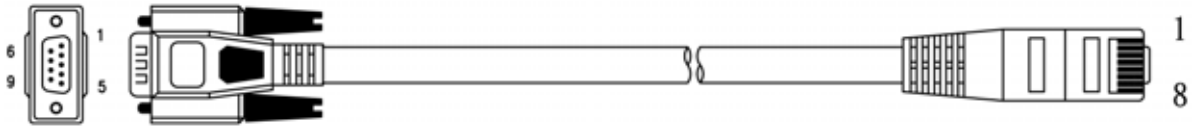


Таблица 6 Цветовые коды консольного кабеля с разъемами RJ-45 и DB-9

СИГНАЛ DB-9	НОМЕР КОНТАКТА DB-9	ЦВЕТ ПРОВОДА	НОМЕР КОНТАКТА RJ45
CTS	8	Белый/Оранжевый	1
DSR/DCD	6+1	Оранжевый	2
RD	2	Белый/Зеленый	3
GND	5	Синий	4
GND	5	Белый/Синий	5
TD	3	Зеленый	6
DTR	4	Белый/Коричневый	7
RTS	7	Коричневый	8

Порты USB 2.0

Подключите USB-накопитель к USB-порту устройства NXC для архивации системных журналов, хранящихся на устройстве NXC, или сохранения дампов ядра операционной системы устройства NXC.

2.2.3 Индикаторы на передней панели

В этом разделе приведено описание индикаторов, располагающихся на передней панели.

2.2.3.1 NXC2500

Описание индикаторов приводится в следующей таблице.

Таблица 7 Индикаторы передней панели: NXC2500

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PWR		Нет	Устройство NXC выключено.
	Зеленый	Горит	Устройство NXC включено.
	Красный	Горит	Обнаружен сбой оборудования. Оставите работу устройства, подождите несколько минут и вновь запустите (см. разд. 1.6 на стр. 22). Если индикатор по-прежнему светится красным, свяжитесь с торгующей организацией.

Таблица 7 Индикаторы передней панели: NXC2500 (продолжение)

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
SYS	Зеленый	Нет	Устройство NXC не готово или обнаружен отказ.
		Горит	Устройство NXC готово к работе и работает.
		Мигает	Выполняется загрузка устройства NXC.
	Красный	Горит	На устройстве NXC обнаружена ошибка или отказ.
P1~P6	Зеленый	Горит	Через данный порт успешно установлено соединение с сетью Ethernet на скорости 10/100 Мбит/с
		Мигает	Устройство NXC отправляет или принимает пакеты из сети Ethernet через этот порт на скорости 10/100 Мбит/с
	Оранжевый	Горит	Через данный порт успешно установлено соединение с сетью Ethernet на скорости 1000 Мбит/с.
		Мигает	Устройство NXC отправляет или принимает пакеты из сети Ethernet через этот порт на скорости 1000 Мбит/с
		Нет	Подключение к данному порту отсутствует.

2.2.3.2 NXC5500

Описание индикаторов приводится в следующей таблице.

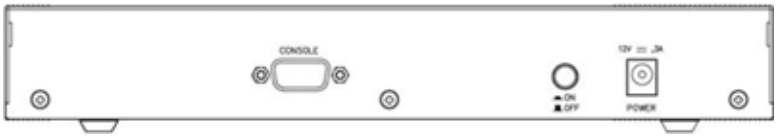
Таблица 8 Индикаторы передней панели: NXC5500

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PWR	Зеленый	Нет	Устройство NXC выключено.
		Горит	Устройство NXC включено.
SYS	Зеленый	Нет	Устройство NXC не готово или обнаружен отказ.
		Горит	Устройство NXC готово к работе и работает.
		Мигает	Выполняется загрузка устройства NXC.
P1~P6 Соединение (Слева)	Зеленый	Горит	Через данный порт успешно установлено соединение с сетью Ethernet
		Мигает	Устройство NXC отправляет или принимает пакеты в/из сети Ethernet через данный порт
		Нет	Подключение к данному порту отсутствует.
P1~P6 Скорость (Справа)	Зеленый	Горит	Скорость соединения Ethernet на данном порту составляет 100 Мбит/с.
	Оранжевый	Горит	Скорость соединения Ethernet на данном порту составляет 1000 Мбит/с.
		Нет	Скорость соединения Ethernet на данном порту составляет 10 Мбит/с.

2.3 Задняя панель

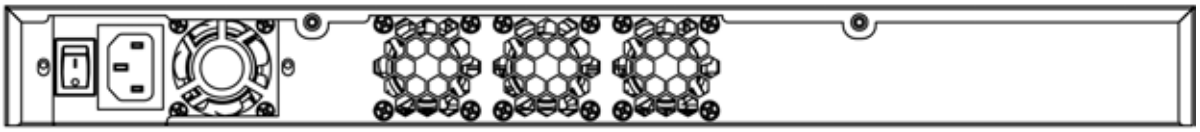
На задней панели устройства NXC2500 располагаются консольный порт, выключатель питания и разъем для шнура питания.

Рисунок 6 Задняя панель: NXC2500



На задней панели устройства NXC5500 располагаются консольный порт, выключатель питания, разъем для шнура питания и вентиляторный модуль.

Рисунок 7 Задняя панель: NXC5500



Консольный порт (только для модели NXC2500)

Подключите к этому порту компьютер (с помощью кабеля RS-232), если необходимо настроить параметры устройства NXC с помощью интерфейса командной строки (CLI) через консольный порт.

Для локального управления можно использовать компьютер с установленной на нем программой-эмулятором терминала, настроенной со следующими параметрами:

- Эмуляция терминала VT100
- 115200 бод
- Четность – нет, 8 бит данных, 1 стоп-бит
- Управление потоком – нет

Подключите 9-пиновый разъем типа «папа» консольного кабеля RS-232 к консольному порту устройства NXC. Подключите другой конец кабеля с разъемом типа «мама» к последовательному порту (COM1, COM2 или другому COM-порту) компьютера.

3

Web-конфигуратор

3.1 Обзор

Web-конфигуратор устройства NXC представляет собой удобный интерфейс для администрирования устройства с помощью браузера.

Для использования Web-конфигуратора потребуется:

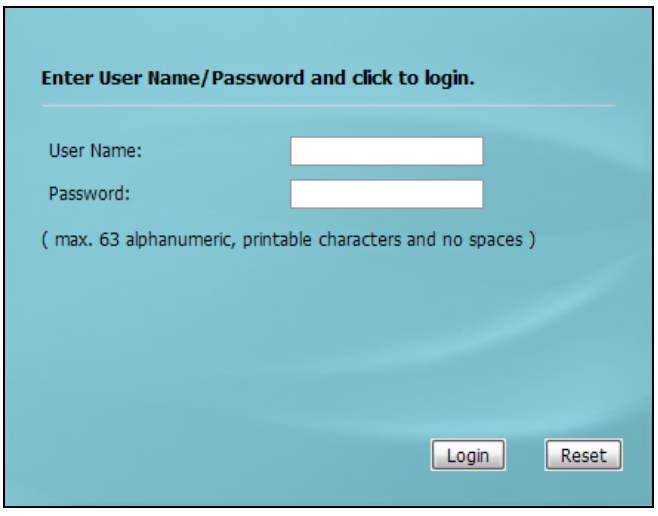
- Используйте следующие браузеры: Internet Explorer версии 7.0 или более поздней, Mozilla Firefox версии 9.0 или более поздней, Safari версии 4.0 или более поздней или Google Chrome версии 10.0 или более поздней.
- Разрешите всплывающие окна
- Разрешите использование JavaScript (по умолчанию разрешено)
- Разрешите использование Java (по умолчанию разрешено)
- Включите cookies

Рекомендуемое разрешение экрана: 1024 x 768 пикселей и выше.

3.2 Получение доступа

1 Убедитесь, что устройство NXC надлежащим образом подключено. См. Краткое руководство по началу работы.

2 Наберите в браузере адрес http://192.168.1.1 и перейдите по нему. Появится экран ввода имени пользователя и пароля (**Login**).



3 Введите имя пользователя (по умолчанию «admin») и пароль (по умолчанию «1234»).

4 Нажмите **Login**. Если вход в систему выполнен с использованием имени и пароля по умолчанию, в окне браузера откроется экран **Update Admin Info**. В противном случае откроется панель мониторинга устройства.

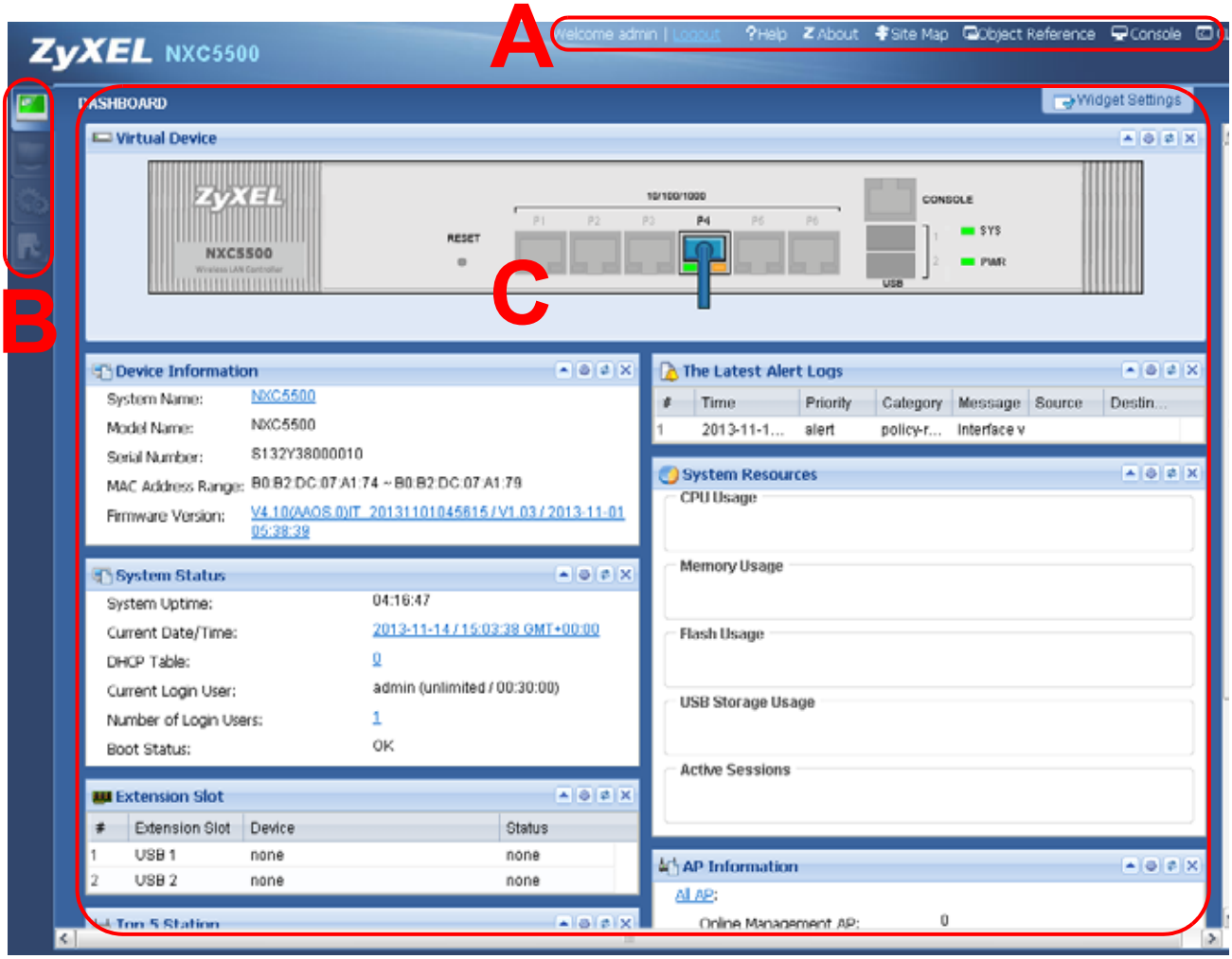
Этот экран открывается при каждом входе в систему с использованием имени пользователя и пароля по умолчанию. Если изменить пароль для пользователя по умолчанию, этот экран больше открываться не будет.

3.3 Основной экран

В этом руководстве для примера использованы экраны NXC5500. Для других моделей экраны могут иметь немного другой вид.

Основной экран Web-конфигуратора разделен на следующие части:

Рисунок 8 Основной экран Web-конфигуратора



- **A** – Строка заголовка
- **B** – Панель навигации
- **C** – Основное окно

3.3.1 Верхняя панель

Строка заголовка содержит некоторые полезные ссылки, которые всегда присутствуют на экранах, приведенных ниже, независимо от текущего уровня меню Web-конфигуратора.

Рисунок 9 Верхняя панель

Значки в верхней панели обеспечивают доступ к следующим функциям.

Таблица 9 Верхняя панель: значки Web-конфигуратора

ПОЛЕ	ОПИСАНИЕ
Logout	Нажатие на данную ссылку вызывает выход из Web-конфигуратора.
Help	Нажатие на данную ссылку открывает страницу справки по текущему экрану.

Таблица 9 Верхняя панель: значки Web-конфигуратора (продолжение)

ПОЛЕ	ОПИСАНИЕ
About	Нажатие на данную ссылку позволяет отобразить основную информацию об устройстве NXC.
Site Map	Нажатие на данную ссылку позволяет открыть обзорную страницу с ссылками на все экраны Web-конфигуратора.
Object Reference	Нажатие на эту ссылку позволяет перейти к экрану, на котором можно увидеть, какие элементы конфигурации ссылаются на данный объект.
Console	Нажатие на эту ссылку открывает консоль, в окне которой можно будет воспользоваться интерфейсом командной строки (CLI). Более подробную информацию можно найти в Справочном руководстве по интерфейсу командной строки устройства NXC.
CLI	Нажатие на эту ссылку открывает всплывающее окно, в котором отображаются команды интерфейса командной строки, направляемые Web-конфигуратором на устройство.

Окно About

Нажатие на **About** позволяет отобразить основную информацию об устройстве NXC.

Рисунок 10 Окно About

В приведенной ниже таблице описаны все поля, которые могут появиться на этом экране.

Таблица 10 Окно About

ПОЛЕ	ОПИСАНИЕ
Boot Module	В этом поле отображается номер версии программного обеспечения, управляющего процессом загрузки устройства NXC.
Current Version	В этом поле отображается версия встроенного программного обеспечения устройства NXC.
Released Date	В этом поле отображается дата (гггг-мм-дд) и время (чч:мм:сс) выпуска встроенного программного обеспечения.
OK	Нажатие позволяет закрыть окно.

Окно Site Map

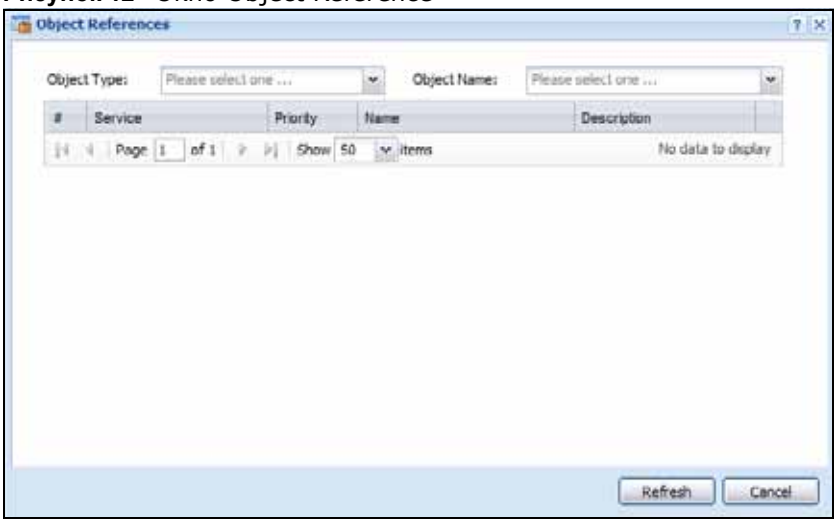
Нажмите на **Site MAP**, чтобы открыть обзорную страницу с ссылками на экраны Web-конфигуратора. Нажимая на ссылки в этом окне, можно перейти к соответствующему экрану.

Рисунок 11 Окно Site Map

Окно Object Reference

Нажмите на **Object Reference**, чтобы открыть экран **Object Reference**. Выбрав тип объекта и конкретный объект, по нажатию на **Refresh** можно отобразить настройки конфигурации, которые ссылаются на данный объект.

Рисунок 12 Окно Object Reference



Отображаемые поля зависят от типа объекта. В приведенной ниже таблице описаны все поля, которые могут появиться на этом экране.

Таблица 11 Окно Object Reference

ПОЛЕ	ОПИСАНИЕ
Object Name	В этом поле приводится идентификатор объекта, который задействован в отображаемых настройках конфигурации. Нажатие на имя объекта позволяет отобразить экран настройки объекта в основном окне.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.

Таблица 11 Окно Object Reference (продолжение)

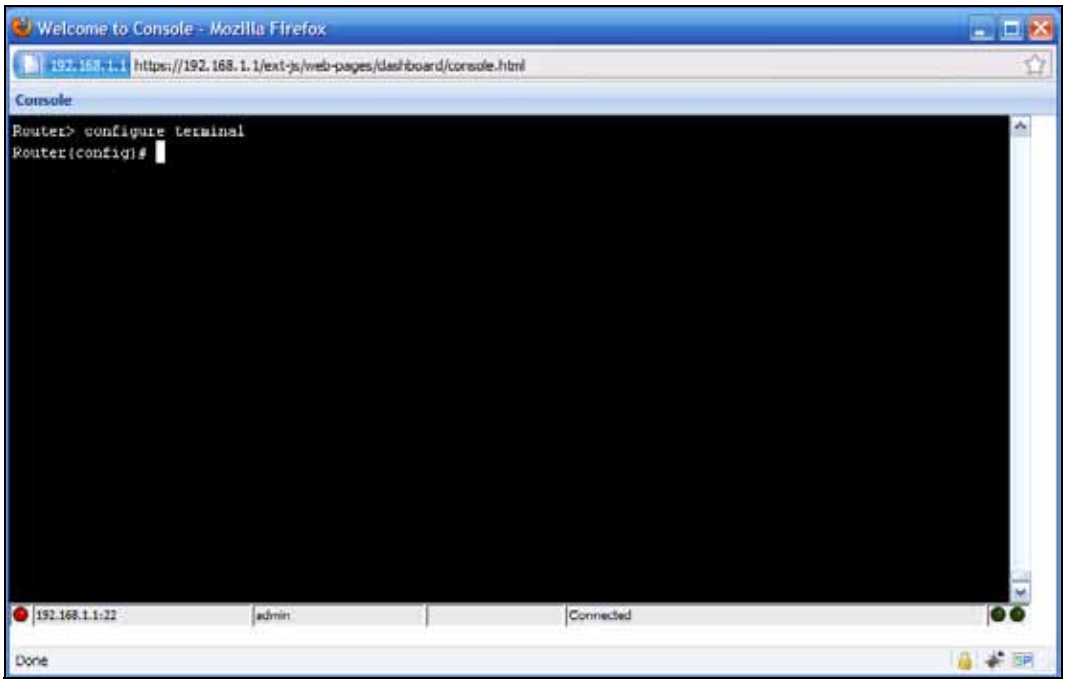
ПОЛЕ	ОПИСАНИЕ
Service	Обозначает тип настройки, которая ссылается на выбранный объект. Нажатие на имени службы позволяет отобразить экран настройки службы в основном окне.
Priority	В данном поле отображается, если это применимо, позиция в списке элемента конфигурации, ссылающегося на объект; в противном случае в этом поле отображается **N/A**.
Name	В данном поле отображается идентификатор элемента конфигурации, ссылающегося на объект.
Description	Если для ссылающегося на объект элемента конфигурации имеется описание, оно отображается в этом поле.
Refresh	Нажатие на эту ссылку позволяет обновить информацию на данном экране.
Cancel	Нажатие на **Cancel** позволяет закрыть окно.

Окно Console

Консоль позволяет использовать команды интерфейса командной строки непосредственно из Web-конфигуратора вместо отдельной терминальной программы. Помимо входа непосредственно на интерфейс командной строки устройства NXC, можно подключиться через эту консоль и к другим устройствам, находящимся в этой сети. Для установки соединения используется протокол SSH.

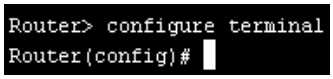
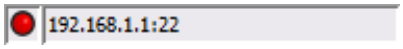
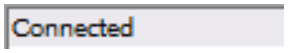
Примечание: Для просмотра функций в пользовательском интерфейсе Web-конфигуратора, которые соответствуют определенным командам интерфейса командной строки устройства NXC, используйте окно CLI Messages (см. «Окно CLI Messages» на стр. 37) в сочетании с этим окном.

Рисунок 13 Окно Console



Элементы экрана описаны в следующей таблице.

Таблица 12 Окно Console

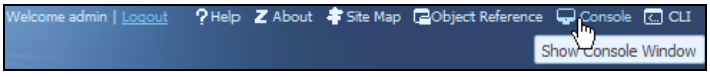
ПОЛЕ	ОПИСАНИЕ
Командная строка	 Введите команды для устройства, на которое выполнен вход. Если выполнен вход на устройство NXC, подробную информацию о возможностях настройки устройства с помощью командной строки можно найти в Справочном руководстве по интерфейсу командной строки,.
IP-адрес устройства	 Это IP-адрес устройства, на который выполнен вход.
Пользователь	 В этом поле отображается имя пользователя, который выполнил вход на устройство NXC через окно Console. Примечание: Имеется возможность выполнить вход в Web-конфигуратор от имени другого пользователя, чем тот, под именем которого был выполнен вход на устройство NXC через консоль.
Состояние соединения	 В этом поле отображается состояние соединения пользователя, который в данный момент выполнил вход на устройство. Если вход на устройство выполнен и имеется подключение, в этом поле отображается значение «Connected». Если соединение по каким-либо причинам разорвано или выполнен выход с устройства, в этом поле отображается значение «Not Connected».
Монитор активности по передаче/ приему	 В этом поле отображается текущая активность по выгрузке / загрузке данных. Чем быстрее и чаще мигает индикатор, тем выше скорость передачи данных.

Перед тем, как воспользоваться консолью, необходимо удостовериться в следующем:

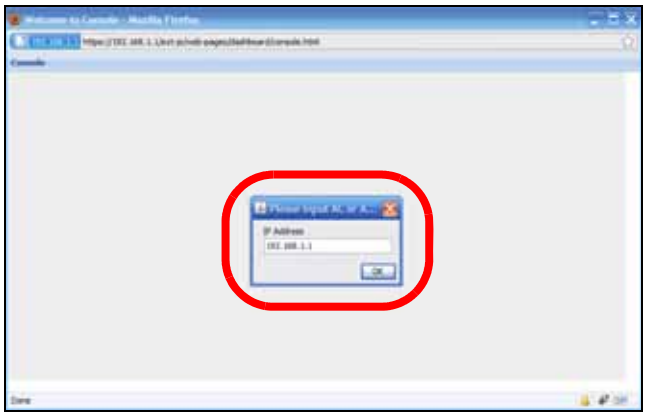
- Выбранный браузер поддерживает всплывающие окна при обращении к IP-адресу, назначенному устройству NXC.
- Веб-браузер разрешает использование Java-программ.
- Используется последняя версия Java (http://www.java.com).

Чтобы выполнить вход на устройство через консоль:

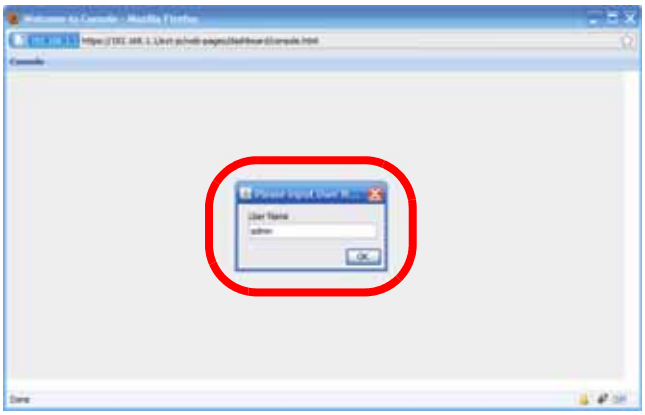
1 Нажмите кнопку **Console** в строке заголовка Web-конфигуратора.



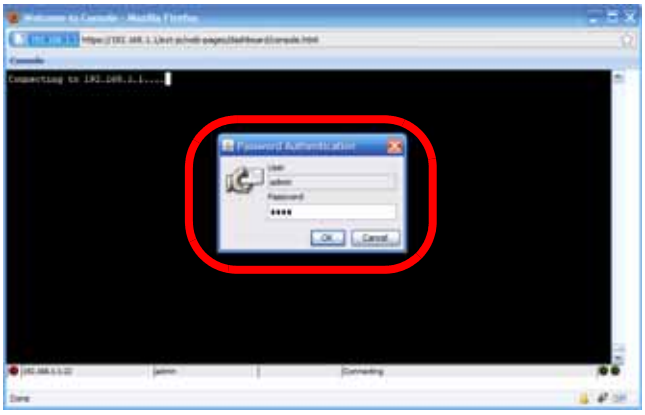
2 Введите IP-адрес устройства NXC и нажмите кнопку **OK**.



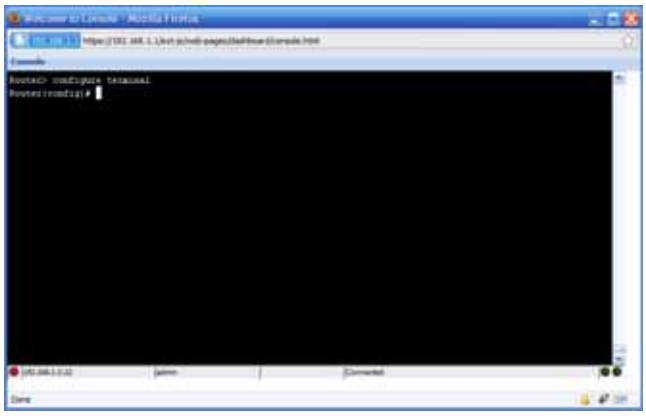
3 Затем введите имя пользователя, под которым необходимо выполнить вход на целевое устройство, и нажмите кнопку **OK**.



4 В зависимости от типа устройства, на которое выполняется вход, может быть предложено ввести пароль для данного пользователя. Введите пароль и нажмите кнопку **OK**.



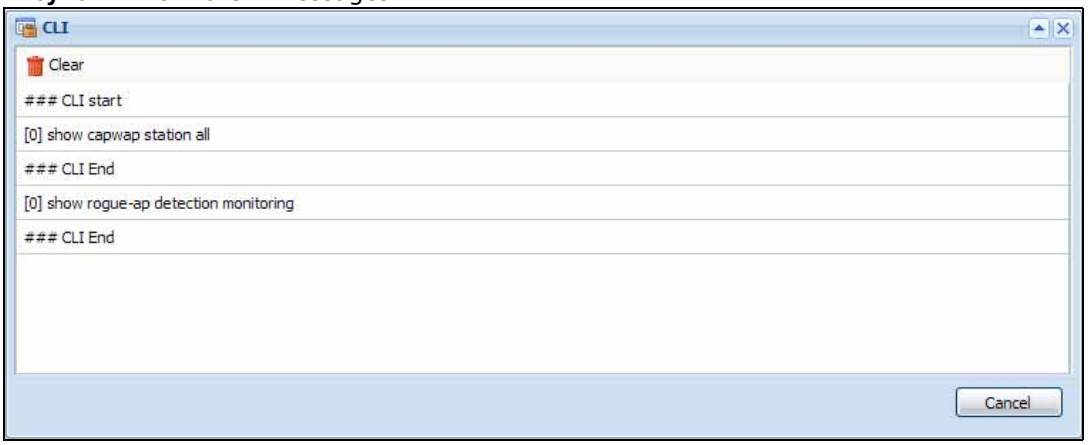
5 В случае успешного входа на устройство на экране появится командная строка, и в панели состояния в нижней части окна консоли изменится информация о состоянии подключения.



Окно CLI Messages

При нажатии на **CLI** открывается окно, в котором можно видеть команды интерфейса командной строки, направляемые Web-конфигуратором. Эти команды появляются во всплывающем окне, наподобие того, что изображено на рисунке ниже.

Рисунок 14 Окно CLI Messages



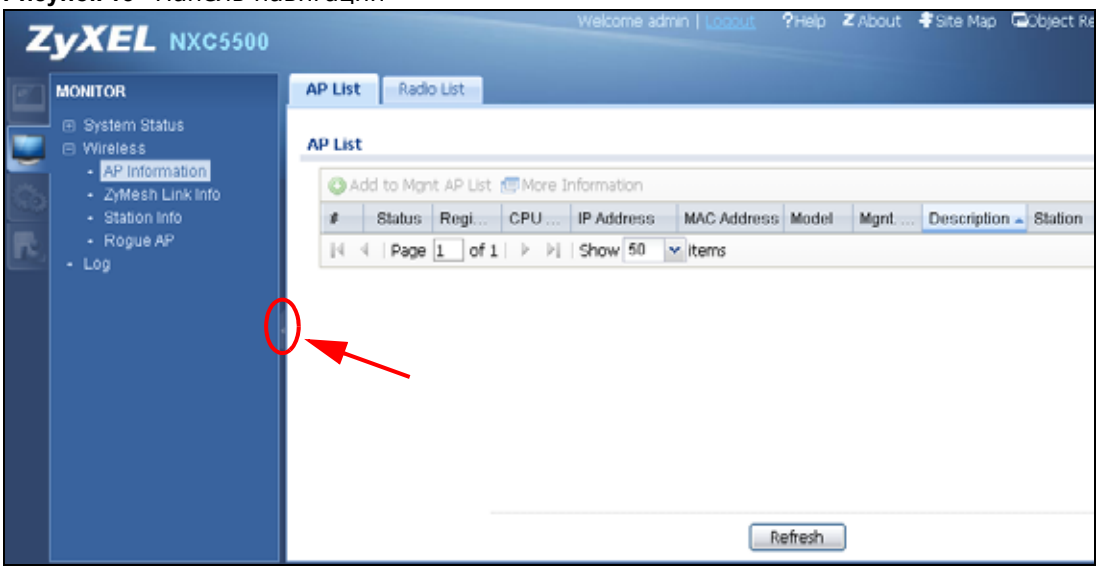
Нажмите кнопку **Clear**, чтобы стереть отображаемую в данный момент информацию.

Информацию о командах можно найти в Справочном руководстве по интерфейсу командной строки.

3.3.2 Панель навигации

Используйте пункты меню на навигационной панели, чтобы открыть экраны, позволяющие настраивать функции устройства NXC. Щелкните на стрелке в центре правого края навигационной панели, чтобы скрыть меню навигационной панели, или потяните мышью за край панели, чтобы изменить ее размер. Описание пунктов меню панели навигации и соответствующих экранов устройства NXC приводится в следующих разделах.

Рисунок 15 Панель навигации



3.3.2.1 Панель мониторинга (Dashboard)

На панели мониторинга в виде виджетов, которые можно упорядочить по собственному усмотрению, отображается общая информация об устройстве, о состоянии системы, о загрузке системных ресурсов, о состоянии лицензируемых служб, а также о состоянии интерфейсов.

Более подробную информацию о возможностях панели мониторинга можно найти в гл. 4 на стр. 48.

3.3.2.2 Меню мониторинга (Monitor)

С помощью меню мониторинга можно получить доступ к экранам, на которых отображается информация о состоянии и статистика.

Таблица 13 Краткое описание экранов меню Monitor

ПАПКА ИЛИ ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
System Status		
Port Statistics		Отображает статистику по пакетам для каждого физического порта.
Interface Status		Отображает общие сведение об интерфейсе и статистику по пакетам.
Traffic Statistics		Сбор и отображение статистики по трафику.
Session Monitor		Отображает состояние всех текущих сессий.

Таблица 13 Краткое описание экранов меню Monitor (продолжение)

ПАПКА ИЛИ ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
IP/MAC Binding		Выводит список устройств, которые получили IP-адреса от интерфейсов устройства NXC с использованием привязки IP/MAC-адресов.
Login Users		Выводит список пользователей, выполнивших вход на устройство NXC.
Dynamic Guest		Выводит список динамических гостевых имен пользователей в локальных базах данных устройства NXC.
USB Storage		Отображает информацию о USB-устройстве, подключенном к устройству NXC.
Wireless		
AP Information	AP List	Отображает информацию о подключенных точках доступа.
	Radio List	Отображает информацию о радиомодулях подключенных точек доступа.
All ZyMesh AP	ZyMesh Link Info	Отображает статистику о соединениях ZyMesh/WDS между управляемыми точками доступа.
Station Info	Station List	Отображает информацию о подключенных станциях.
Detected Device		Отображает информацию о подозрительных точках доступа, которые могут оказаться мошенническими.
Log	View Log	Выводит записи из журнала устройства NXC.
	View AP Log	Позволяет запросить сведения о подключенных точках доступа и вывести записи из журнала, относящиеся к ним.

3.3.2.3 Меню настройки (Configuration)

С помощью экранов меню настройки устройства NXC осуществляется конфигурирование его функционала.

Таблица 14 Краткое описание экранов меню Configuration

ПАПКА ИЛИ ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Licensing		
Registration	Registration	Регистрация устройства.
	Service	Просмотр состояния лицензируемых служб и обновление лицензируемых служб.
Wireless		
Controller	Configuration	Настройка правил поведения устройства NXC с только что подключенными к сети точками доступа.
AP Management	Mgnt. AP List	Изменение сведений о беспроводных точках доступа, удаление беспроводных точек доступа и их перезагрузка.
	AP Policy	Настройка IP-адреса контроллера точек доступа на управляемых точках доступа и выбор действий, которые должны предпринять управляемые точки доступа в случае сбоя текущего контроллера.
MON Mode	Rogue/Friendly AP List	Настройка правил мониторинга устройством NXC мошеннических точек доступа.
Load Balancing		Настройка балансировки нагрузки для трафика, поступающего от и идущего к беспроводным клиентам.
DCS		Настройка динамического выбора беспроводных каналов.

Таблица 14 Краткое описание экранов меню Configuration (продолжение)

ПАПКА ИЛИ ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
Auto Healing		Включать режим автоматического восстановления работоспособности (auto healing) для расширения зоны покрытия беспроводных услуг управляемых точек доступа в случае сбое одной точки доступа.
Network		
Interface	Ethernet	Управление интерфейсами Ethernet и виртуальными интерфейсами Ethernet.
	VLAN	Создание и управление интерфейсами VLAN и виртуальными интерфейсами VLAN.
Routing	Policy Route	Создание и управление политиками маршрутизации.
	Static Route	Создание и управление параметрами статической IP-маршрутизации.
Zone		Настройка зон, используемых для определения различных политик.
NAT		Настройка и управление правилами перенаправления портов.
ALG		Настройка сквозного режима (pass-through) для FTP.
IP/MAC Binding	Summary	Настройка привязок IP- и MAC-адресов для устройств, подключенных к каждому из поддерживаемых интерфейсов.
	Exempt List	Настройка диапазонов IP-адресов, для которых устройством NXC не применяются привязки IP- и MAC-адресов.
Captive Portal	Captive Portal	Назначение Web-страницы непокидаемого портала различным сетевым службам.
	Login Page	Назначение и адаптация страницы входа в систему для пользователей (то есть содержимого, которое они видят при попадании на непокидаемый портал).
RTLS	Real Time Location System	Использование управляемых точек доступа как элемента системы Ekahau RTLS, обнаруживающей местонахождение меток Wi-Fi Ekahau.
Firewall	Firewall	Включение и отключение межсетевого экрана и асимметричных маршрутов, настройка правил межсетевого экрана.
	Session Control	Ограничение количества одновременных сессий NAT/межсетевого экрана, которые может использовать клиент.
Object		
User/Group	User	Создание и управление пользователями.
	Group	Создание и управление группами пользователей.
	Setting	Управление настройками по умолчанию для всех пользователей, общими настройками для пользовательских сессий, а также правил принудительной аутентификации пользователей.
	MAC Address	Привязка MAC-адресов беспроводных клиентов к MAC-ролям (учетным записям MAC-адресов).
AP Profile	Radio	Создание и управление файлами настроек беспроводных радиомодулей, которые могут быть ассоциированы с разными точками доступа.
	SSID	Создание и управление идентификаторами беспроводных сетей, безопасность, фильтрация по MAC-адресам и файлы настроек изоляции второго уровня, которые могут быть ассоциированы с разными точками доступа.

Таблица 14 Краткое описание экранов меню Configuration (продолжение)

ПАПКА ИЛИ ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
MON Profile		Создание и управление файлами мониторинга мошеннических точек доступа, которые могут быть ассоциированы с различными точками доступа.
ZyMesh Profile	ZyMesh	Создание и управление файлами ZyMesh, которые могут быть ассоциированы с различными точками доступа.
Address	Address	Создание и управление хостами, диапазонами и адресами (под)сетей.
	Address Group	Создание и управление группами адресов.
Service	Service	Создание и управление службами TCP и UDP.
	Service Group	Создание и управление группами служб.
Schedule		Создание расписаний для однократных и периодических заданий.
AAA Server	Active Directory	Настройка параметров Active Directory по умолчанию.
	LDAP	Настройка параметров LDAP по умолчанию.
	RADIUS	Настройка параметров RADIUS по умолчанию.
Auth. Method		Создание и управление способами аутентификации пользователей.
Certificate	My Certificates	Создание и управление сертификатами устройства NXC.
	Trusted Certificates	Импорт и управление сертификатами от доверенных источников.
DHCPv6	Request	Настройка объектов с типом запроса DHCPv6.
System		
Host Name		Настройка имени системы и доменного имени для устройства NXC.
USB Storage	Settings	Настройка параметров подключенных устройств USB.
Date/Time		Настройка текущих даты, времени и часового пояса для устройства NXC.
Console Speed		Настройка скорости консольного порта.
DNS		Настройка сервера DNS и записей адресов для устройства NXC.
WWW		Настройка HTTP, HTTPS и общих параметров аутентификации.
SSH		Настройка сервера SSH и параметров службы SSH.
TELNET		Настройка параметров сервера telnet для устройства NXC.
FTP		Настройка параметров сервера FTP.
SNMP		Настройка сообществ и служб SNMP.
Auth. Server		Настройка устройства NXC для работы в качестве сервера RADIUS.
Language		Выбор языка для Web-конфигуратора.
IPv6		Включение или отключение поддержки IPv6 на устройстве NXC.
Log & Report		
Email Daily Report		Настройка адреса и порядка отправки ежедневных отчетов, а также выбор отправляемых отчетов.
Log Settings		Настройка системного журнала, журнала электронной почты и удаленных серверов syslog.

3.3.2.4 Меню обслуживания (Maintenance)

С помощью экранов меню обслуживания можно управлять файлами конфигурации и встроенного программного обеспечения, запускать диагностические процедуры, а также перезагружать и выключать устройство NXC.

Таблица 15 Краткое описание экранов меню Maintenance

ПАПКА ИЛИ ССЫЛКА	ВКЛАДКА	ФУНКЦИЯ
File Manager	Configuration File	Управление файлами конфигурации и передача файлов конфигурации на устройство NXC.
	Firmware Package	Просмотр текущей версии встроенного программного обеспечения и передача на устройство встроенного программного обеспечения.
	Shell Script	Управление и запуск файлов сценариев командной строки на устройстве NXC.
Diagnostics	Diagnostic	Сбор диагностической информации.
	Packet Capture	Запись пакетов для анализа.
	Core Dump	Сохранение ядра операционной системы устройства NXC на предварительно подключенное к устройству NXC USB-устройство.
	System Log	Архивирование системных журналов устройства NXC на предварительно подключенное к устройству NXC USB-устройство.
	Wireless Frame Capture	Захват беспроводных кадров с точек доступа с целью анализа.
Packet Flow Explore	Routing Status	Проверка порядка выбора маршрута для пакета устройством NXC.
	SNAT Status	Получение точной картины того, каким образом устройство NXC выполняет преобразование IP-адреса источника в пакетах и соответствующих настроек.
Reboot		Перезагрузка устройства NXC.
Shutdown		Выключение устройства NXC.

3.3.3 Предупредительные сообщения

Предупредительные сообщения, являющиеся, к примеру, следствием неверной настройки, отображаются во всплывающем окне.

Рисунок 16 Предупредительное сообщение

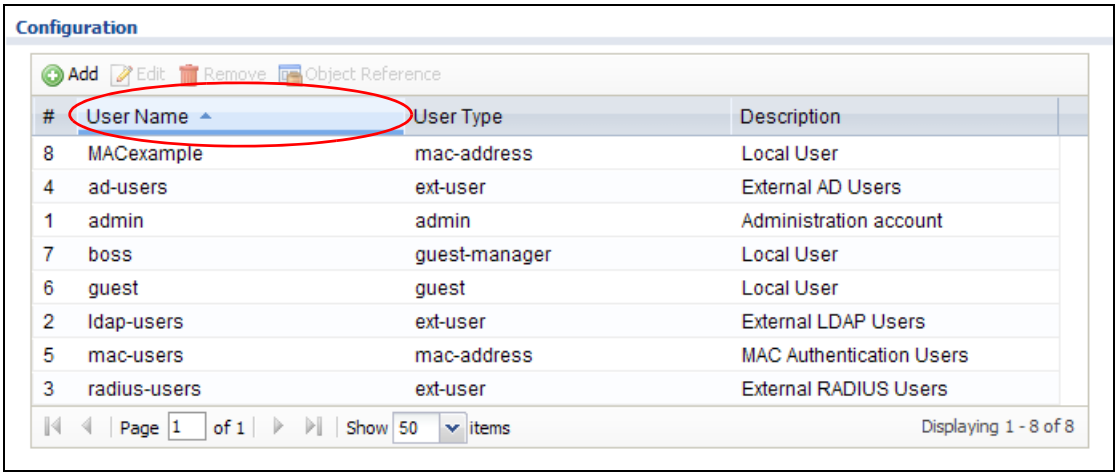
3.3.4 Таблицы и списки

Таблицы и списки Web-конфигуратора весьма гибки в настройке и предлагают несколько вариантов отображения собственных записей.

Манипуляция отображением таблиц

Существует несколько вариантов манипуляции таблицами Web-конфигуратора.

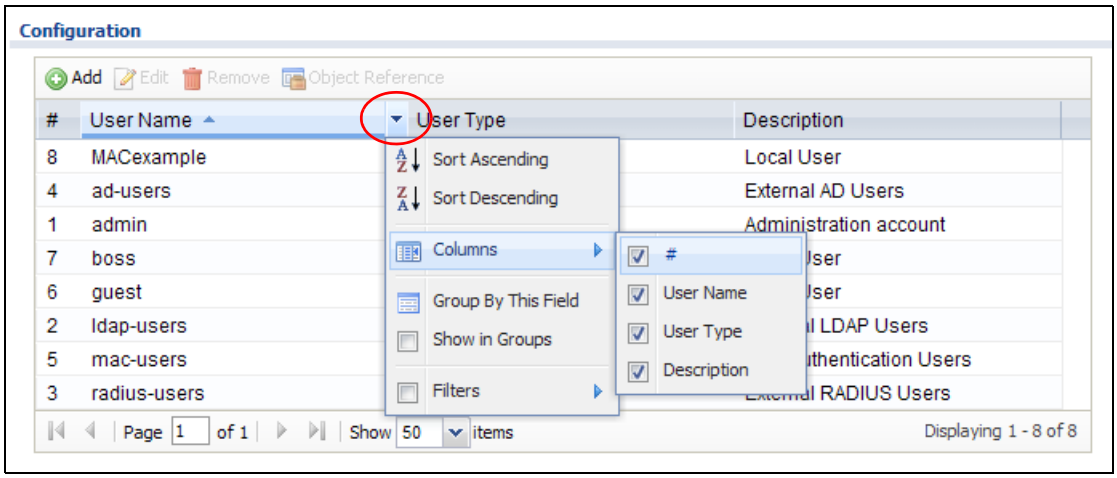
1 Нажатие на заголовок столбца позволяет отсортировать записи таблицы по значению в этом столбце.



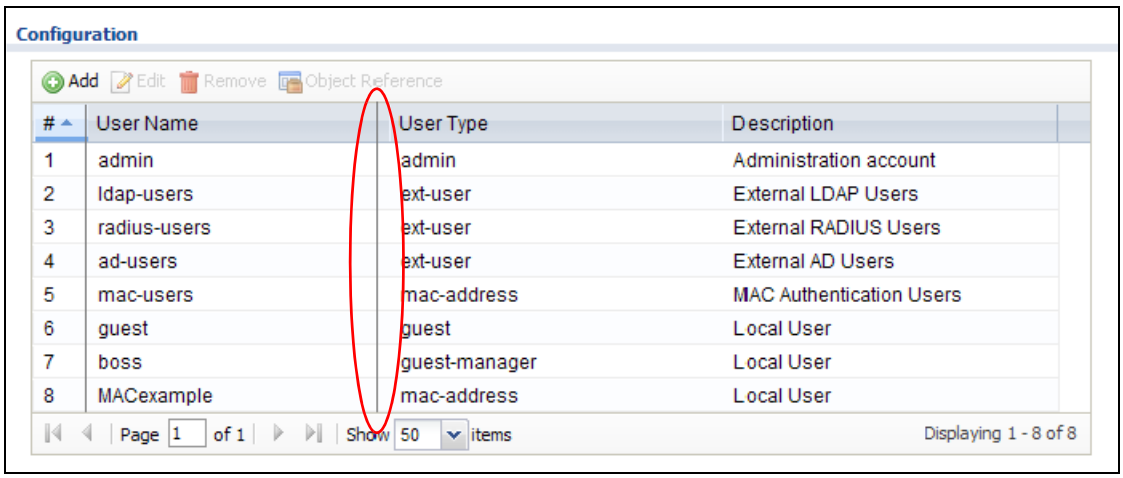
2 Нажатие на стрелку вниз рядом с заголовком столбца позволяет открыть дополнительные параметры отображения записей. Доступные параметры зависят от типа поля в соответствующем столбце. Некоторые примеры приводятся ниже:

- Сортировка в возрастающем алфавитном порядке
- Сортировка в убывающем (обратном) алфавитном порядке
- Выбор столбцов для отображения
- Группировка записей по полю
- Отображение записей по группам

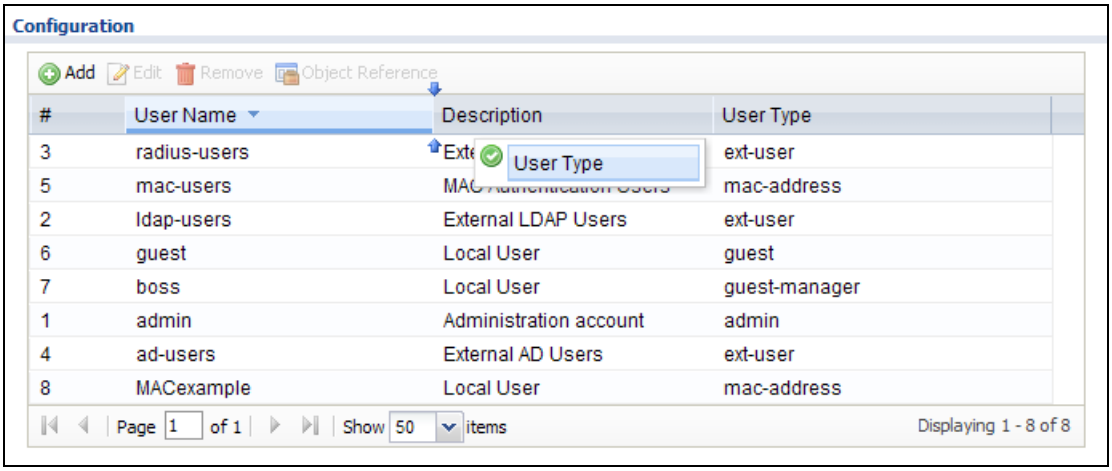
- Фильтрация с использованием математических операторов (<, > или =) или поиск по тексту.



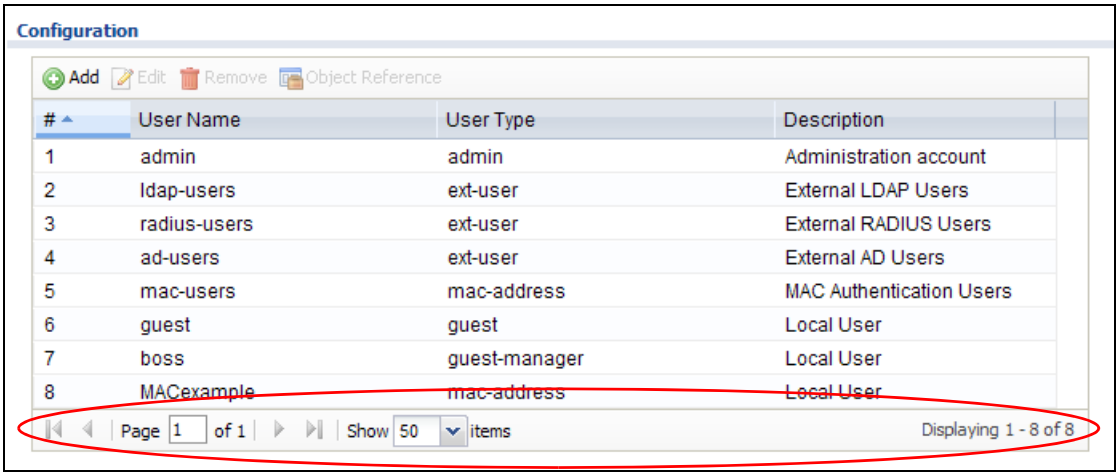
3 Чтобы изменить ширину столбца, необходимо перетащить его правую границу в заголовке.



4 Чтобы изменить порядок следования столбцов, перетащите в нужное место соответствующий заголовок. При перетаскивании столбца в новое допустимое положение у его заголовка появляется зеленый значок «галочки».



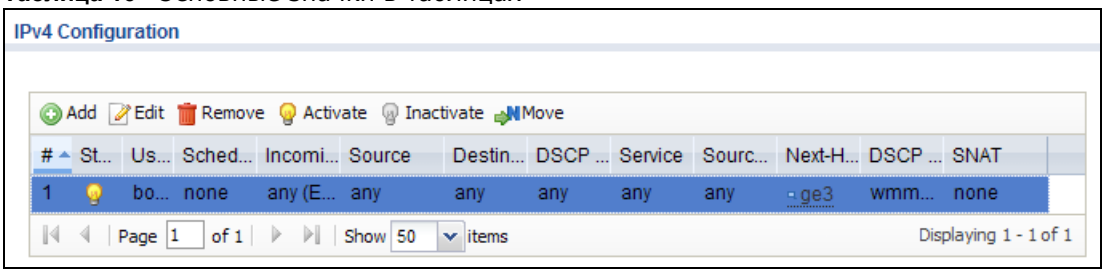
5 Перемещение между различными страницами записей и управление количеством одновременно отображаемых записей осуществляется с использованием значков и полей в нижней части таблицы.



Работа с записями в таблицах

В таблицах предусмотрены значки для работы с записями таблицы. Ниже показан пример. С помощью клавиш [Shift] или [Ctrl] в большинстве случаев можно выбрать несколько записей для удаления, включения или отключения.

Таблица 16 Основные значки в таблицах



Описание наиболее часто используемых значков для таблиц приводится ниже.

Таблица 17 Основные значки в таблицах

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись. Для тех функций, для которых позиция записи в упорядоченном списке имеет значение (это функции, в которых устройство NXC применяет записи таблицы поочередно), для создания новой записи под определенной записью нужно выбрать эту запись и нажать **Add**.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**. В некоторых таблицах для изменения значений записи достаточно щелкнуть на ней и ввести новые значения непосредственно в таблице. В таких таблицах у записей, которые были изменены, но изменения еще не были применены, отображается небольшой красный треугольник.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.

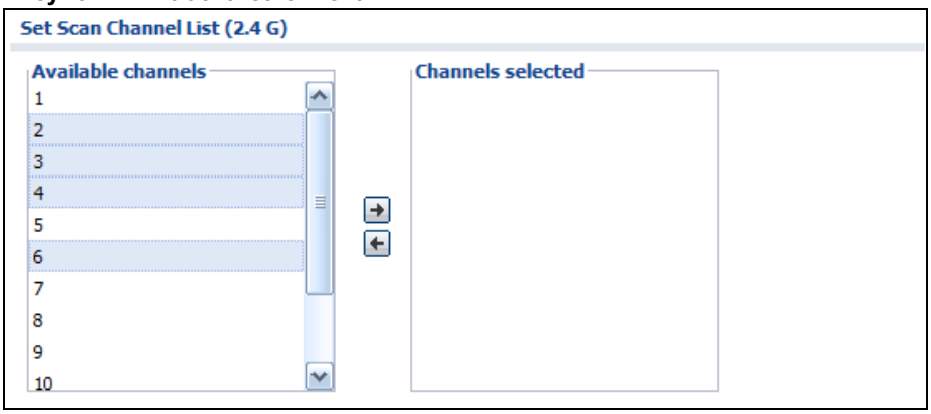
Таблица 17 Основные значки в таблицах (продолжение)

ПОЛЕ	ОПИСАНИЕ
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
Move	Чтобы изменить положение записи в нумерованном списке необходимо выбрать ее и нажать на **Move**. При этом появится поле, в которое можно ввести номер позиции, на которую необходимо перенести запись. Перемещение записи в новое место осуществляется после нажатия на [ENTER]. Например, если ввести в это поле значение 6, то перемещаемая запись станет записью под номером 6, а предыдущая запись под номером 6 (если таковая была) будет сдвинута на одну позицию вверх (или вниз).

Работа со списками

В тех случаях, когда рядом со списком выбранных значений отображается список доступных значений, перемещение элемента из одного списка в другой в большинстве случаев может быть выполнено двойным щелчком. В некоторых списках можно также использовать клавиши [Shift] или [Ctrl] для выбора нескольких значений, после чего перенести их в другой список нажатием на кнопки со стрелками.

Рисунок 17 Работа со списками



Часть II
Техническое справочное руководство

4

Панель мониторинга

4.1 Обзор

Для ознакомления с информацией о состоянии устройства NXC используйте экраны панели мониторинга (**Dashboard**).

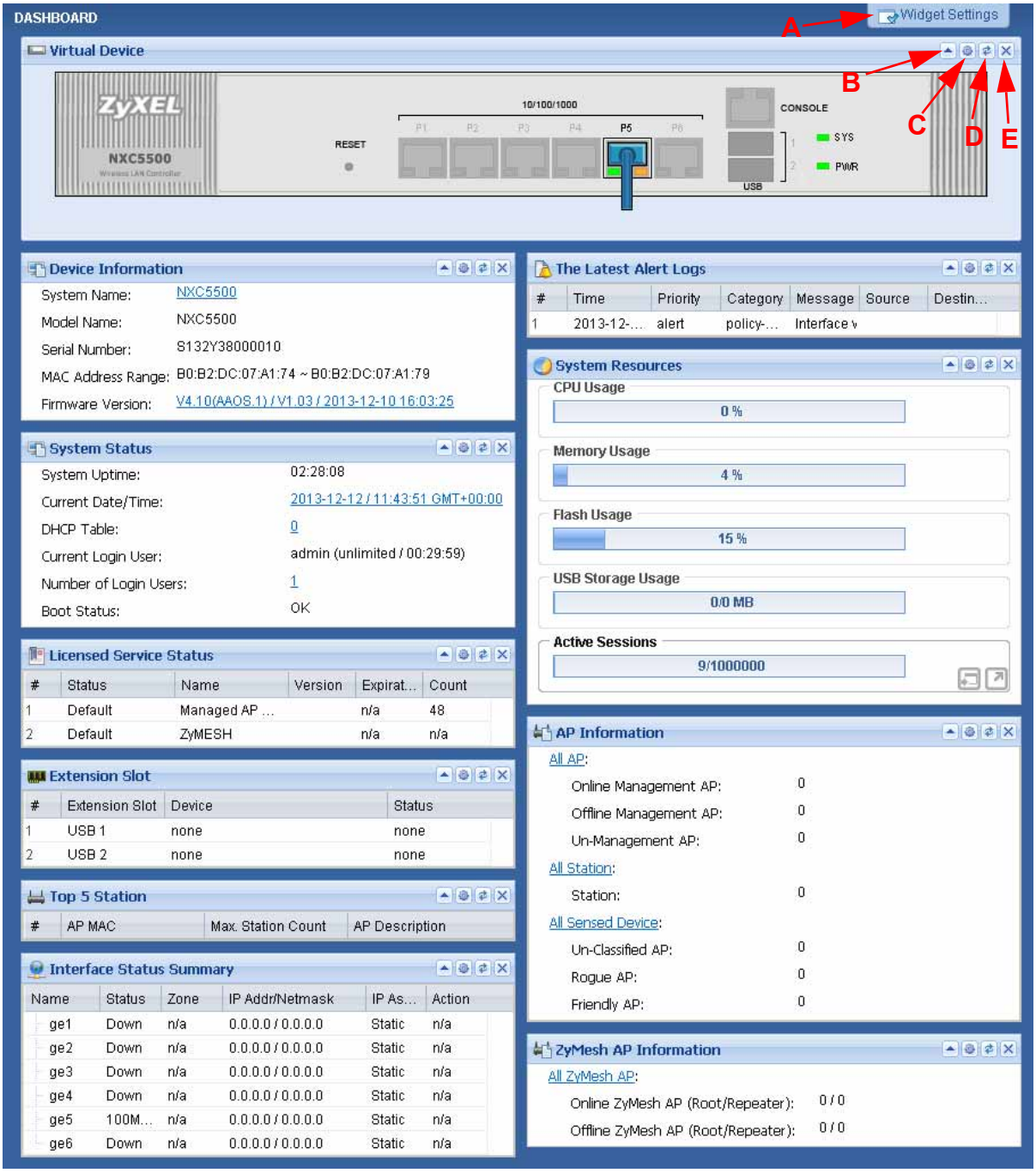
4.1.1 О чем рассказывается в этой главе

- На основном экране панели мониторинга (разд. 4.2 на стр. 49) отображается общая информация об устройстве NXC, состояние системы, сведения об утилизации системных ресурсов, состояние лицензированных служб и состояние интерфейсов. Более подробную информацию можно увидеть на других экранах состояния.
- На экране **DHCP Table** (разд. 4.2.4 на стр. 56) отображаются IP-адреса, ассоциированные в данный момент с DHCP-клиентами, и IP-адреса, зарезервированные для определенных MAC-адресов.
- На экране **Number of Login Users** (разд. 4.2.5 на стр. 57) отображается список пользователей, которые в данный момент выполнили вход на устройство NXC.

4.2 Панель мониторинга (Dashboard)

Этот экран – это первое, что появляется при входе на устройство NXC. Кроме того, он появляется каждый раз при нажатии на пиктограмму **Dashboard** в навигационной панели. На панели мониторинга в форме виджетов, которые можно перемещать по своему усмотрению, отображается общая информация об устройстве, состояние системы, сведения об утилизации системных ресурсов, состояние лицензированных служб и состояние интерфейсов. Отдельные виджеты можно сворачивать, обновлять и закрывать.

Рисунок 18 Панель мониторинга (Dashboard)



Поля экрана описаны в следующей таблице.

Таблица 18 Панель мониторинга (Dashboard)

ПОЛЕ	ОПИСАНИЕ
Widget Settings (A)	С помощью этой ссылки можно снова открыть ранее закрытые виджеты. Виджеты, которые уже открыты, отображаются в сером цвете.
Arrow (B)	С помощью этой ссылки можно свернуть или развернуть виджет.
Refresh Time Setting (C)	Этот параметр задает интервал обновления информации, отображаемой виджетом.
Refresh Now (D)	С помощью этой ссылки можно немедленно обновить информацию в данном виджете.
Close Widget (E)	С помощью этой ссылки можно закрыть виджет. Чтобы снова открыть виджет, воспользуйтесь ссылкой **Widget Settings**.
Virtual Device	Наведите курсор мыши на изображение индикатора или подключенного порта Ethernet, чтобы вывести на экран подробную информацию о состоянии индикаторов и соединений устройства NXC. Описание индикаторов можно найти в разд. 2.2.3 на стр. 26. Интерфейс без подключения отображается в сером цвете. При наведении курсора на подключенный интерфейс на экране появляются следующие поля.
Name	В этом поле отображается имя интерфейса или слота.
Status	В этом поле отображается текущее состояние каждого интерфейса или устройства, установленного в слоте. Возможные значения параметра зависят от типа интерфейса. **Inactive** – Интерфейс Ethernet отключен. **Down** – Интерфейс Ethernet включен, но на нем нет подключения. **Speed / Duplex** – Интерфейс Ethernet включен, и на нем есть подключение. В этом поле отображается скорость порта и настройки дуплексного режима (**Full или Half** – дуплекс или полудуплекс).
Zone	В этом поле отображается зона, которой назначен в настоящее время данный интерфейс.
IP Address/Mask	В этом поле отображается текущие IP-адрес и маска подсети, назначенные данному интерфейсу.
Device Information	
System Name	В этом поле отображается имя, которое используется для идентификации устройства NXC в любой сети. Щелкните по этой ссылке, чтобы открыть экран, на котором можно поменять имя.
Модель	В этом поле отображается название модели устройства NXC.
Serial Number	В этом поле отображается серийный номер данного устройства NXC.
MAC Address Range	В этом поле отображается список MAC-адресов, используемых данным устройством NXC. Каждый физический порт имеет только один MAC-адрес. Первый MAC-адрес присваивается физическому порту 1, второй MAC-адрес – физическому порту 2 и т.д.
Firmware Version	В этом поле отображается номер версии и дата встроенного программного обеспечения, под управлением которого в настоящее время работает устройство NXC. Щелкните по этой ссылке, чтобы открыть экран, на котором можно выполнить выгрузку встроенного программного обеспечения.
System Status	
System Uptime	В этом поле отображается время работы устройства NXC с момента последнего перезапуска или включения питания.

Таблица 18 Панель мониторинга (Dashboard) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Current Date/ Time	В этом поле отображаются текущие дата и время устройства NXC. Значение в этом поле имеет следующий формат: гггг-мм-дд чч:мм:сс. Щелкните по этой ссылке, чтобы открыть экран, на котором можно задать дату и время для устройства NXC.
DHCP Table	В этом поле отображается количество IP-адресов, назначенных устройством NXC через DHCP. Щелкните по этой ссылке, чтобы вывести список IP-адресов, назначенных DHCP-клиентам устройства NXC, и список IP-адресов, зарезервированных для определенных MAC-адресов.
Current Login User	В этом поле отображается имя пользователя, под которым выполняется текущая сессия, время, остающееся до повторной аутентификации, и оставшееся время аренды.
Number of Login Users	В этом поле отображается количество пользователей, выполнивших в настоящее время вход на устройство NXC. Щелкните по этой ссылке, чтобы вывести во всплывающем окне список пользователей, выполнивших в настоящее время вход на устройство NXC.
Boot Status	В этом поле отображается подробная информация о состоянии запуска устройства NXC. **OK** – Запуск устройства NXC завершился успешно. **Firmware update OK –** Обновление встроенного программного обеспечения завершено успешно. **Problematic configuration after firmware update** – Не удалось применить настройки конфигурации после обновления программного обеспечения. **System default configuration** – Конфигурация по умолчанию успешно применена для устройства NXC. Это происходит при первом запуске устройства NXC, либо при умышленном сбросе конфигурации устройства NXC до системных значений по умолчанию. **Fallback to lastgood configuration** – Устройству NXC не удалось применить настройки конфигурационного файла startup-config.conf, поэтому был выполнен возврат к последнему успешно примененному конфигурационному файлу lastgood.conf. **Fallback to system default configuration** – Устройству NXC не удалось применить конфигурационный файл lastgood.conf, поэтому был выполнен возврат к системному конфигурационному файлу с настройками по умолчанию (system-default.conf). **Booting in progress** – Идет процесс применения системной конфигурации устройством NXC.
Licensed Service Status	
#	В этом поле отображается количество лицензированных служб.
Status	В этом поле отображается текущий состояние лицензии.
Name	Значение в этом поле идентифицирует лицензированную службу.
Version	В этом поле отображается номер версии службы.
Expiration	Если лицензия на службу является действующей, то в этом поле отображается дата истечения срока ее действия. Значение «**n/a**» означает, что срок действия лицензии на данную службу не ограничен. Значение «**0**» отображается в том случае, если служба не является лицензируемой, или срок действия лицензии истек.
Count	В этом поле отображается количество точек управляемых точек доступа, которые данное устройство NXC способно поддерживать при текущей лицензии. Это поле не применимо для других служб.
Extension Slot	В этой части экрана отображается информация о состоянии USB-портов.

Таблица 18 Панель мониторинга (Dashboard) (продолжение)

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается количество USB-портов.
Extension Slot	В этом поле отображается имя каждого слота расширения.
Устройство	В этом поле отображается имя устройства, подключенного к данному слоту расширения (или **none**, если никаких устройств не обнаружено).
Status	**Ready** – USB-накопитель, подключенный к устройству NXC, готов к использованию устройством NXC. **none** – Устройству NXC не удается смонтировать подключенный к устройству NXC USB-накопитель.
Top 5 Station	Отображает первые 5 точек доступа с максимальным номером подключений (беспроводных клиентов).
#	В этом поле отображается ранг станции.
AP MAC	В этом поле отображается MAC-адрес точки доступа, к которой принадлежит данная станция.
Max. Station Count	В этом поле отображается максимальное количество беспроводных клиентов, которые когда-либо подключались к данной точке доступа.
AP Description	В этом поле отображается описание точки доступа. Формат описания по умолчанию выглядит так: «AP-» плюс MAC-адрес точки доступа.
System Resources	
CPU Usage	В этом поле отображается доля (в процентах) вычислительной процессорной мощности устройства NXC, которая используется в настоящее время. Наведите курсор на это поле, чтобы вывести на экран пиктограмму **Show CPU Usage**, которая позволяет открыть график использования процессорных ресурсов устройства NXC за последнее время.
Memory Usage	В этом поле отображается доля (в процентах) используемой в настоящее время оперативной памяти устройства NXC. Наведите курсор на это поле, чтобы вывести на экран пиктограмму **Show Memory Usage**, которая позволяет открыть график использования оперативной памяти устройства NXC за последнее время.
Flash Usage	В этом поле отображается доля (в процентах) используемой в настоящее время встроенной флэш-памяти устройства NXC.
USB Storage Usage	В этом поле отображается объем используемого пространства USB-накопителя, подключенного к устройству NXC.
Active Sessions	В этом поле отображается количество сессий трафика, открытых в настоящее время на устройстве NXC. Здесь будут перечислены сессии, в рамках которых трафик проходит через устройство NXC. Наведите курсор мыши на это поле, чтобы вывести на экран пиктограммы. Нажмите на пиктограмму **Detail**, чтобы перейти на экран **Session Monitor**, содержащий подробную информацию об активных сессиях. Нажмите на пиктограмму **Show Active Sessions**, чтобы отобразить график сессий устройства NXC за последнее время.
Interface Status Summary	
Name	В этом поле отображается название каждого интерфейса.
Status	В этом поле отображается текущее состояние каждого интерфейса. Возможные значения параметра зависят от типа интерфейса. **Inactive** – Интерфейс Ethernet отключен. **Down** – Интерфейс Ethernet включен, но на нем нет подключения. **Speed / Duplex** – Интерфейс Ethernet включен, и на нем есть подключение. В этом поле отображается скорость порта и настройки дуплексного режима (**Full или Half** – дуплекс или полудуплекс).

Таблица 18 Панель мониторинга (Dashboard) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Zone	В этом поле отображается зона, которой назначен в настоящее время данный интерфейс.
IP Addr/ Netmask	В этом поле отображается текущие IP-адрес и маска подсети, назначенные данному интерфейсу. Если IP-адрес выглядит как 0.0.0.0, это означает, что интерфейс либо отключен, либо ему не были назначены IP-адрес и маска подсети через DHCP.
IP Assignment	В этом поле отображается способ получения интерфейсом IP-адреса. **Static** – Этот интерфейс имеет статический IP-адрес. **DHCP Client** – Этот интерфейс получает IP-адрес от DHCP-сервера.
Action	С помощью этого поля можно получить информацию или изменить IP-адрес для данного интерфейса. Нажмите **Renew**, чтобы отправить новый DHCP-запрос DHCP-серверу.
The Latest Alert Logs	В этой части экрана отображается информация из недавно сгенерированных устройством NXC журналов.
#	Это ранг записи в списке журналов оповещений.
Time	В этом поле отображаются дата и время создания журнала.
Priority	В этом поле отображается уровень серьезности журнала.
Категория	В этом поле отображается тип генерируемого журнала.
Message	В этом поле отображается фактическое сообщение журнала.
Source	В этом поле отображается адрес источника (если таковой есть) в пакете, который сгенерировал журнал.
Destination	В этом поле отображается адрес назначения (если таковой есть) в пакете, который сгенерировал журнал.
AP Information	Здесь отображаются общие сведения о подключенных беспроводных точках доступа.
All AP	В этой части экрана представлены общие сведения обо всех подключенных беспроводных точках доступа. Щелкните по этой ссылке, чтобы перейти к экрану **AP information** > **AP List**.
Online Management AP	Это поле показывает количество подключенных в настоящий момент управляемых точек доступа.
Offline Management AP	Это поле показывает количество находящихся сейчас в отключенном состоянии управляемых точек доступа.
Un-Management AP	Это поле показывает количество неуправляемых точек доступа.
All Station	В этой части экрана представлены общие сведения о подключенных станциях. Щелкните по этой ссылке, чтобы перейти к экрану **Station Info** > **Station List**.
Station	Это поле показывает количество станций, подключенных к сети в настоящий момент.
All Sensed Device	В этой части экрана отображаются общие сведения обо всех беспроводных устройствах, обнаруженных в сети. Щелкните по этой ссылке, чтобы перейти к экрану **Rogue AP** > **Detected Device**.
Un-Classified AP	Это поле показывает количество обнаруженных неклассифицированных точек доступа.
Rogue AP	Это поле показывает количество обнаруженных мошеннических точек доступа.
Friendly AP	Это поле показывает количество обнаруженных дружественных точек доступа.
ZyMesh AP Information	Здесь содержится общая информация об управляемых точках доступа, которые выступают в качестве корневых точек доступа или повторителей для формирования ZyMesh/WDS.

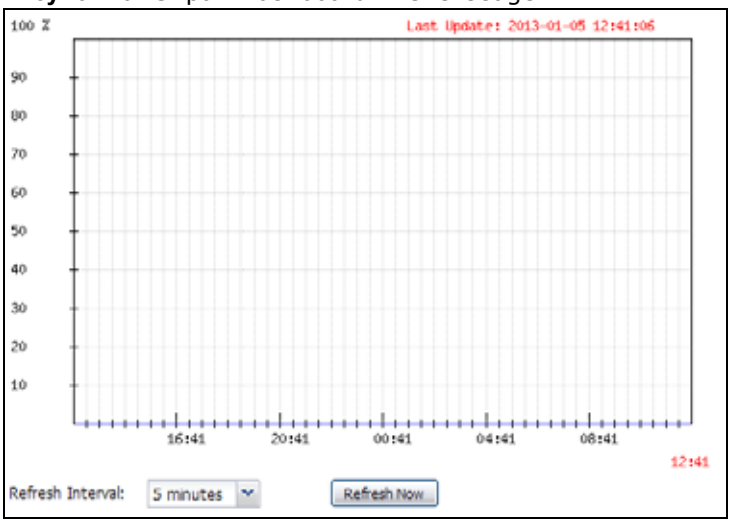
Таблица 18 Панель мониторинга (Dashboard) (продолжение)

ПОЛЕ	ОПИСАНИЕ
All ZyMesh AP	В этой части экрана представлена общая информация обо всех точках доступа ZyMesh. Щелкните по этой ссылке, чтобы перейти к экрану **Monitor > Wireless > All ZyMesh AP > ZyMesh Link Info**.
Online ZyMesh AP	Это поле показывает количество подключенных в настоящее время точек доступа ZyMesh.
Offline ZyMesh AP	Это поле показывает количество точек доступа ZyMesh, находящихся в отключенном состоянии.

4.2.1 Экран CPU Usage

На этом экране устройства NXCможно увидеть информацию о потреблении процессорных ресурсов за последнее время. Чтобы открыть этот экран, выберите в меню панели мониторинга **Show CPU Usage**.

Рисунок 19 Экран Dashboard > CPU Usage



Поля экрана описаны в следующей таблице.

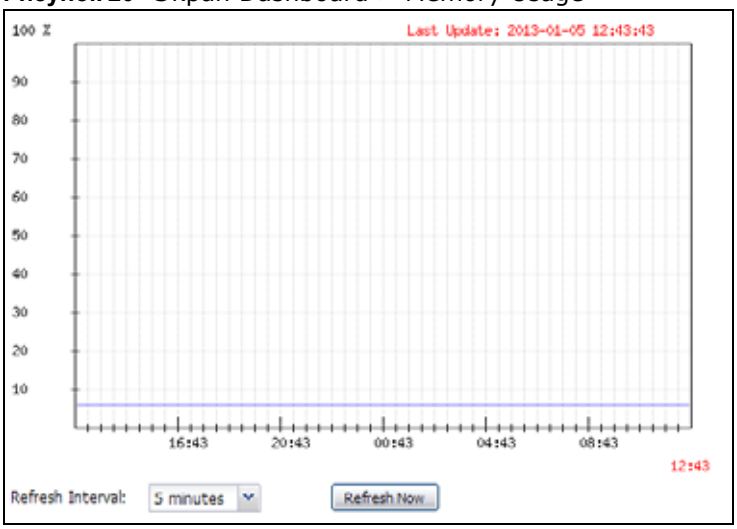
Таблица 19 Экран Dashboard > CPU Usage

ПОЛЕ	ОПИСАНИЕ
	На оси y показан процент использования процессорных ресурсов.
	На оси x показан временной интервал, за который отслеживалось использование процессорных ресурсов
Refresh Interval	Укажите период автоматического обновления информации в этом окне.
Refresh Now	Нажмите на эту кнопку, чтобы обновить информацию в этом окне немедленно.

4.2.2 Экран Memory Usage

На этом экране устройства NXCможно увидеть информацию об использовании оперативной памяти (ОЗУ). Чтобы открыть этот экран, выберите в меню панели мониторинга **Show Memory Usage**.

Рисунок 20 Экран Dashboard > Memory Usage



Поля экрана описаны в следующей таблице.

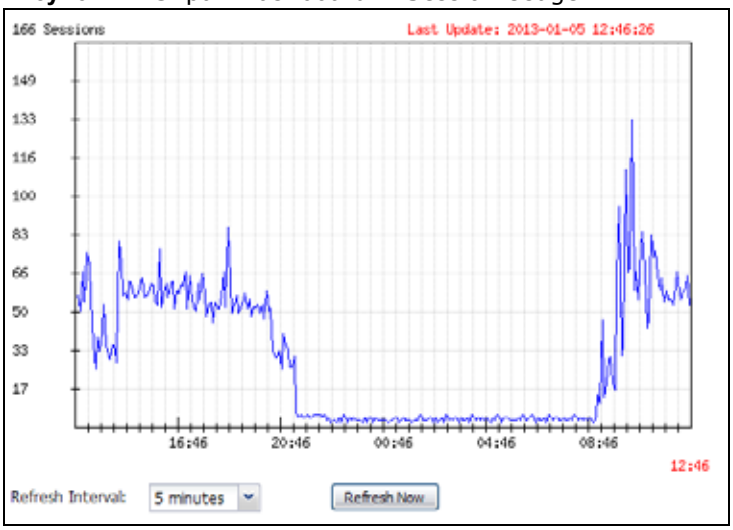
Таблица 20 Экран Dashboard > Memory Usage

ПОЛЕ	ОПИСАНИЕ
	На оси y показан процент использования ОЗУ.
	На оси x показан временной интервал, за который отслеживалось использование ОЗУ
Refresh Interval	Укажите период автоматического обновления информации в этом окне.
Refresh Now	Нажмите на эту кнопку, чтобы обновить информацию в этом окне немедленно.

4.2.3 Экран Session Usage

На этом экране устройства NXCможно увидеть информацию об использовании сессий трафика за последнее время. Чтобы открыть этот экран, выберите в меню панели мониторинга **Show Active Sessions**.

Рисунок 21 Экран Dashboard > Session Usage



Поля экрана описаны в следующей таблице.

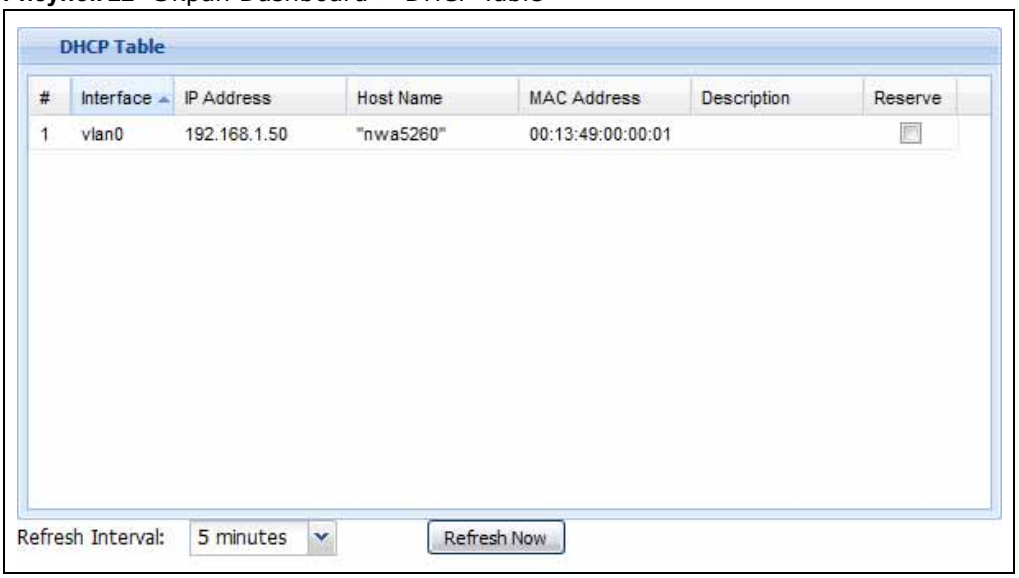
Таблица 21 Экран Dashboard > Session Usage

ПОЛЕ	ОПИСАНИЕ
Sessions	На оси y показано количество сессий.
	На оси x показан временной интервал, за который отслеживалось использование сессий
Refresh Interval	Укажите период автоматического обновления информации в этом окне.
Refresh Now	Нажмите на эту кнопку, чтобы обновить информацию в этом окне немедленно.

4.2.4 Экран DHCP Table

На этом экране можно увидеть списки IP-адресов, назначенных DHCP-клиентам на текущий момент, и IP-адресов, зарезервированных для определенных MAC-адресов. Чтобы открыть этот экран, нажмите на пиктограмму, расположенную под надписью **DHCP Table** в панели мониторинга.

Рисунок 22 Экран Dashboard > DHCP Table



Поля экрана описаны в следующей таблице.

Таблица 22 Экран Dashboard > DHCP Table

ПОЛЕ	ОПИСАНИЕ
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
Interface	Это поле идентифицирует интерфейс, который назначил IP-адрес DHCP-клиенту.
IP Address	В этом поле отображается IP-адрес, назначенный DHCP-клиенту в данный момент или зарезервированный для определенного MAC-адреса. Чтобы отсортировать записи в таблице по IP-адресу, щелкните по заголовку столбца. Чтобы поменять порядок сортировки на обратный, щелкните по заголовку столбца еще раз.
Host Name	В этом поле отображается имя, используемое для идентификации устройства в сети (имя компьютера). Устройство NXC получает эти имена из запросов DHCP-клиентов. Значение «None» указывает на то, что это статическая запись DHCP.

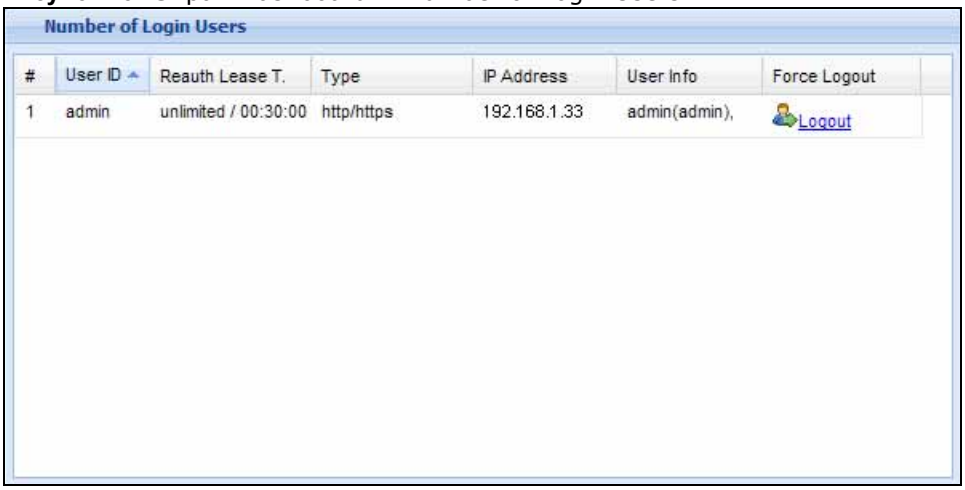
Таблица 22 Экран Dashboard > DHCP Table (продолжение)

ПОЛЕ	ОПИСАНИЕ
MAC Address	В этом поле отображается MAC-адрес, которому назначен данный IP-адрес в данный момент или для которого данный IP-адрес зарезервирован. Чтобы отсортировать записи в таблице по MAC-адресу, щелкните по заголовку столбца. Чтобы поменять порядок сортировки на обратный, щелкните по заголовку столбца еще раз.
Description	Для статических записей DHCP в этом поле будет отображаться имя хоста или введенное описание. Для динамических записей DHCP это поле будет пустым.
Reserve	Если в этом поле установлен переключатель для определенной записи, то эта запись является статической записью DHCP. Данный IP-адрес зарезервирован для данного MAC-адреса. Если переключатель в этом поле не установлен, то эта запись является динамической записью DHCP. Данный IP-адрес назначен DHCP-клиентом. Чтобы создать статическую запись DHCP на основе существующей динамической записи DHCP, установите переключатель в этом поле. Чтобы удалить статическую запись DHCP, очистите это поле.

4.2.5 Экран Number of Login Users

На этом экране можно увидеть список пользователей, выполнивших в данный момент вход на устройство NXC. Чтобы открыть этот экран, нажмите на пиктограмму **Number of Login Users** на панели мониторинга.

Рисунок 23 Экран Dashboard > Number of Login Users



Поля экрана описаны в следующей таблице.

Таблица 23 Экран Dashboard > Number of Login Users

ПОЛЕ	ОПИСАНИЕ
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
User ID	В этом поле отображается имя каждого пользователя, выполнившего в данный момент вход на устройство NXC.
Reauth Lease T.	В этом поле отображается время, оставшееся до повторной аутентификации, и время окончания аренды, оставшееся для каждого пользователя.
Type	В этом поле отображается способ, с помощью которого пользователь выполнил вход на устройство NXC.

Таблица 23 Экран Dashboard > Number of Login Users (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Address	В этом поле отображается IP-адрес компьютера, с которого осуществлен вход на устройство NXC.
User Info	В этом поле отображаются типы и имена пользователей, которые использует устройство NXC. Для типа пользователя **ext-user** (внешний пользователь) в этом поле будет показана информация о его внешней группе при наведении курсора мыши. Если внешнему пользователю соответствуют два объекта внешних групп, то в этом поле будут показаны имена обоих объектов.
Force Logout	Нажмите на эту пиктограмму, чтобы завершить сессию пользователя.

5

Мониторинг работы устройства

5.1 Обзор

Экраны **Monitor** служат для просмотра информации о состоянии и статистической информации.

5.1.1 О чем рассказывается в этой главе

- Экран **Port Statistics** (разд. 5.3 на стр. 60) показывает статистику пакетов для каждого физического порта.
- Экран **Port Statistics Graph** (разд. 5.3.1 на стр. 61) показывает линейный граф статистики пакетов для каждого физического порта.
- Экран **Interface Status** (разд. 5.4 на стр. 62) показывает все интерфейсы устройства NXC и статистику пакетов для них.
- Экран **Traffic Statistics** (разд. 5.5 на стр. 65) позволяет начать или остановить сбор данных и просмотреть статистику.
- Экран **Session Monitor** (разд. 5.6 на стр. 68) показывает информацию о сессиях в разбивке по пользователям или службам.
- Экран **IP/MAC Binding** (разд. 5.7 на стр. 71) показывает списки устройств, которые получили IP-адреса от интерфейсов устройства NXC со включенной привязкой IP/MAC.
- Экран **Login Users** (разд. 5.8 на стр. 71) показывает список пользователей, выполнивших в настоящее время вход на устройство NXC.
- Экран **Dynamic Guest** (разд. 5.9 на стр. 73) показывает список гостевых пользовательских учетных записей, которые создаются автоматически и дают возможность пользоваться службами устройства NXC в течение определенного периода времени.
- Экран **USB Storage** (разд. 5.10 на стр. 74) показывает информацию о подключенном USB-накопителе.
- Экран **AP List** (разд. 5.11 на стр. 75) показывает список точек доступа, подключенных к устройству NXC в настоящий момент.
- Экран **Radio List** (разд. 5.12 на стр. 79) показывает статистику по беспроводным радиопередатчикам каждой из точек доступа, подключенных к устройству NXC.
- Экран **ZyMesh Link Info** (разд. 5.13 на стр. 82) показывает статистику по соединениям ZyMesh/WDS между управляемыми точками доступа.
- Экран **Station List** (разд. 5.14 на стр. 83) показывает статистику по подключенным станциям (или «беспроводным клиентам»).
- Экран **Detected Device** (разд. 5.15 на стр. 85) показывает список беспроводных устройств, пассивно обнаруженных устройством NXC.
- Экран **View Log** (разд. 5.16 на стр. 86) показывает недавние сообщения журнала устройства NXC. Имеется возможность изменить способ показа журнала, организовать его отправку по электронной почте и стереть отображаемое содержимое журнала на этом экране.

- Экран **View AP Log** (разд. 5.17 на стр. 88) показывает сообщения журналов беспроводных точек доступа, подключенных к устройству NXC.

5.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Мошенническая точка доступа

Мошенническими называют точки доступа, которые действуют в зоне покрытия сети и при этом не контролируются администраторами сети. Они могут стать причиной возникновения брешей в политике безопасности сети. Более подробную информацию можно найти в гл. 19 на стр. 250.

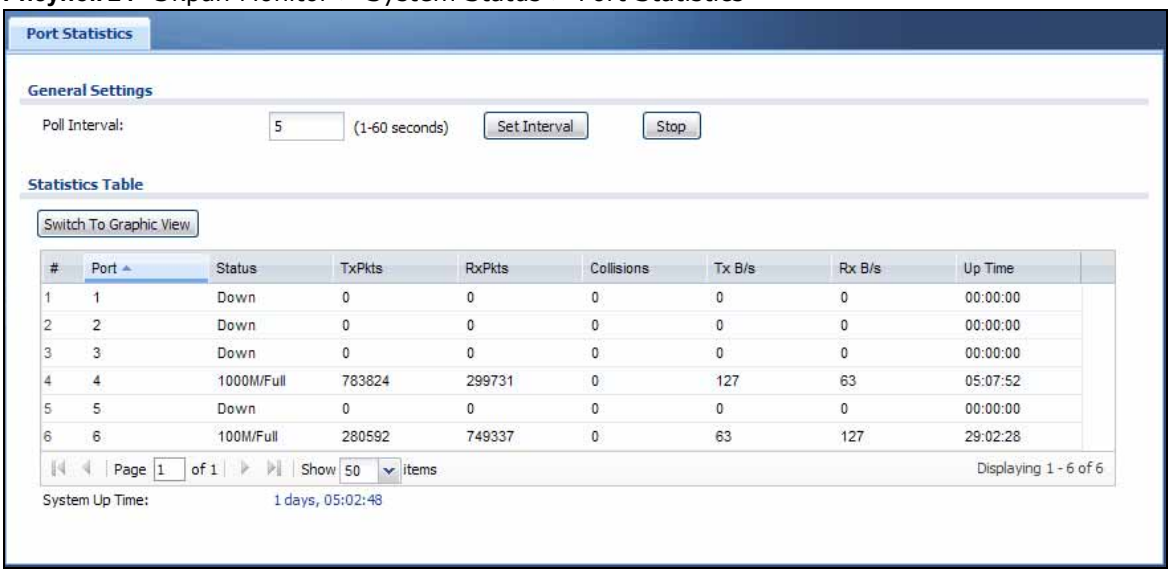
Дружественная точка доступа

Дружественными точками доступа называют другие точки доступа, которые обнаружены в сети, а также любые другие точки доступа, о которых известно, что они не представляют угрозы (например, точки доступа из соседних сетей). Более подробную информацию можно найти в гл. 19 на стр. 250.

5.3 Экран Port Statistics

Этот экран показывает статистику пакетов для каждого порта Gigabit Ethernet. Чтобы открыть этот экран, выберите в меню **Monitor > System Status** > **Port Statistics**.

Рисунок 24 Экран Monitor > System Status > Port Statistics



Поля экрана описаны в следующей таблице.

Таблица 24 Экран Monitor > System Status > Port Statistics

ПОЛЕ	ОПИСАНИЕ
Poll Interval	Укажите желаемый интервал автоматического обновления информации в этом окне и нажмите кнопку **Set Interval**.
Set Interval	С помощью этой кнопки задается интервал опроса данных (значение в поле **Poll Interval**) для этого экрана.
Stop	С помощью этой кнопки можно остановить процесс автоматического обновления информации в окне. Чтобы снова запустить автоматическое обновление, задайте интервал обновления в поле **Poll Interval** и нажмите кнопку **Set Interval**.
Switch to Graphic View	Эта кнопка позволяет отобразить статистику по портам в виде линейного графа.
#	Это поле показывает номер порта в списке.
Port	Это поле показывает физический номер порта.
Status	Это поле показывает текущее состояние физического порта. **Down** – На физическом порту нет подключения. **Speed / Duplex** – На физическом порту есть подключение. В этом поле отображается скорость порта и настройки дуплексного режима (**Full или Half** – дуплекс или полудуплекс).
TxPkts	Это поле показывает количество пакетов, переданных устройством NXC через физический порт с момента последнего подключения.
RxPkts	Это поле показывает количество пакетов, полученных устройством NXC через физический порт с момента последнего подключения.
Collisions	Это поле показывает количество коллизий на физическом порту с момента последнего подключения.
Tx B/s	Это поле показывает скорость передачи в байтах в секунду на физическом порту с интервалом обновления экрана, равным одной секунде.
Rx B/s	Это поле показывает скорость приема в байтах в секунду на физическом порту с интервалом обновления экрана, равным одной секунде.
Up Time	Это поле показывает длительность подключения, установленного на данном физическом порту.
System Up Time	В этом поле отображается время работы устройства NXC с момента последнего перезапуска или включения питания.

5.3.1 Экран Port Statistics Graph

Экран Port Statistics Graph позволяет ознакомиться с линейным графом статистики пакетов для каждого физического порта. Чтобы открыть этот экран, выберите в меню **Monitor > System Status** > **Port Statistics**, а затем нажмите кнопку **Switch to Graphic View**.

Рисунок 25 Экран Monitor > System Status > Port Statistics > Switch to Graphic View

Поля экрана описаны в следующей таблице.

Таблица 25 Экран Monitor > System Status > Port Statistics > Switch to Graphic View

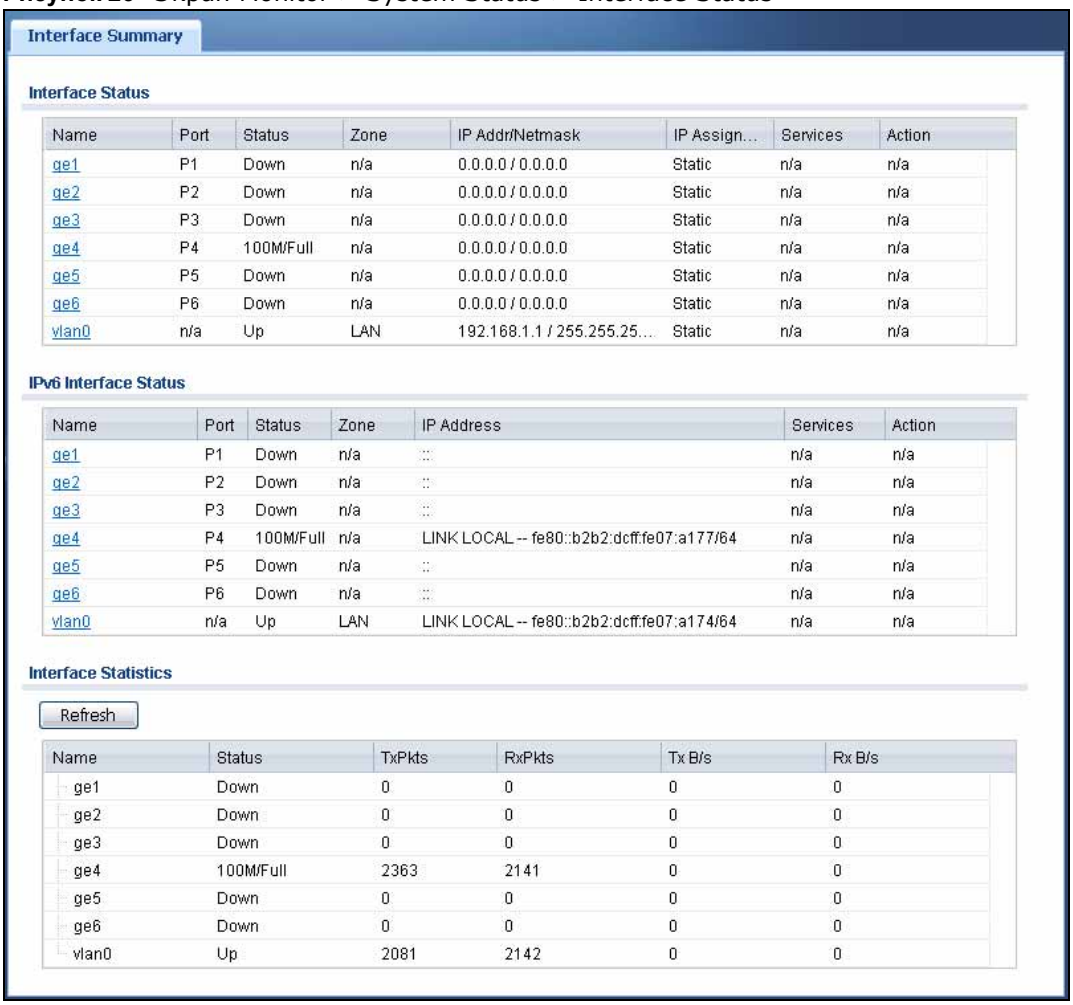
ПОЛЕ	ОПИСАНИЕ
Refresh Interval	Укажите период автоматического обновления информации в этом окне.
Refresh Now	Нажмите на эту кнопку, чтобы обновить информацию в этом окне немедленно.
Port Selection	Позволяет выбрать номер физического порта, для которого необходимо вывести графическое представление статистики.
Switch to Grid View	С помощью этой кнопки можно вернуть отображение статистики по порту в виде таблицы.
Mbps (Мбит/с)	На оси y показана скорость передачи или приема.
time	На оси x показан временной интервал, в течение которого отслеживался процесс передачи или приема пакетов
TX	Эта линия показывает трафик, переданный устройством NXC через физический порт с момента последнего подключения.
RX	Эта линия показывает трафик, полученный устройством NXC через физический порт с момента последнего подключения.
Last Update	В этом поле показаны дата и время последнего обновления информации в окне.

5.4 Экран Interface Status

На этом экране отображается список всех интерфейсов устройства NXC, и для каждого из них приведена статистика пакетов. Если включить поддержку IPv6 на экране **Configuration > System > IPv6**, то на этом экране также будет отображаться состояние интерфейса IPv6.

Чтобы перейти к этому экрану, выберите в меню **Monitor > System Status > Interface Status**.

Рисунок 26 Экран Monitor > System Status > Interface Status



Описание каждого из полей приведено в таблице ниже.

Таблица 26 Экран Monitor > System Status > Interface Status

ПОЛЕ	ОПИСАНИЕ
Interface Status IPv6 Interface Status	Раздел **Interface Status** описывает сетевые настройки IPv4. Раздел **IPv6 Interface Status** описывает сетевые настройки IPv6 (если устройство NXC подключается к сети IPv6). В обоих разделах присутствуют схожие поля, которые описаны ниже.
Name	В этом поле отображается название каждого интерфейса.
Port	Это поле показывает физический номер порта.

Таблица 26 Экран Monitor > System Status > Interface Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Status	В этом поле отображается текущее состояние каждого интерфейса. Возможные значения параметра зависят от типа интерфейса. Для интерфейсов Ethernet: **Inactive** – Интерфейс Ethernet отключен. **Down** – Интерфейс Ethernet включен, но на нем нет подключения. **Speed / Duplex** – Интерфейс Ethernet включен, и на нем есть подключение. В этом поле отображается скорость порта и настройки дуплексного режима (**Full или Half** – дуплекс или полудуплекс). Для интерфейсов VLAN: **Up** – Интерфейс VLAN включен, и на одном из участвующих интерфейсов Ethernet установлено подключение. **Down** – Интерфейс VLAN включен, но ни на одном из участвующих интерфейсов Ethernet нет подключений. **Inactive** – Интерфейс VLAN отключен.
Zone	В этом поле отображается зона, которой назначен данный интерфейс.
IP Addr/Netmask IP Address	В этом поле отображается текущие IP-адрес и маска подсети данного интерфейса. Если для IP-адреса и маски подсети отображается значение 0.0.0.0 (в сети IPv4) или для IP-адреса отображается значение :: (в сети IPv6), то это означает, что интерфейс выключен, или ему еще не назначен IP-адрес. Для сети IPv6 этот экран показывает еще и информацию о том, является ли IP-адрес статическим (**STATIC**), относящимся к локальному соединению (**LINK LOCAL**), динамически назначенным (**DHCP**) или IP-адресом IPv6 **SLAAC** (StateLess Address AutoConfiguration).Дополнительную информацию об IPv6 можно найти в прил. E на стр. 477.
IP Assignment	В этом поле отображается способ получения интерфейсом IP-адреса. **Static** – Этот интерфейс имеет статический IP-адрес. **DHCP Client** – Этот интерфейс получает IP-адрес от DHCP-сервера.
Services	Это поле отображает список служб, которые данный интерфейс предоставляет сети. В качестве примера можно привести «**DHCP relay**» и «**DHCP server**». Если данный интерфейс не предоставляет никаких служб сети, в этом поле отображается значение «**n/a**».
Action	С помощью этого поля можно получить информацию или изменить IP-адрес для данного интерфейса. Нажмите **Renew**, чтобы отправить новый DHCP-запрос DHCP-серверу. Чтобы попытаться подключиться к интерфейсу, нажмите кнопку **Connect**. Значение «**n/a**» в этом поле означает, что данный интерфейс не может использовать какой-либо из перечисленных способов получения или обновления IP-адреса.
Interface Statistics	В этой таблице содержится статистика пакетов для каждого интерфейса.
Refresh	Нажмите эту кнопку, чтобы обновить информацию на экране.
Name	В этом поле отображается название каждого интерфейса.

Таблица 26 Экран Monitor > System Status > Interface Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Status	В этом поле отображается текущее состояние каждого интерфейса. Возможные значения параметра зависят от типа интерфейса. Для интерфейсов Ethernet: **Inactive** – Интерфейс Ethernet отключен. **Down** – Интерфейс Ethernet включен, но на нем нет подключения. **Speed / Duplex** – Интерфейс Ethernet включен, и на нем есть подключение. В этом поле отображается скорость порта и настройки дуплексного режима (**Full или Half** – дуплекс или полудуплекс). Для интерфейсов VLAN: **Up** – Интерфейс VLAN включен, и на одном из участвующих интерфейсов Ethernet установлено подключение. **Down** – Интерфейс VLAN включен, но ни на одном из участвующих интерфейсов Ethernet нет подключений. **Inactive** – Интерфейс VLAN отключен.
TxPkts	Это поле показывает количество пакетов, переданных устройством NXC через интерфейс с момента последнего подключения.
RxPkts	Это поле показывает количество пакетов, полученных устройством NXC через интерфейс с момента последнего подключения.
Tx B/s	Это поле показывает скорость передачи в байтах в секунду через данный интерфейс с интервалом обновления экрана, равным одной секунде.
Rx B/s	Это поле показывает скорость приема в байтах в секунду через данный интерфейс с интервалом обновления экрана, равным одной секунде.

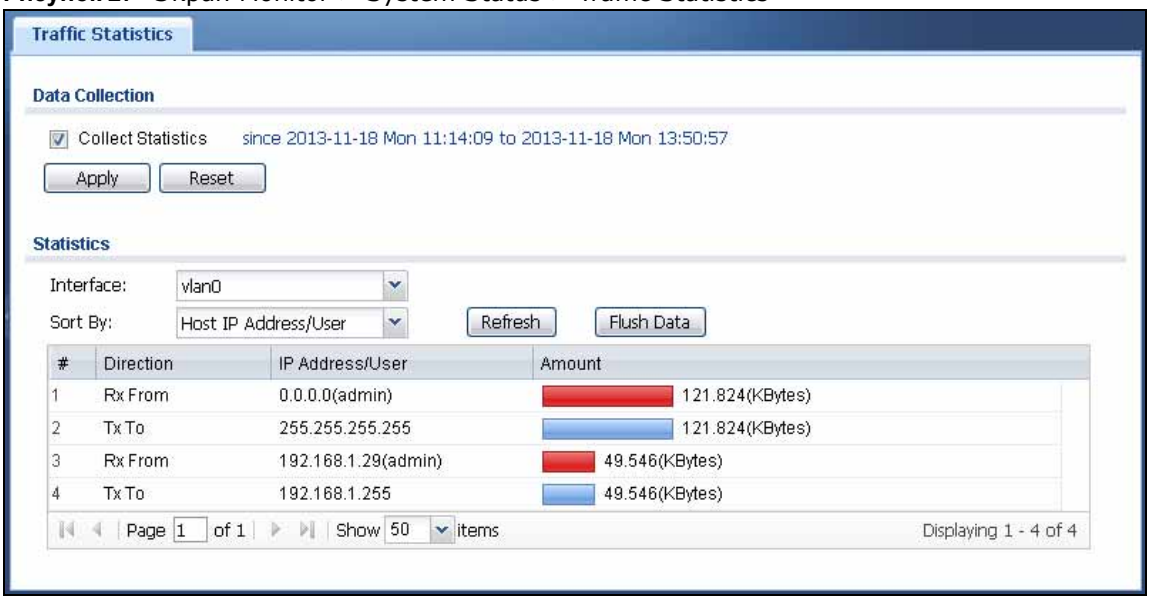
5.5 Экран Traffic Statistics

Чтобы открыть этот экран, выберите в меню **Monitor > System Status > Traffic Statistics**.Этот экран содержит основные сведения о различных видах трафика данных, проходящих через устройство NXC. Например:

- Наиболее часто посещаемые Web-сайты и количество посещений каждого сайта. В некоторых случаях значение этого счетчика может быть неточным, поскольку устройство NXC подсчитывает пакеты типа HTTP GET.
- Наиболее часто используемые протоколы или порты служб и объем трафика для каждого протокола/порта.
- IP-адреса локальной сети, через которые проходит максимальный объем трафика, с указанием объема входящего/исходящего трафика для каждого порта.

На экране **Traffic Statistics** можно запустить и остановить сбор информации устройством NXC для этих отчетов. Запускать или останавливать сбор данных по расписанию нельзя; это можно сделать только вручную на экране **Traffic Statistics**.

Рисунок 27 Экран Monitor > System Status > Traffic Statistics



Количество записей, отображаемых в отчете, ограничено. Дополнительную информацию можно найти в табл. 28 на стр. 68. Поля экрана описаны в следующей таблице.

Таблица 27 Экран Monitor > System Status > Traffic Statistics

ПОЛЕ	ОПИСАНИЕ
Data Collection	
Collect Statistics	Установите этот переключатель, чтобы устройство NXC собирало данные для данного отчета. Если устройство NXC уже выполняет сбор данных, то справа от этого поля отображается интервал сбора. Прогресс не отслеживается в реальном времени, но свежую информацию всегда можно получить, нажав кнопку **Refresh**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.
Statistics	
Interface	Выберите интерфейс, с которого требуется собирать информацию. Собирать информацию можно с интерфейсов Ethernet или VLAN.
Sort By	Выберите тип отчета для вывода на экран. Возможные варианты: **Host IP Address/User** – показывает IP-адреса или пользователей с максимальным трафиком, при этом для каждого IP-адреса/пользователя указывается объем полученного/отправленного трафика. **Service/Port** – показывает наиболее часто используемые протоколы или порты служб и объем трафика для каждого протокола/порта. **Web Site Hits** – показывает наиболее часто посещаемые Web-сайты и количество посещений каждого сайта. В каждом из перечисленных типов отчетов содержится разная информация (см. ниже).
Refresh	С помощью этой кнопки можно обновить содержимое отчета.
Flush Data	С помощью этой кнопки можно стереть всю статистику на экране и обновить содержимое отчета.
	Эти поля доступны для отчета с типом **Host IP Address/User**.
#	Это поле показывает ранг каждой записи. Список IP-адресов и пользователей отсортирован по объему трафика.

Таблица 27 Экран Monitor > System Status > Traffic Statistics (продолжение)

ПОЛЕ	ОПИСАНИЕ
Direction	Это поле указывает на то, является ли данный IP-адрес или пользователь отправителем или получателем трафика. **Rx From** – трафик идет от данного IP-адреса или пользователя на устройство NXC. **Tx To** – трафик поступает от устройства NXC на данный IP-адрес или к данному пользователю.
IP Address/User	В этом поле отображается IP-адрес или имя пользователя для данной записи. Максимальное число IP-адресов или пользователей для данного отчета показано в табл. 28 на стр. 68.
Amount	Это поле показывает объем трафика, который был отправлен или получен на указанный IP-адрес или данным пользователем. Если в поле **Direction** указано значение **Rx From**, на экране отображается красная полоса; если в поле **Direction** указано значение **Tx To**, на экране отображается синяя полоса. В качестве единицы измерения используются байты, килобайты, мегабайты или гигабайты, в зависимости от объема трафика для конкретного IP-адреса или пользователя. При прохождении установленного лимита байт счетчик начинает отсчитывать объем с нуля. См. табл. 28 на стр. 68.
	Эти поля доступны для отчета с типом **Service/Port**.
#	Это поле показывает ранг каждой записи. Протоколы и порты служб отсортированы по объему трафика.
Service Port	В этом поле отображается название службы и номер порта для данной записи. Максимальное число служб и портов для них для данного отчета показано в табл. 28 на стр. 68.
Protocol	Это поле показывает протокол, который использует данная служба.
Direction	Это поле указывает на то, является ли данный протокол или порт службы отправителем или получателем трафика. **Ingress** – через данный интерфейс трафик поступает на устройство NXC. **Egress** – через данный интерфейс трафик идет от устройства NXC.
Amount	Это поле показывает объем трафика, который был отправлен или получен указанной службой / портом. Если в поле **Direction** указано значение **Ingress**, на экране отображается красная полоса; если в поле **Direction** указано значение **Egress**, на экране отображается синяя полоса. В качестве единицы измерения используются байты, килобайты, мегабайты или гигабайты, в зависимости от объема трафика для конкретного протокола или порта службы. При прохождении установленного лимита байт счетчик начинает отсчитывать объем с нуля. См. табл. 28 на стр. 68.
	Эти поля доступны для отчета с типом **Web Site Hits**.
#	Это поле показывает ранг каждой записи. Имена доменов отсортированы по количеству посещений.
Web Site	В этом поле отображаются имена наиболее посещаемых доменов. Устройство NXC считает просмотр каждой страницы на Web-сайте за новое посещение. Максимальное число имен доменов для данного отчета показано в табл. 28 на стр. 68.
Hits	В этом поле отображается количество полученных Web-сайтом посещений. Устройство NXC считает посещения по количеству пакетов HTTP GET. Многие Web-сайты имеют ссылки HTTP GET на другие Web-сайты, и устройство NXC также считает их за посещения. При прохождении установленного лимита посещений счетчик начинает отсчитывать их с нуля. См. табл. 28 на стр. 68.

В таблице, приведенной ниже, описаны максимальное количество записей, отображаемых в отчете, ограничение для счетчика байт и ограничение для счетчика посещений.

Таблица 28 Максимальные значения для записей в отчетах

ПОЛЕ	ОПИСАНИЕ
Maximum Number of Records (макс. число записей)	20
Byte Count Limit (ограничение на число байт)	2^{64} байт; это меньше, чем 17 миллионов терабайт.
Hit Count Limit (макс. число посещений)	2^{64} посещения; это свыше 1,8 x 10^{19} посещений.

5.6 Экран Session Monitor

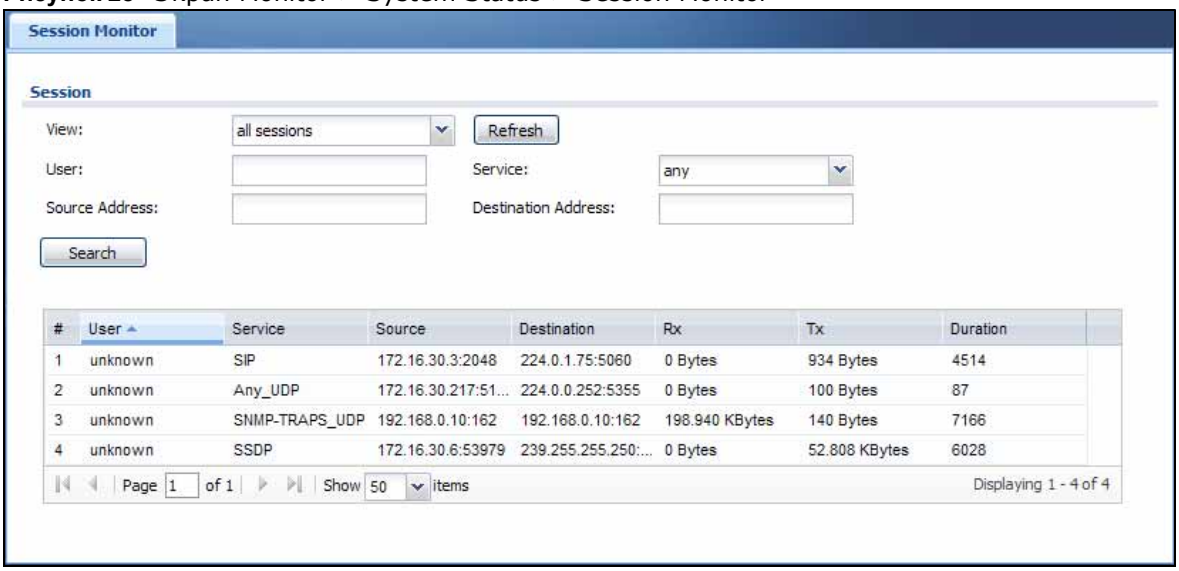
Этот экран показывает информацию об активных сессиях, которая нужна для отладки или статистического анализа. Управлять сессиями с помощью этого экрана нельзя. Экран отображает следующие сведения.

- Пользователь, который инициировал сессию
- Используемый протокол или порт службы
- IP-адрес источника
- IP-адрес назначения
- Количество принятых байт (на текущий момент)
- Количество отправленных байт (на текущий момент)
- Продолжительность (на текущий момент)

Сведения обо всех активных сессиях можно просмотреть в разрезе пользователей, служб, IP-адресов источника или IP-адресов назначения. Кроме того, можно отфильтровать информацию по имени пользователя, протоколу / службе или группе служб, адресу источника и/или адресу назначения и просмотреть ее в разбивке по именам пользователей.

Чтобы открыть следующий экран, выберите в меню **Monitor > System Status > Session Monitor**.

Рисунок 28 Экран Monitor > System Status > Session Monitor



Поля экрана описаны в следующей таблице.

Таблица 29 Экран Monitor > System Status > Session Monitor

ПОЛЕ	ОПИСАНИЕ
View	Выберите способ отображения информации. Возможные варианты: **sessions by users** (сессии по именам пользователей) – показ всех активных сессий, сгруппированных по имени пользователя **sessions by services** (сессии по службам) – показ всех активных сессий, сгруппированных по службе или протоколу **sessions by source IP** (сессии по IP-адресу источника) – показ всех активных сессий, сгруппированных по IP-адресу источника **sessions by destination IP** (сессии по IP-адресу назначения) – показ всех активных сессий, сгруппированных по IP-адресу назначения **all sessions** (все сессии) – фильтрация активных сессий по **имени пользователя**, **службе**, **адресу источника** и **адресу назначения** и отдельный показ сведений о каждой сессии (отсортированных по имени пользователя).
Refresh	Нажмите эту кнопку, чтобы обновить информацию на экране. При открытии и закрытии экран также обновляется автоматически.
	Поля **User**, **Service**, **Source Address** и **Destination Address** будут видны на экране при выборе значения «all sessions» (просмотр всех сессий). Выберите требуемые критерии фильтрации и нажмите кнопку **Search, чтобы отфильтровать список сессий**.
User	Это поле будет видно на экране, если в поле **View** выбрано значение «**all sessions**». Введите имя пользователя, сведения о сессиях которого необходимо увидеть. В этом поле нельзя набрать часть имени или использовать замещающие символы; имя пользователя необходимо ввести целиком.
Service	Это поле будет видно на экране, если в поле **View** выбрано значение «**all sessions**». Выберите службу или группу служб, сведения о сессиях которых необходимо увидеть. Устройство NXC идентифицирует службу, сравнивая протокол и порт назначения каждого пакета с протоколом и портом для всех определенных служб. (Более подробную информацию о службах можно найти в гл. 22 на стр. 264).
Source	Это поле будет видно на экране, если в поле **View** выбрано значение «**all sessions**». Введите IP-адрес источника для сессий, сведения о которых необходимо увидеть. Включить порт источника в запрос нельзя.

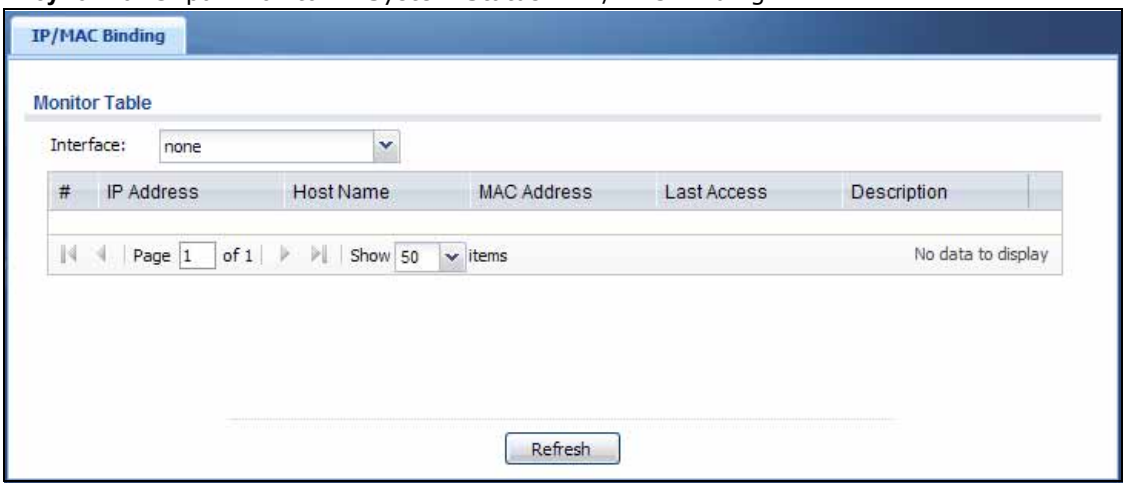
Таблица 29 Экран Monitor > System Status > Session Monitor (продолжение)

ПОЛЕ	ОПИСАНИЕ
Destination	Это поле будет видно на экране, если в поле **View** выбрано значение «**all sessions**». Введите IP-адрес назначения для сессий, сведения о которых необходимо увидеть. Включить порт назначения в запрос нельзя.
Search	Эта кнопка будет видна на экране, если в поле **View** выбрано значение «**all sessions**». Нажмите эту кнопку, чтобы обновить информацию на экране с учетом критериев фильтрации, указанных в полях **User**, **Service**, **Source Address** и **Destination Address**.
#	Это поле показывает порядковый номер для каждой активной сессии.
User	Это поле показывает имя пользователя каждой активной сессии. При просмотре отчетов, для которых в поле View выбрано значение «**sessions by users**» или «**all sessions**», можно использовать клавиши **+** и **–** для отображения или сокрытия подробной информации о пользовательских сессиях.
Service	В этом поле отображается протокол, используемый каждой активной сессией. При просмотре отчетов, для которых в поле View выбрано значение «**sessions by services**», можно использовать клавиши **+** или **–** для отображения или сокрытия подробной информации о сессиях, относящихся к данному протоколу.
Source	Это поле показывает IP-адрес и порт источника для каждой активной сессии. При просмотре отчетов, для которых в поле View выбрано значение «**sessions by source IP**», можно использовать клавиши **+** или **–** для отображения или сокрытия подробной информации о сессиях, у которых в качестве IP-адреса источника указан данный IP-адрес.
Destination	Это поле показывает IP-адрес и порт назначения для каждой активной сессии. При просмотре отчетов, для которых в поле View выбрано значение «**sessions by destination IP**», можно использовать клавиши **+** или **–** для отображения или сокрытия подробной информации о сессиях, у которых в качестве IP-адреса назначения указан данный IP-адрес.
Rx	Это поле показывает объем информации, полученной источником в ходе активной сессии.
Tx	Это поле показывает объем информации, переданной источником в ходе активной сессии.
Duration	Это поле показывает длительность активной сессии в секундах.

5.7 Экран IP/MAC Binding Monitor

Чтобы открыть следующий экран, выберите в меню **Monitor > System Status > IP/MAC Binding**. Этот экран показывает список устройств, которые получили IP-адреса от интерфейсов устройства NXC со включенной привязкой IP/MAC и которые когда-либо устанавливали сессию с устройством NXC. Устройства, которые никогда не устанавливали сессию с устройством NXC, не попадают в отображаемый список.

Рисунок 29 Экран Monitor > System Status > IP/MAC Binding



Поля экрана описаны в следующей таблице.

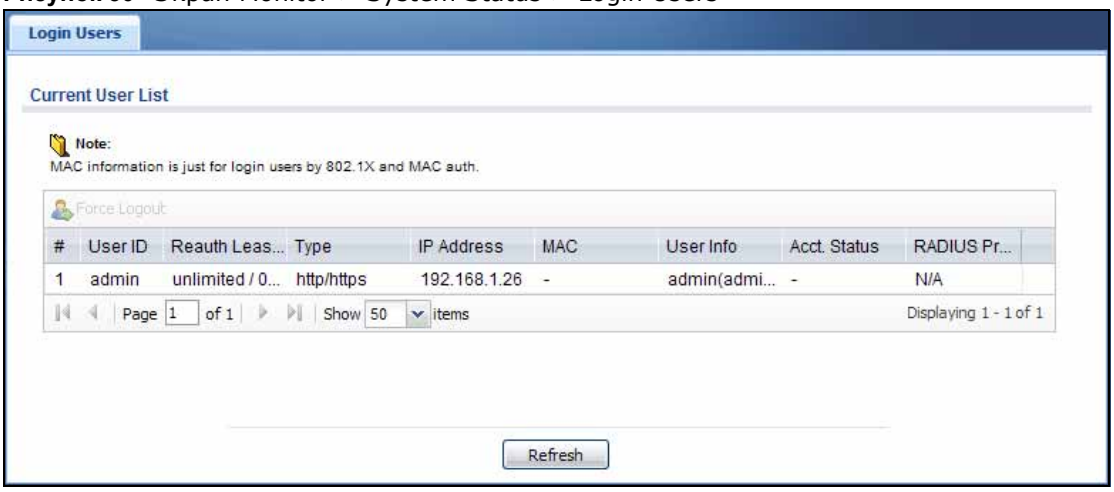
Таблица 30 Экран Monitor > System Status > IP/MAC Binding

ПОЛЕ	ОПИСАНИЕ
Interface	Выберите интерфейс устройства NXC, для которого включена привязка IP/MAC, чтобы вывести на экран список устройств, которым через данный интерфейс был назначен IP-адрес.
#	В этом поле отображается порядковый номер записи привязки IP/MAC.
IP Address	Это поле показывает IP-адрес, который устройство NXC назначило данному устройству.
Host Name	В этом поле отображается имя, используемое для идентификации устройства в сети (имя компьютера). Устройство NXC получает эти имена из запросов DHCP-клиентов.
MAC Address	Это поле показывает MAC-адрес, которому в данный момент назначен данный IP-адрес.
Last Access	Это поле показывает время начала последней сессии с устройством NXC через этот интерфейс.
Description	В этом поле содержится имя-описание, которое помогает идентифицировать запись.
Refresh	Нажмите эту кнопку, чтобы обновить информацию на экране.

5.8 Экран Login Users

На этом экране можно увидеть список пользователей, выполнивших в данный момент вход на устройство NXC. Чтобы открыть этот экран, выберите в меню **Monitor > System Status > Login Users**.

Рисунок 30 Экран Monitor > System Status > Login Users



Поля экрана описаны в следующей таблице.

Таблица 31 Экран Monitor > System Status > Login Users

ПОЛЕ	ОПИСАНИЕ
Force Logout	Выберите идентификатор пользователя и нажмите на пиктограмме, чтобы завершить сессию пользователя.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
User ID	В этом поле отображается имя каждого пользователя, выполнившего в данный момент вход на устройство NXC.
Reauth Lease T.	В этом поле отображается время, оставшееся до повторной аутентификации, и время окончания аренды, оставшееся для каждого пользователя. См. гл. 17 на стр. 208.
Type	В этом поле отображается способ, с помощью которого пользователь выполнил вход на устройство NXC.
IP address	В этом поле отображается IP-адрес компьютера, с которого осуществлен вход на устройство NXC.
MAC	При входе в систему с использованием аутентификации IEEE 802.1x или аутентификации по MAC-адресу в этом поле отображается MAC-адрес компьютера пользователя. При других типах входа в систему в поле содержится значение А «-».
User Info	Это поле показывает типы учетных записей пользователей, которые использует устройство NXC. Для типа пользователя **ext-user** (внешний пользователь) в этом поле будет показана информация о его внешней группе при наведении курсора мыши. Если внешнему пользователю соответствуют два объекта внешних групп, то в этом поле будут показаны имена обоих объектов.
Acct. Status	При входе в систему через непокидаемый портал это поле показывает состояние учета для учетной записи пользователя, под именем которого был выполнен вход на устройство NXC. Значение «**Accounting-on**» означает, что для данной учетной записи ведется учет. Значение «**Accounting-off**» означает, что учет для данной учетной записи остановлен. Значение «**-**» означает, что функция учета для данной учетной записи отключена.

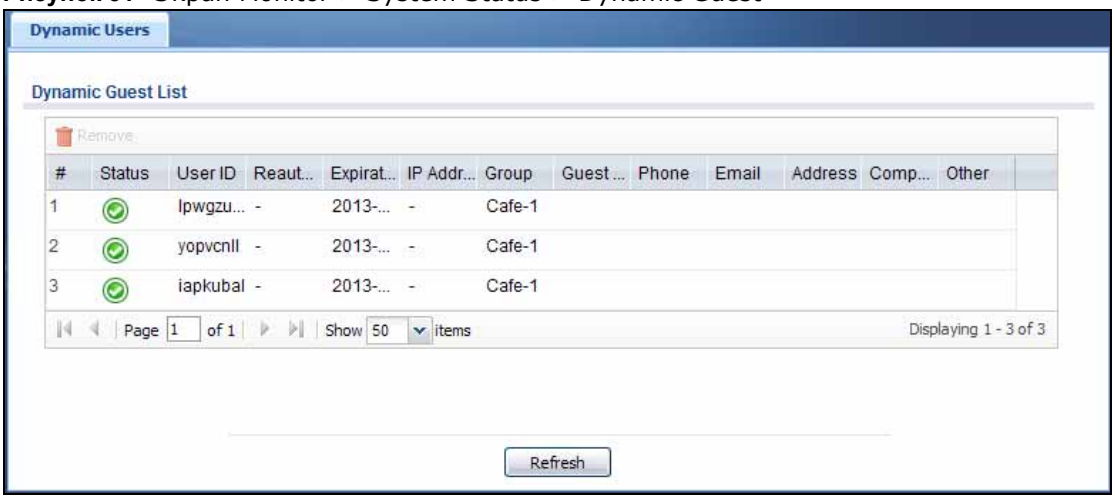
Таблица 31 Экран Monitor > System Status > Login Users

ПОЛЕ	ОПИСАНИЕ
RADIUS Profile Name	Это поле отображает название профиля RADIUS, используемого для аутентификации пользователей при входе на устройство через непокидаемый портал. Значение «**N/A**» отображается для тех учетных записей, которые не использовали непокидаемый портал и аутентификацию с использованием сервера RADIUS при входе в систему.
Refresh	Нажмите эту кнопку, чтобы обновить информацию на экране.

5.9 Экран Dynamic Guest

Для динамических гостевых учетных записей в динамическом режиме создаются имя пользователя и пароль, при помощи которых пользователь-гость может пользоваться Интернетом или службами устройства NXC в течение определенного периода времени. Для гостевых пользователей можно одновременно автоматически сгенерировать несколько динамических гостевых учетных записей с помощью Web-конфигуратора и учетной записи администратора гостей. Пользователи-гости могут подключаться к сети с определенным идентификатором (SSID) под динамическими учетными записями на ограниченное время. На этом экране можно увидеть список динамических гостевых учетных записей, хранящихся в локальной базе данных устройства NXC. Чтобы открыть этот экран, выберите в меню **Monitor > System Status > Dynamic Guest**.

Рисунок 31 Экран Monitor > System Status > Dynamic Guest



Поля экрана описаны в следующей таблице.

Таблица 32 Экран Monitor > System Status > Dynamic Guest

ПОЛЕ	ОПИСАНИЕ
Remove	Выберите соответствующую запись и нажмите эту кнопку, чтобы удалить ее из списка. Примечание: При удалении из списка действующей учетной записи пользователя, под которой в данный момент идет работа, устройство NXC завершает пользовательскую сессию.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
Status	Это поле показывает, ограничен ли срок действия данной учетной записи или нет.

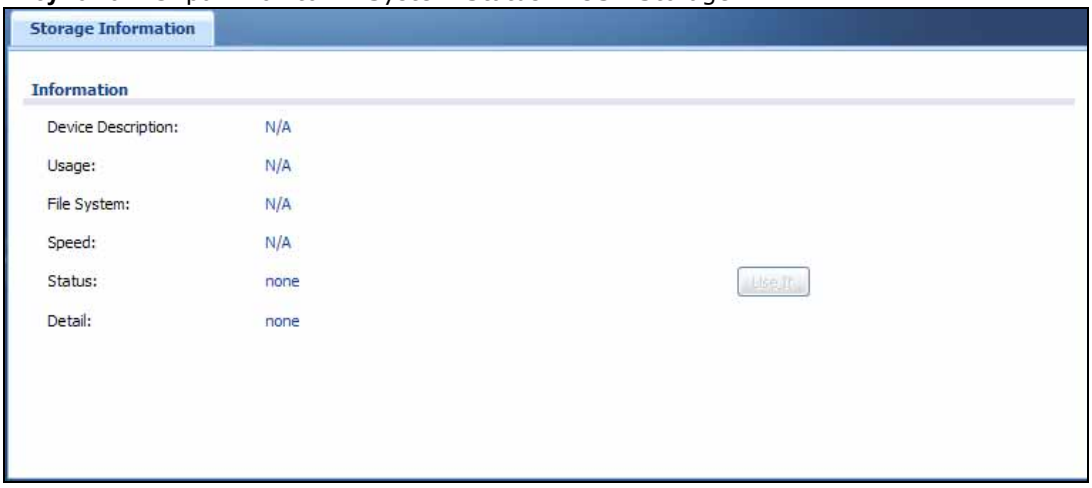
Таблица 32 Экран Monitor > System Status > Dynamic Guest

ПОЛЕ	ОПИСАНИЕ
User ID	Это поле показывает имя пользователя для данной учетной записи.
Reauth Lease T.	В этом поле отображается время, оставшееся до повторной аутентификации, и время окончания аренды, оставшееся для каждого пользователя. См. гл. 17 на стр. 208.
Expiration Time	Это поле отображает дату и время окончания срока действия пользовательской учетной записи.
IP address	В этом поле отображается IP-адрес компьютера, с которого осуществлен вход на устройство NXC.
Group	Это поле отображает название группы динамических гостевых учетных записей, к которой принадлежит данная учетная запись.
Guest Name	Это поле отображает имя человека, который использует данную учетную запись.
Phone	Это поле показывает номер телефона для данной учетной записи.
Email	Это поле показывает адрес электронной почты для данной учетной записи.
Address	Это поле показывает географический адрес для данной учетной записи.
Компания	Это поле показывает имя компании для данной учетной записи.
Other	В этом поле отображается дополнительная информация для данной учетной записи.
Refresh	Нажмите эту кнопку, чтобы обновить информацию на экране.

5.10 Экран USB Storage

На этом экране отображается информация о подключенном USB-накопителе. Чтобы открыть этот экран, выберите в меню **Monitor > System Status > USB Storage**.

Рисунок 32 Экран Monitor > System Status > USB Storage



Поля экрана описаны в следующей таблице.

Таблица 33 Экран Monitor > System Status > USB Storage

ПОЛЕ	ОПИСАНИЕ
Device description	Поле содержит краткое описание типа USB-устройства.
Usage	Это поле показывает, какая часть совокупной емкости USB-накопителя задействована в настоящий момент (в абсолютных единицах и в процентах).

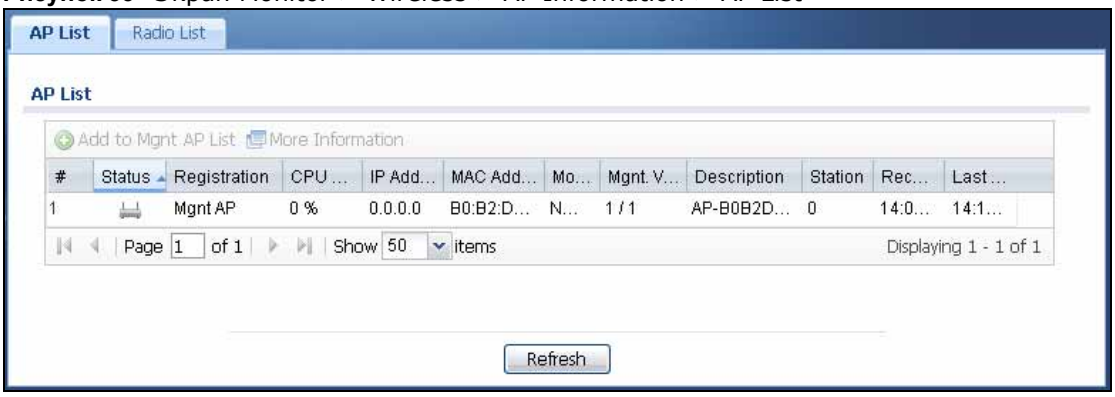
Таблица 33 Экран Monitor > System Status > USB Storage (продолжение)

ПОЛЕ	ОПИСАНИЕ
File System	Это поле показывает тип файловой системы, под которую отформатирован USB-накопитель. Если файловая система USB-накопителя не поддерживается устройством NXC, например, NTFS, то в этом поле отображается значение «Unknown».
Speed	Это поле показывает скорость соединения, которую поддерживает USB-накопитель.
Status	**Ready** – устройство NXC может работать с USB-накопителем. Нажмите кнопку **Remove Now**, чтобы остановить работу устройства NXC с USB-накопителем с тем, чтобы его можно было отключить. **Unused** – подключенный USB-накопитель был демонтирован вручную с использованием кнопки **Remove Now**, либо устройство NXC по каким-то причинам не может его смонтировать. Нажмите кнопку **Use It**, чтобы смонтировать подключенный USB-накопитель на устройстве NXC. Если устройство NXC не поддерживает файловую систему USB-накопителя (Unknown), то эта кнопка будет недоступна и окрашена в серый цвет. **none** – к устройству не подключены USB-накопители.
Detail	Это поле отображает любую дополнительную информацию, которую устройству NXC удается получить о USB-накопителе. **Deactivated** – возможность использования USB-накопителей на устройстве NXC отключена. **OutofSpace** – доступное дисковое пространство меньше заданного порога переполнения диска (информацию о настройке порога переполнения диска можно найти здесь разд. 28.3 на стр. 313). **Mounting** – устройство NXC в данный момент монтирует USB-накопитель. **Removing** – устройство NXC в данный момент демонтирует USB-накопитель. **none** – USB-накопитель работает в нормальном режиме или не подключен.

5.11 Экран AP List

На этом экране можно увидеть, какие точки доступа в настоящий момент подключены к устройству NXC. Чтобы открыть этот экран, выберите в меню **Monitor > Wireless > AP Information > AP List**.

Рисунок 33 Экран Monitor > Wireless > AP Information > AP List



Поля экрана описаны в следующей таблице.

Таблица 34 Экран Monitor > Wireless > AP Information > AP List

ПОЛЕ	ОПИСАНИЕ
Add to Mgnt AP List	Нажмите эту кнопку, чтобы добавить выбранную точку доступа в список управляемых точек доступа.
More Information	Нажмите эту кнопку, чтобы увидеть количество станций, которые подключились к выбранной точке доступа в течение суток. Данный счетчик показывает активность станций за непрерывный 24-часовой период.
#	В этом поле показан последовательный номер точки доступа в списке.
Status	Это поле визуально отображает состояние подключения точки доступа с помощью пиктограмм. Более подробно возможные варианты состояний для поля **Status** описаны в следующей таблице.
Registration	Это поле показывает, зарегистрирована ли данная точка доступа в списке управляемых точек доступа.
CPU Usage	В этом поле отображается доля (в процентах) вычислительной процессорной мощности точки доступа, которая используется в настоящее время.
IP Address	В этом поле отображается IP-адрес точки доступа.
MAC Address	В этом поле отображается MAC-адрес точки доступа.
Model	В этом поле отображается номер модели точки доступа.
Mgnt. VLAN ID(AC/AP)	В этом поле отображаются значение идентификатора сети VLAN управления для данной точки доступа, установленное на контроллере доступа (устройства NXC), и значение идентификатора сети VLAN управления в режиме выполнения, установленное на данной точке доступа. Это поле принимает значение **VLAN Conflict**, если идентификатор сети VLAN управления точки доступа не совпадает с идентификатором сети VLAN управления, установленным на устройстве NXCдля данной точки доступа. В этом поле отображается значение **n/a**, если устройство NXC не может получить информацию о сети VLAN от точки доступа.
Description	Это поле содержит описание, ассоциированное с данной точкой доступа. Описание по умолчанию выглядит так: «AP-» плюс MAC-адрес точки доступа.
Station	В этом поле отображается количество станций (или беспроводных клиентов), ассоциированных с данной точкой доступа.
Recent On-line Time	Это поле показывает, когда точка доступа в последний раз подключалась к сети. Значение **N/A** означает, что точка доступа не подключалась к сети с момента последнего запуска устройства NXC.
Last Off-line Time	Это поле показывает, когда точка доступа в последний раз отключалась от сети. Значение **N/A** означает, что точка доступа либо ни разу не подключалась к сети, либо ни разу не отключалась от сети с момента последнего запуска устройства NXC.

В таблице ниже описаны пиктограммы, которые могут присутствовать на этом экране.

Таблица 35 Значки на экране Monitor > Wireless > AP Information > AP List

ПОЛЕ	ОПИСАНИЕ
	Данная точка доступа отсутствует в списке управляемых точек доступа.
	Данная точка доступа присутствует в списке управляемых точек доступа и подключена к сети.
	Данная точка доступа находится в процессе обновления встроенного программного обеспечения.

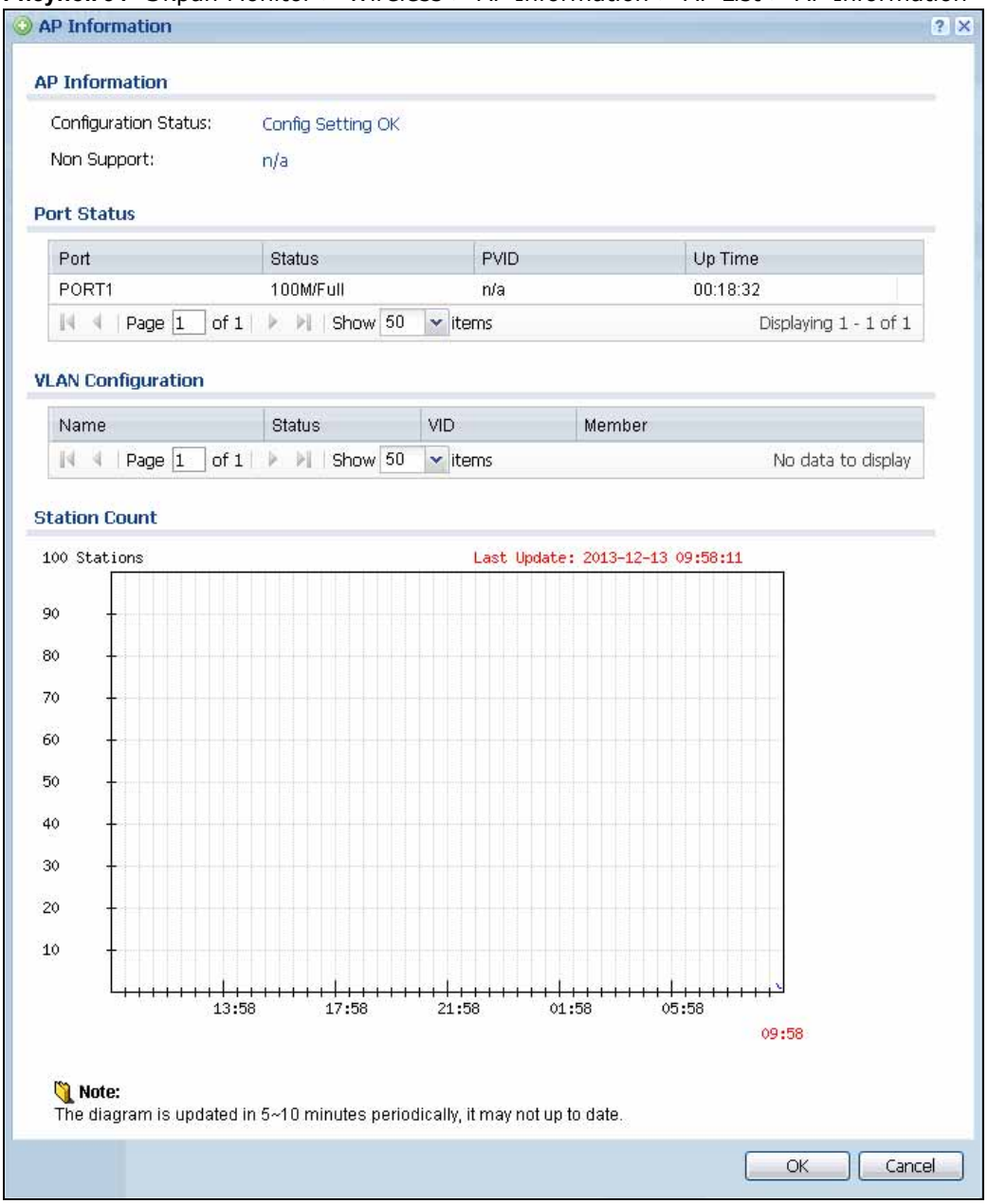
Таблица 35 Значки на экране Monitor > Wireless > AP Information > AP List (продолжение)

ПОЛЕ	ОПИСАНИЕ
	Данная точка доступа присутствует в списке управляемых точек доступа, но отключена к сети.
	Это возможно в одном из следующих случаев: • Идентификатор сети VLAN управления, установленный на этой точке доступа, конфликтует с идентификатором сети VLAN управления, установленным на контроллере доступа (устройстве NXC). • Параметр, установленный для данной точки доступа на устройстве NXC, не соответствует функциональным характеристикам точки доступа. • Пакеты, направляемые на порт локальной сети этой точки доступа, возвращаются через обратную петлю на точку доступа.

5.11.1 Экран Station Count of AP

Этот экран показывает сведения о конфигурации, состоянии портов и статистике станций для подключенных точек доступа. Чтобы открыть этот экран, выберите нужную запись и нажмите кнопку **More Information** на экране **AP List**.

Рисунок 34 Экран Monitor > Wireless > AP Information > AP List > AP Information



Поля экрана описаны в следующей таблице.

Таблица 36 Экран Monitor > Wireless > AP Information > AP List > AP Information

ПОЛЕ	ОПИСАНИЕ
Configuration Status	Это поле указывает на то, вступает ли конфигурация какой-либо из точек доступа в конфликт с параметрами, установленными на устройстве NXC'для данной точки доступа.
Non Support	Если конфигурация какой-либо из точек доступа вступает в конфликт с настройками устройства NXC, то в этом поле отображается информация об этой конфигурации. Значение **n/a** говорит о том, что никаких конфликтов между конфигурациями точек доступа и параметрами устройства NXC, установленными для точек доступа, нет.
Port Status	

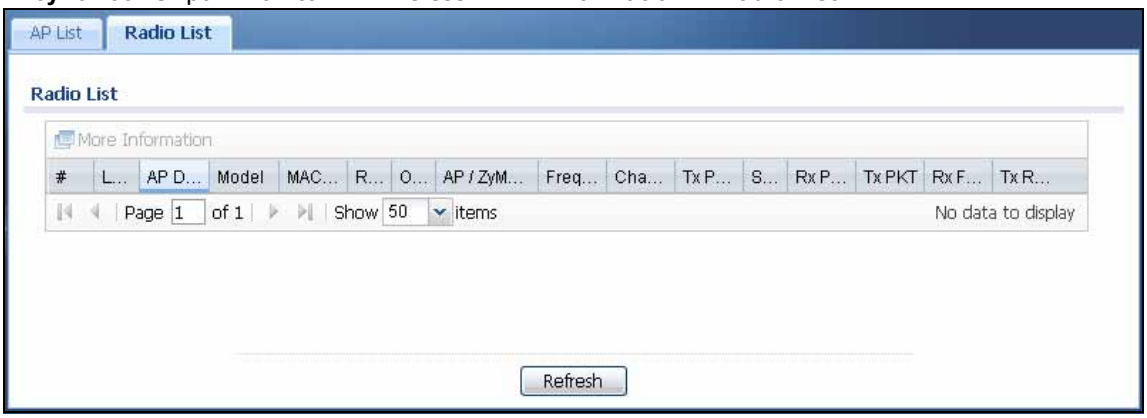
Таблица 36 Экран Monitor > Wireless > AP Information > AP List > AP Information

ПОЛЕ	ОПИСАНИЕ
Port	Это поле показывает имя физического порта Ethernet на устройстве NXC.
Status	Это поле отображает текущее состояние каждого физического порта на точке доступа. **Down** – На порту нет подключения. **Speed / Duplex** – На порту есть подключение. В этом поле отображается скорость порта и настройки дуплексного режима (**Full или Half** – дуплекс или полудуплекс).
PVID	Это поле показывает кадр приоритета (PVID) порта. PVID (идентификатор сети VLAN порта) – это тег, которым помечаются входящие кадры без тегов, принимаемые портом, с тем, чтобы потом перенаправить эти кадры в группу VLAN, которую определяет данный тег.
Up Time	Это поле показывает длительность подключения, установленного на данном физическом порту.
VLAN Configuration	
Name	Это поле показывает имя сети VLAN.
Status	В этом поле отображается состояние сети VLAN: активирована или нет.
VID	Это поле показывает идентификатор сети VLAN.
Member	Это поле содержит список портов Ethernet, входящих в данную сеть VLAN.
Station Count	На оси y показано количество подключенных станций.
Time	На оси x показано время с момента подключения каждой станции.
Last Update	В этом поле показаны дата и время последнего обновления информации в окне.

5.12 Экран Radio List

С помощью этого экрана можно ознакомиться со статистикой по беспроводным радиопередатчикам, установленным на каждой из точек доступа, подключенных к устройству NXC. Чтобы открыть этот экран, выберите в меню **Monitor > Wireless > AP Information > Radio List**.

Рисунок 35 Экран Monitor > Wireless > AP Information > Radio List



Поля экрана описаны в следующей таблице.

Таблица 37 Экран Monitor > Wireless > AP Information > Radio List

ПОЛЕ	ОПИСАНИЕ
More Information	Нажмите эту кнопку, чтобы просмотреть дополнительную информацию об идентификаторах сетей выбранных радиомодулей, объемах беспроводного трафика и беспроводных клиентах. Информация охватывает интервал продолжительностью 24 часа.
#	В этом поле указан последовательный номер радиомодуля в списке.
Loading	Это поле указывает на состояние балансировки нагрузки точки доступа (**UnderLoad** [«недогрузка»] или **OverLoad** [«перегрузка»]), если на данной точке доступа включен режим балансировки нагрузки. Значение «**-**» свидетельствует о том, что режим балансировки нагрузки выключен, либо радиомодуль находится в режиме мониторинга.
AP Description	Это поле содержит описание точки доступа, к которой принадлежит данный радиомодуль.
Model	Это поле отображает название модели точки доступа, к которой принадлежит радиомодуль.
MAC Address	Это поле показывает MAC-адрес радиомодуля.
Radio	Это поле отображает номер радиомодуля на точке доступа, к которой он принадлежит.
OP Mode	Это поле показывает режим работы радиомодуля. Возможные режимы работы: **AP** (точка доступа), **MON** (мониторинг), **Root AP** (корневая точка доступа) или **Repeater** (повторитель).
AP / ZyMesh Profile	Это поле показывает имена профилей радиомодуля и ZyMesh точки доступа, к которой принадлежит данный радиомодуль.
Frequency Band	Это поле показывает, какую радиочастоту использует в настоящий момент данный радиомодуль. Значение «**-**» означает, что радиомодуль работает в режиме мониторинга.
Channel ID	Это поле показывает идентификатор канала радиомодуля.
Tx Power	Это поле показывает выходную мощность радиомодуля (в дБм).
Station	В этом поле отображается количество станций (или беспроводных клиентов), ассоциированных с данным радиомодулем.
Rx PKT	Это поле показывает общее количество пакетов, принятых радиомодулем.
Tx PKT	Это поле показывает общее количество пакетов, отправленных радиомодулем.
Rx FCS Error Count	Это поле показывает число накопленных радиомодулем ошибок, связанных с полученными пакетами.
Tx Retry Count	Это поле показывает, сколько раз радиомодуль совершал попытку повторной отправки пакетов.

В таблице ниже описаны пиктограммы, которые могут присутствовать на этом экране.

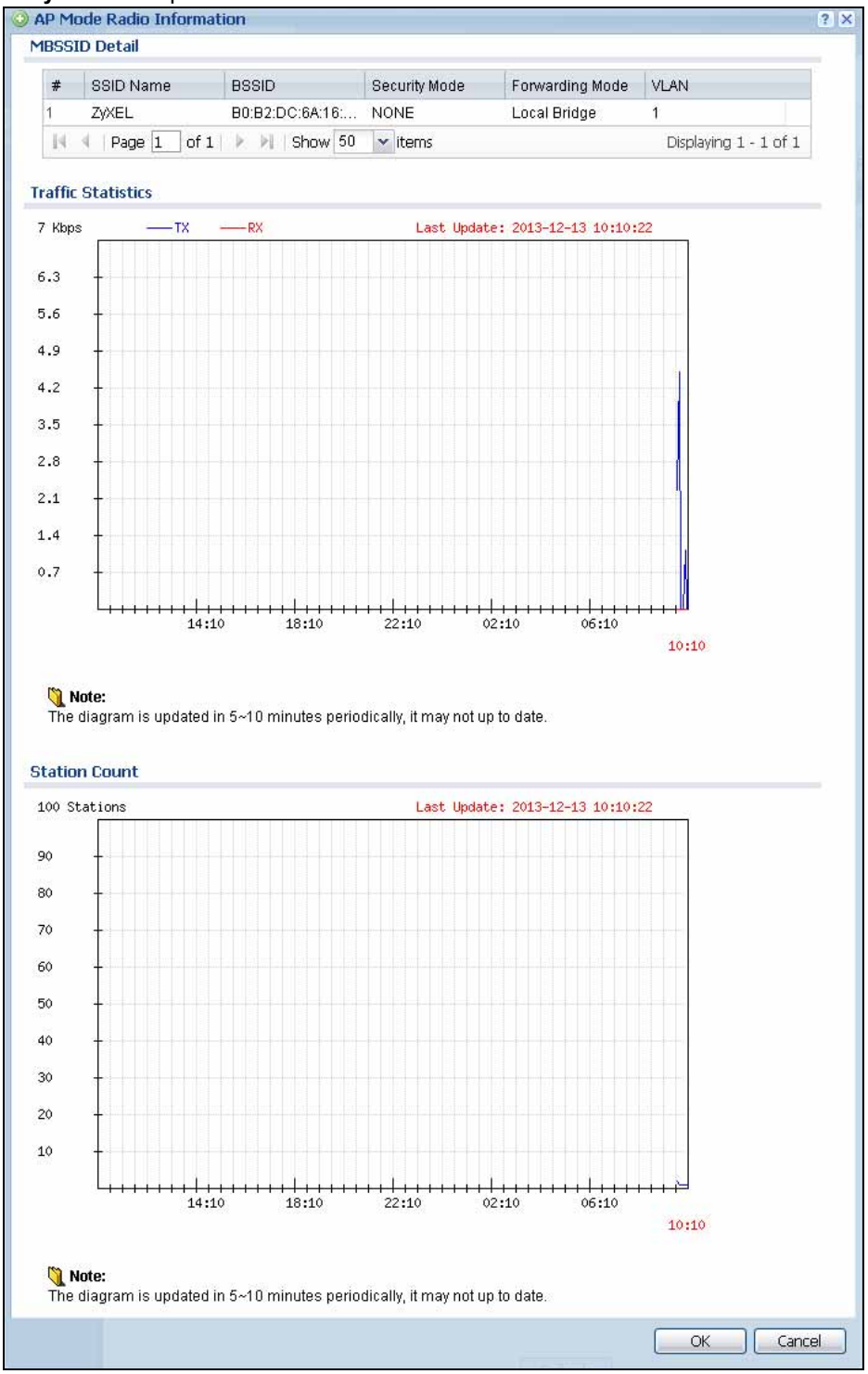
Таблица 38 Значки экрана Monitor > Wireless > AP Information > Radio List

ПОЛЕ	ОПИСАНИЕ
	Если точка доступа работает в режиме балансировки нагрузки, то эта пиктограмма указывает на то, что она работает с превышением максимальной выделенной полосы пропускания.
	Если точка доступа работает в режиме балансировки нагрузки, то эта пиктограмма указывает на то, что она не задействует максимальную выделенную полосу пропускания.

5.12.1 Экран AP Mode Radio Information

На этом экране можно познакомиться с подробной информацией об идентификаторах сетей, объемах беспроводного трафика и беспроводных клиентах, подключавшихся к данному радиомодулю за последние 24 часа.Чтобы открыть это окно, выберите нужную запись и нажмите кнопку **More Information** на экране **Radio List**.

Рисунок 36 Экран Monitor > Wireless > AP Information > Radio List > AP Mode Radio Information



Поля экрана описаны в следующей таблице.

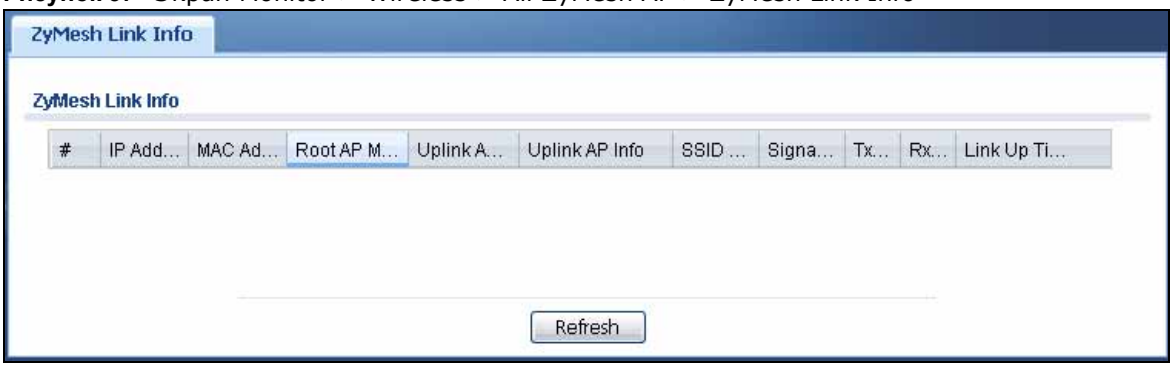
Таблица 39 Экран Monitor > Wireless > AP Info > Radio List > AP Mode Radio Information

ПОЛЕ	ОПИСАНИЕ
MBSSID Detail	Этот список содержит перечень идентификаторов сетей, которые были ассоциированы с данным радиомодулем за последние 24 часа.
#	В этом поле показана позиция записи в списке. Она не имеет никакой связи с реальными данными из списка.
SSID Name	Это поле содержит идентификатор сети, ассоциированной с данным радиомодулем. Длина значения не может превышать восьми символов.
BSSID	Это поле показывает MAC-адрес, ассоциированный с данным идентификатором сети.
Security Mode	Это поле указывает на режим безопасности, в котором работает сеть с данным идентификатором.
Forwarding Mode	Это поле показывает режим пересылки (локальный мост **Local Bridge** или туннель **Tunnel**), ассоциированный с данным профилем SSID.
VLAN	Это поле показывает идентификатор VLAN, ассоциированный с данным идентификатором сети.
Traffic Statistics	Этот график содержит общую информацию о трафике данного радиомодуля за последние 24 часа.
y-axis	На этой оси показан объем данных, прошедших через этот радиомодуль (в мегабайтах в секунду).
x-axis	На этой оси показан временной интервал, в течение которого данные проходили через радиомодуль.
Station Count	Этот график показывает информацию обо всех беспроводных клиентах, которые подключались к данному радиомодулю за последние 24 часа.
y-axis	На оси y показано количество подключавшихся беспроводных клиентов.
x-axis	На оси x показан интервал времени, в течение которого был подключен данный беспроводной клиент.
Last Update	В этом поле показаны дата и время последнего обновления информации в окне.
OK	Нажмите на эту кнопку, чтобы закрыть окно.
Cancel	Нажмите на эту кнопку, чтобы закрыть окно.

5.13 Экран ZyMesh Link Info

Этот экран показывает статистику трафика ZyMesh/WDS между управляемыми точками доступа. Выберите в меню **Monitor > Wireless > All ZyMesh AP > ZyMesh Link Info**, чтобы открыть этот экран.

Рисунок 37 Экран Monitor > Wireless > All ZyMesh AP > ZyMesh Link Info



Поля экрана описаны в следующей таблице.

Таблица 40 Экран Monitor > Wireless > All ZyMesh AP > ZyMesh Link Info

ПОЛЕ	ОПИСАНИЕ
#	В этом поле показан последовательный номер управляемой точки доступа в списке.
IP Address	Это поле показывает IP-адрес управляемой точки доступа.
MAC Address	Это поле показывает MAC-адрес управляемой точки доступа.
Root AP MAC	Это поле показывает MAC-адрес корневой точки доступа, к которой управляемая точка доступа подключена по беспроводному каналу.
Uplink AP Role	Это поле указывает на то, выступает ли управляемая точка доступа, к которой данная управляемая точка доступа подключена по беспроводному каналу, в качестве корневой точки доступа или повторителя в структуре ZyMesh.
Uplink AP Info	Это поле содержит информацию об управляемой точке доступа, к которой данная управляемая точка доступа подключена по беспроводному каналу.
SSID Name	Это поле показывает идентификатор беспроводной сети (SSID), который данная управляемая точка доступа использует для ассоциации с другими управляемыми точками доступа.
Signal Strength	Это поле показывает силу радиосигнала в беспроводном канале между этой управляемой точкой доступа и корневой точкой доступа или повторителем.
Tx Rate	Это поле показывает максимальную скорость передачи корневой точки доступа или повторителя, к которому подключена данная управляемая точка доступа.
Rx Rate	Это поле показывает максимальную скорость приема корневой точки доступа или повторителя, к которому подключена данная управляемая точка доступа.
Link Up Time	Это поле показывает момент времени, в который эта управляемая точка доступа первый раз установила связь (ассоциировалась) с корневой точкой доступа или повторителем.

5.14 Экран Station List

На этом экране можно ознакомиться со статистикой по ассоциированным станциям (или «беспроводным клиентам»). Чтобы открыть этот экран, выберите в меню **Monitor > Wireless > Station Info > Station List**.

Рисунок 38 Экран Monitor > Wireless > Station Info > Station List

Поля экрана описаны в следующей таблице.

Таблица 41 Экран Monitor > Wireless > Station Info > Station List

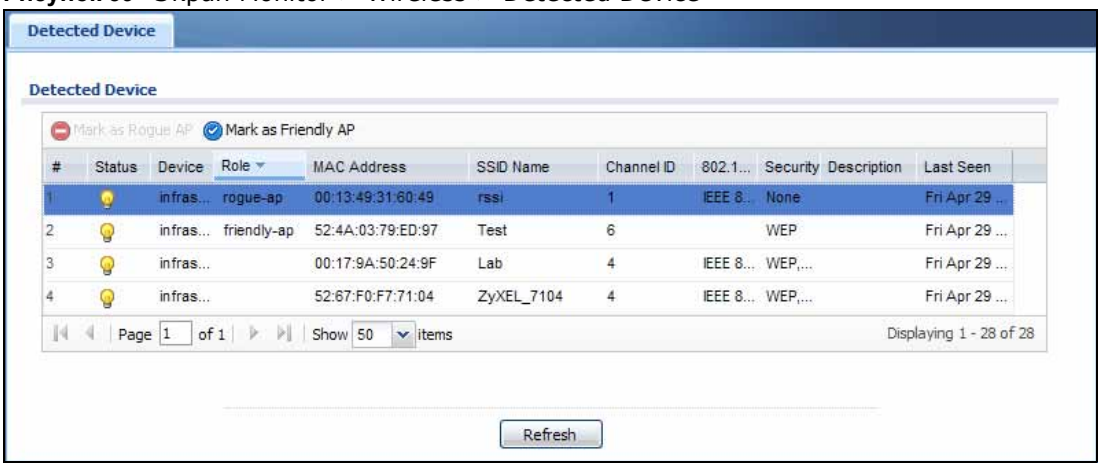
ПОЛЕ	ОПИСАНИЕ
SSID Name	Это поле показывает имя сети, с которой ассоциирована хотя бы одна станция. Воспользуйтесь клавишами + или -, чтобы скрыть или показать дополнительные сведения о беспроводных станциях, подключенных к сети.
#	Это поле показывает последовательный номер станции в списке.
MAC Address	Это поле содержит MAC-адрес станции.
Associated AP	Это поле указывает на точку доступа, через которую данная станция подключается к сети.
SSID Name	Это поле показывает имя беспроводной сети, к которой подключена станция. Одной точке доступа может соответствовать несколько идентификаторов SSID (или сетей).
Security Mode	Это поле описывает методы шифрования, которые использует станция при подключении к сети.
Signal Strength	Это поле отображает силу сигнала. Сила сигнала зависит в первую очередь от выходной мощности и расстояния между станцией и точкой доступа.
Channel	Это поле показывает номер канала, используемого станцией для подключения к сети.
IP Address	Это поле содержит IP-адрес станции. IP-адрес вида 169.x.x.x IP является локальным, это означает, что станция не получила IP-адрес с DHCP-сервера.
Tx Rate	Это поле показывает текущую скорость передачи данных станции.
Rx Rate	Это поле показывает текущую скорость получения данных станции.
Tx	Это поле показывает количество пакетов, переданных станцией.
Rx	Это поле показывает количество пакетов, полученных станцией.
Association Time	Это поле показывает момент времени, в который беспроводная станция впервые подключилась (ассоциировалась) к данной точке доступа.
Refresh	Нажмите эту кнопку, чтобы обновить информацию на странице.

5.15 Экран Detected Device

С помощью этого экрана можно просмотреть информацию о беспроводных устройствах, обнаруженных данной точкой доступа. Чтобы перейти к этому экрану, выберите в меню **Monitor > Wireless > Detected Device**.

Примечание: Как минимум один из радиомодулей точек доступа, подключенных к устройству NXC, должен быть переведен в режим мониторинга (это делается на экране **Configuration > Wireless > AP Management**) с целью обнаружения других беспроводных устройств, находящихся поблизости.

Рисунок 39 Экран Monitor > Wireless > Detected Device



Поля экрана описаны в следующей таблице.

Таблица 42 Экран Monitor > Wireless > Rogue AP > Detected Device

ПОЛЕ	ОПИСАНИЕ
Mark as Rogue AP	Нажмите эту кнопку, чтобы отметить выбранную точку доступа как мошенническую. Сведения о мошеннической точке доступа могут присутствовать на экране **Configuration > Wireless > MON Mode** (гл. 7 на стр. 99).
Mark as Friendly AP	Нажмите эту кнопку, чтобы отметить выбранную точку доступа как дружественную. Дополнительные возможности по управлению дружественными точками доступа можно найти на экране **Configuration > Wireless > MON Mode** (гл. 7 на стр. 99).
#	Это поле показывает последовательный номер станции в списке.
Status	Это поле отображает состояние обнаруженного устройства.
Device	Это поле указывает на тип сети обнаруженного устройства (например, **infrastructure** или **ad-hoc**).
Role	Это поле показывает роль обнаруженного устройства (например, «friendly» [дружественное] или «rogue» [мошенническое]).
MAC Address	Это поле показывает MAC-адрес обнаруженного устройства.
SSID Name	Это поле отображает идентификатор сети (SSID) обнаруженного устройства.
Channel ID	Это поле показывает идентификатор канала обнаруженного устройства.
802.11 Mode	Это поле указывает на тип режима 802.11 (a/b/g/n), передаваемый обнаруженным устройством.
Security	Это поле указывает на метод шифрования (если таковой имеется), используемый обнаруженным устройством.

Таблица 42 Экран Monitor > Wireless > Rogue AP > Detected Device (продолжение)

ПОЛЕ	ОПИСАНИЕ
Description	Это поле отображает описание обнаруженного устройства. Более подробную информацию об управлении дружественными и мошенническими точками доступа можно найти на экране **Configuration > Wireless > MON Mode** (гл. 7 на стр. 99).
Last Seen	Это поле показывает момент времени, когда данное устройство было в последний раз обнаружено устройством NXC.
Refresh	Нажмите эту кнопку, чтобы обновить информацию на странице.

5.16 Экран View Log

Журнальные сообщения хранятся в двух разных журналах: в один попадают обычные журнальные сообщения, в другой – отладочные сообщения. В обычном журнале можно увидеть все сообщения, выбрав опцию **All Logs**, либо просмотреть только сообщения, относящиеся к какой-то конкретной категории, например, для определенного пользователя. Выбрав опцию **Debug Log**, можно просмотреть журнал с отладочными сообщениями. Все отладочные сообщения имеют одинаковый приоритет.

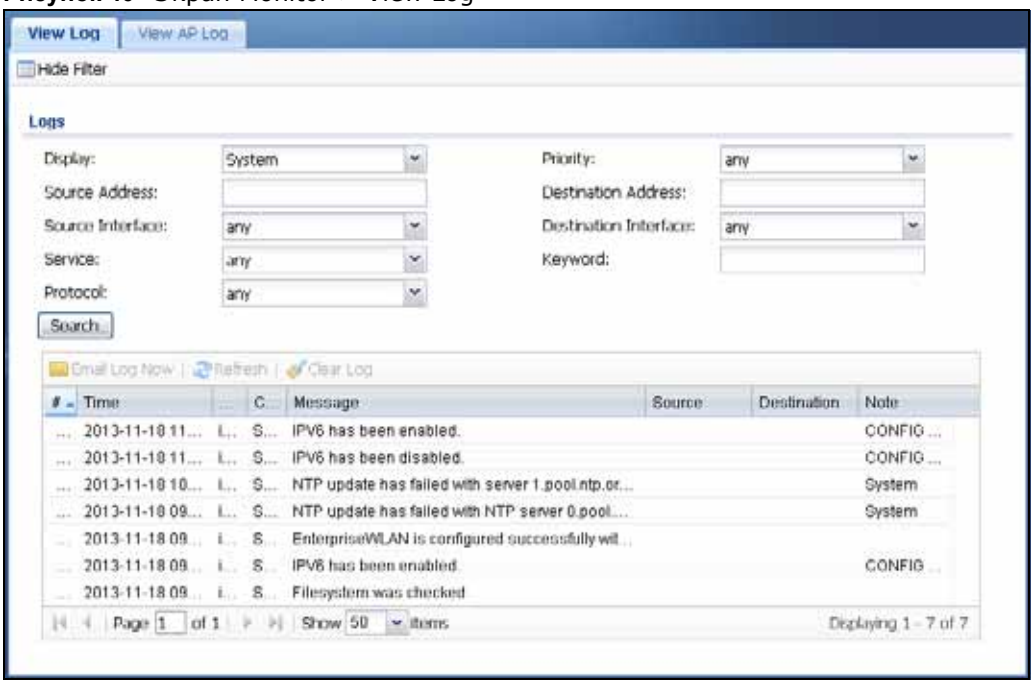
Чтобы открыть этот экран, выберите в меню **Monitor > Log**. Ниже показан вид экрана, отображающего содержимое журнала.

Примечание: При достижении максимального количества сообщений в журнале новые сообщения начинают автоматически перетирать существующие, начиная с самых старых.

- Описания конкретных журналов приведены в прил. A на стр. 417.
- Максимально допустимое количество сообщений в логах устройства NXC описано в спецификации.

События, которые генерируют оповещения или сообщения в журнале, отображаются красным. Обычные события в журналах отображаются черным цветом. Щелкните по заголовку колонки, чтобы отсортировать записи в таблице по полю, представленному этим столбцом. Чтобы поменять порядок сортировки на обратный, щелкните по заголовку столбца еще раз.

Рисунок 40 Экран Monitor > View Log



Поля экрана описаны в следующей таблице.

Таблица 43 Экран Monitor > View Log

ПОЛЕ	ОПИСАНИЕ
Show Filter / Hide Filter	Нажмите эту кнопку, чтобы показать или скрыть настройки фильтров. Если настройки фильтров скрыты, на экране будут видны поля **Display**, **Email Log Now**, **Refresh** и **Clear Log**. Если настройки фильтров показаны, на экране будут видны поля **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Service**, **Keyword**, **Protocol** и **Search**.
Display	Выберите категорию сообщений журнала(-ов), которую необходимо просмотреть. Можно просмотреть все журналы (опция **All Logs**) одновременно, либо просмотреть журнал отладки (опция **Debug Log**).
Priority	Это поле появляется на экране при показе настроек фильтра. Выберите приоритет сообщений журнала, которые необходимо вывести на экран. В журнале будут показаны сообщения с приоритетом не ниже выбранного вами. Возможные варианты: **any** (любые), **emerg** (чрезвычайная ситуация), **alert** (оповещение), **crit** (критично), **error** (ошибка), **warn** (предупреждение), **notice** (уведомление) и **info** (информационное сообщение), если двигаться от максимального приоритета к минимальному. Если выбрана категория **Debug Log**, это поле будет доступно только для чтения.
Source Address	Это поле появляется на экране при показе настроек фильтра. Введите IP-адрес источника входящего пакета, который сгенерировал сообщение в журнале. Не включайте порт в этот фильтр.
Destination Address	Это поле появляется на экране при показе настроек фильтра. Введите IP-адрес назначения входящего пакета, который сгенерировал сообщение в журнале. Не включайте порт в этот фильтр.
Source Interface	Это поле появляется на экране при показе настроек фильтра. Выберите интерфейс источника пакета, который сгенерировал сообщение в журнале.
Destination Interface	Это поле появляется на экране при показе настроек фильтра. Выберите интерфейс назначения пакета, который сгенерировал сообщение в журнале.

Таблица 43 Экран Monitor > View Log (продолжение)

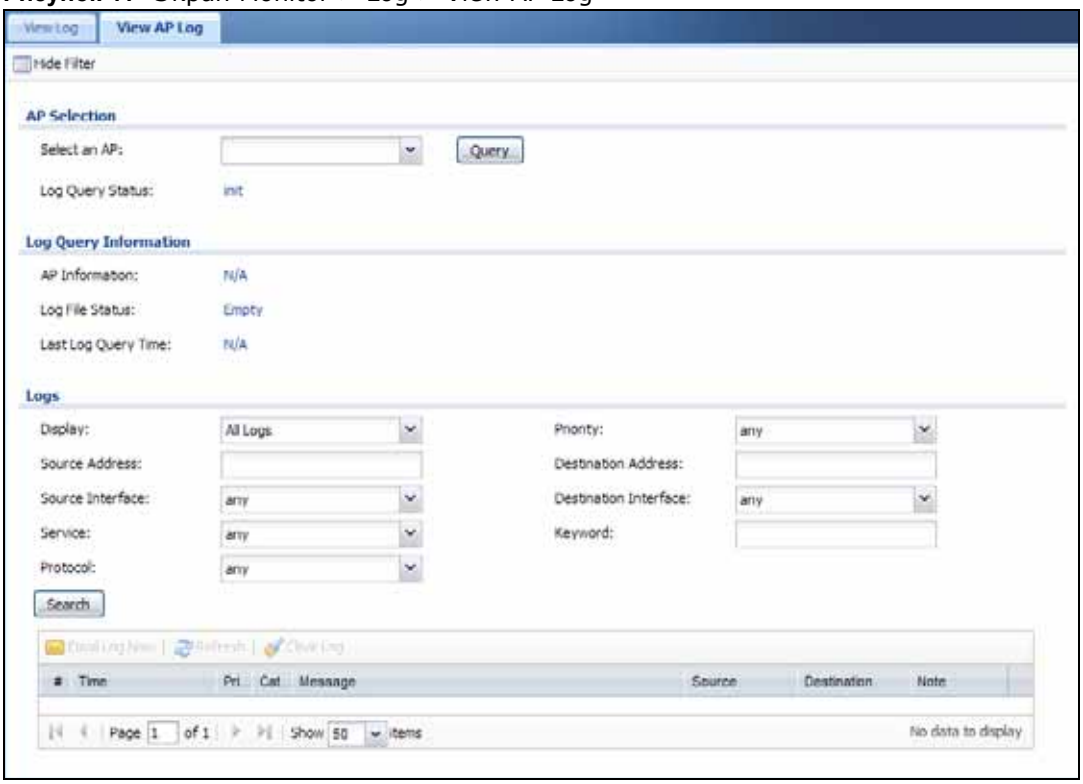
ПОЛЕ	ОПИСАНИЕ
Service	Это поле появляется на экране при показе настроек фильтра. Выберите службу, для которой необходимо посмотреть сообщения журнала. Web-конфигуратор отбирает сообщения журнала, относящиеся к данной службе, по протоколу и номеру порта назначения.
Keyword	Это поле появляется на экране при показе настроек фильтра. Введите ключевое слово, по которому будет осуществляться поиск в полях **Message**, **Source**, **Destination** и **Note**. На экран будут выведены те сообщения журнала, для которых было найдено соответствие в любом из перечисленных полей. Можно использовать алфавитно-цифровые символы (не более 63), символ подчеркивания и знаки пунктуации ()’ ,:;?! +-*/= #$% @ ; использование точки, двойных кавычек и квадратных скобок не допускается.
Protocol	Это поле появляется на экране при показе настроек фильтра. Выберите протокол службы, для которого необходимо посмотреть сообщения в журнале.
Search	Это поле появляется на экране при показе настроек фильтра. Нажмите эту кнопку, чтобы обновить вывод содержимого журнала в соответствии с текущими настройками фильтрации.
Email Log Now	Нажмите эту кнопку, чтобы отправить сообщения журнала на активные почтовые адреса, указанные в поле **Send Log To** на странице **Log Settings**.
Refresh	Нажмите эту кнопку, чтобы обновить таблицу журнала.
Clear Log	Нажмите эту кнопку, чтобы очистить журнал полностью, независимо от того, какая его часть сейчас отображается на экране.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным сообщением в журнале.
Time	Это поле отображает время записи сообщения в журнале.
Priority	Это поле показывает приоритет сообщения в журнале. Оно может принимать те же значения, что и поле **Priority**, описанное выше.
Категория	Это поле содержит название журнала, который сгенерировал сообщение. В этом поле используется то же значение, что и в полях **Display** и **Category** (другие).
Message	В этом поле отображается причина, по которой было сгенерировано сообщение в журнале. В конце значения, содержащегося в поле **Message**, добавляется фрагмент вида «[count=*x*]», где *x* – это число, если включена функция консолидации журналов, и данная запись представляет собой результат агрегации нескольких записей.
Source	В этом поле отображается IP-адрес и номер порта источника для события, которое сгенерировало сообщение в журнале.
Destination	В этом поле отображается IP-адрес и номер порта назначения для события, которое сгенерировало сообщение в журнале.
Note	В этом поле содержится любая дополнительная информация о сообщении в журнале.

Web-конфигуратор сохраняет настройки фильтров, если уйти с экрана **View Log** и вернуться к нему позже.

5.17 Экран View AP Log

С помощью этого экрана можно просмотреть текущие сообщения журнала для беспроводных точек доступа, подключенных к устройству NXC. Чтобы перейти к этому экрану, выберите в меню **Monitor > Log > View AP Log**.

Рисунок 41 Экран Monitor > Log > View AP Log



Поля экрана описаны в следующей таблице.

Таблица 44 Экран Monitor > Log > View AP Log

ПОЛЕ	ОПИСАНИЕ
Show/Hide Filter	Нажмите эту кнопку, чтобы показать или скрыть фильтр для журнала точек доступа.
Select an AP	Выберите нужную точку доступа из списка и нажмите кнопку **Query**, чтобы просмотреть сообщения из ее журнала.
Log Query Status	Это поле указывает на текущее состояние запроса на вывод сообщений из журнала. **init** – Запрос еще не инициализирован. **querying** – Запрос в процессе выполнения. **fail** – Не удалось выполнить запрос. **success** – Запрос успешно выполнен.
AP Information	Это поле показывает MAC-адрес выбранной точки доступа.
Log File Status	Это поле указывает на состояние сообщений журнала для данной точки доступа.
Last Log Query Time	Это поле показывает момент времени, когда точке доступа в последний раз был адресован запрос на вывод сообщений журнала.
Display	Выберите файл журнала, который необходимо вывести на экран для указанной точки доступа. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Priority	Выберите уровень приоритета для фильтрации отображаемых сообщений журнала. Примечание: Это критерий действует только при выбранной опции **Show Filter**.

Таблица 44 Экран Monitor > Log > View AP Log

ПОЛЕ	ОПИСАНИЕ
Source Address	Введите IP-адрес источника, чтобы отобразить только те сообщения журнала, которые его содержат. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Destination Address	Введите IP-адрес назначения, чтобы отобразить только те сообщения журнала, которые его содержат. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Source Interface	Укажите интерфейс источника, чтобы отобразить только те сообщения журнала, которые его содержат. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Destination Interface	Укажите интерфейс назначения, чтобы отобразить только те сообщения журнала, которые его содержат. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Service	Выберите тип службы, чтобы отобразить только сообщения журнала, относящиеся к данному типу. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Keyword	Введите ключевое слово, чтобы отобразить только сообщения журнала, которые его содержат. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Protocol	Выберите протокол, чтобы отобразить только сообщения журнала, имеющие отношение к данному протоколу. Примечание: Это критерий действует только при выбранной опции **Show Filter**.
Search	Нажмите эту кнопку, чтобы запустить запрос на вывод сообщений журнала в соответствии с выбранными критериями. Если никакие критерии фильтрации не указаны, в результате запроса на экран будут выведены все сообщения журнала для данной точки доступа.
Email Log Now	Нажмите эту кнопку, чтобы создать новое сообщение в почтовой программе по умолчанию, к которому будет приложен выбранный журнал.
Refresh	Нажмите эту кнопку, чтобы обновить таблицу журнала.
Clear Log	Нажмите эту кнопку, чтобы очистить журнал для указанной точки доступа.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным сообщением в журнале.
Time	Это поле показывает момент времени, в который были созданы или записаны сообщения журнала для данной точки доступа.
Priority	Это поле показывает приоритет выбранного сообщения журнала.
Категория	Это поле показывает категорию выбранного сообщения журнала.
Message	Это поле отображает содержимое выбранного сообщения журнала.
Source	Это поле отображает IP-адрес источника выбранного сообщения журнала.
Destination	Это поле отображает IP-адрес источника выбранного сообщения журнала.
Note	В этом поле содержатся любые дополнительные примечания, относящиеся к выбранному сообщению журнала.

6

Регистрация устройства

6.1 Обзор

Используйте экран **Configuration > Licensing > Registration** для регистрации устройства NXC и управления подписками на его службы.

6.1.1 О чем рассказывается в этой главе

- Экран **Registration** (разд. 6.2 на стр. 93) служит для регистрации устройства NXC на сайте myZyXEL.com.
- Экран **Service** (разд. 6.3 на стр. 96) отображает состояние регистрации служб и обновления лицензий.

6.1.2 Что необходимо знать

В этом разделе рассказывается о темах, излагаемых в этой главе.

myZyXEL.com

myZyXEL.com – это центр онлайновых служб ZyXEL, в котором можно зарегистрировать устройство NXC и управлять подписками на службы, доступные для устройства NXC. Чтобы пользоваться службой подписок, необходимо зарегистрировать устройство NXC и активировать соответствующую службу на сайте myZyXEL.com (через устройство NXC).

Примечание: Перед тем, как зарегистрировать устройство и активировать службы на сайте myZyXEL.com, необходимо создать учетную запись на сайте myZyXEL.com.

Для регистрации устройства NXC2500 можно создать учетную запись непосредственно на сайте myZyXEL.com, а затем зарегистрировать свое устройство NXC и активировать службу с помощью экрана **Registration**. В качестве альтернативы можно перейти на сайт http://www.myZyXEL.com и указать серийный номер и MAC-адрес устройства NXC в локальной сети в процессе его регистрации. Более подробную информацию можно получить в интерактивной справке на самом сайте.

Для регистрации устройства NXC5500 можно перейти на сайт http://portal.myZyXEL.com и указать в процессе регистрации серийный номер устройства NXC и его MAC-адрес в локальной сети. Более подробную информацию можно получить в интерактивной справке на самом сайте.

Примечание: Чтобы активировать службу на устройстве NXC, необходимо зайти на сайт myZyXEL.com через данное устройство NXC.

Максимальное число управляемых точек доступа

Изначальная конфигурация устройства NXC2500 предусматривает поддержку до 8 управляемых точек доступа (таких, как NWA5123-NI). Для увеличения числа поддерживаемых точек доступа можно оформить подписку на дополнительные лицензии. На момент написания этого документа каждое обновление лицензии дает право на поддержку еще 8 управляемых точек доступа, при этом одно устройство NXC в максимальной конфигурации поддерживает не более 64 точек доступа.

Изначальная конфигурация устройства NXC5500 предусматривает поддержку до 64 управляемых точек доступа (таких, как точки доступа серии NWA512x или серии NWA5301-NJ). Для увеличения числа поддерживаемых точек доступа можно оформить подписку на дополнительные лицензии. На момент написания этого документа каждое обновление лицензии дает право на поддержку еще 8 или 64 управляемых точек доступа, при этом одно устройство NXC в максимальной конфигурации поддерживает не более 512 точек доступа.

Максимальное число корневых точек доступа ZyMesh

По умолчанию устройство NXC поддерживает не более одной корневой точки доступа ZyMesh, то есть только один радиомодуль управляемой точки доступа может быть переведен в режим корневой точки доступа. Чтобы избавиться от этого ограничения, нужно оформить подписку на лицензию ZyMesh.

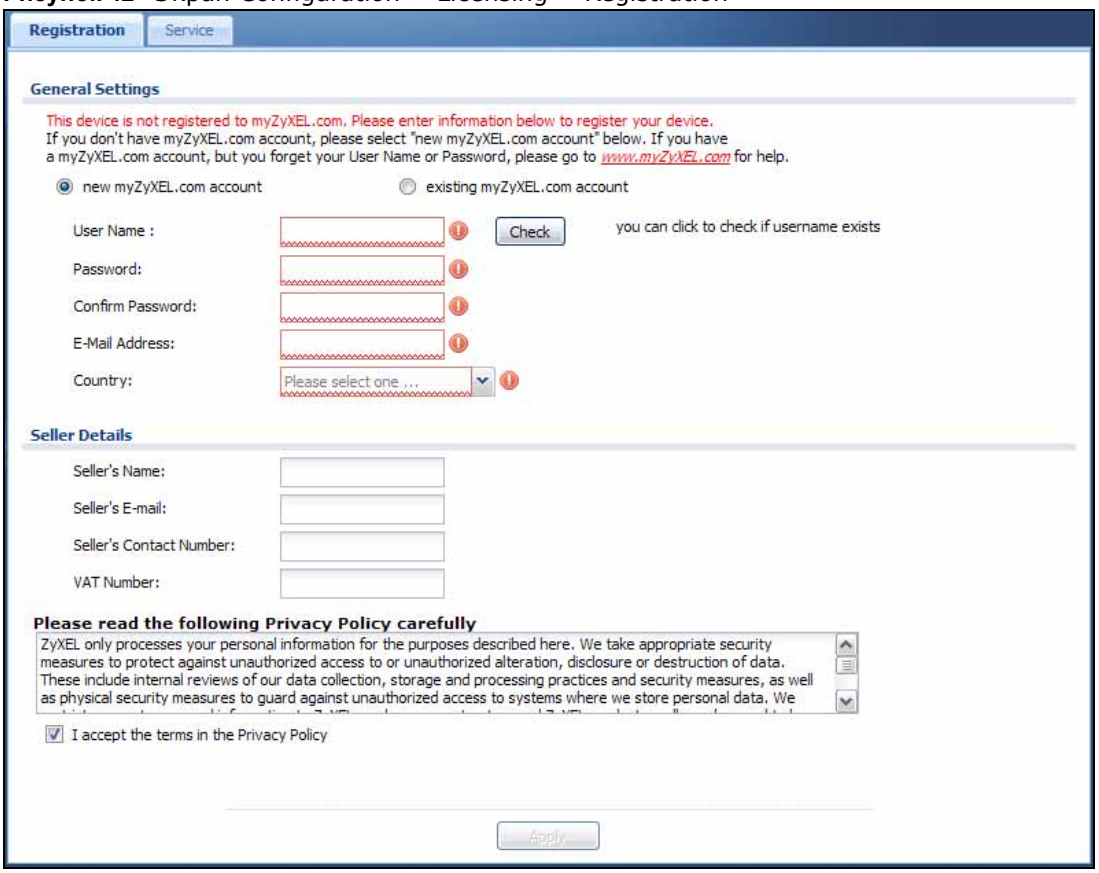
6.2 Экран Registration

Внешний вид этого экрана зависит от используемой модели устройства NXC.

6.2.1 NXC2500

С помощью этого экрана можно зарегистрировать свое устройство NXC на сайте myZyXEL.com.Чтобы открыть экран, изображенный ниже, выберите в меню навигационной панели **Configuration > Licensing > Registration**.

Рисунок 42 Экран Configuration > Licensing > Registration



Поля экрана описаны в следующей таблице.

Таблица 45 Экран Configuration > Licensing > Registration

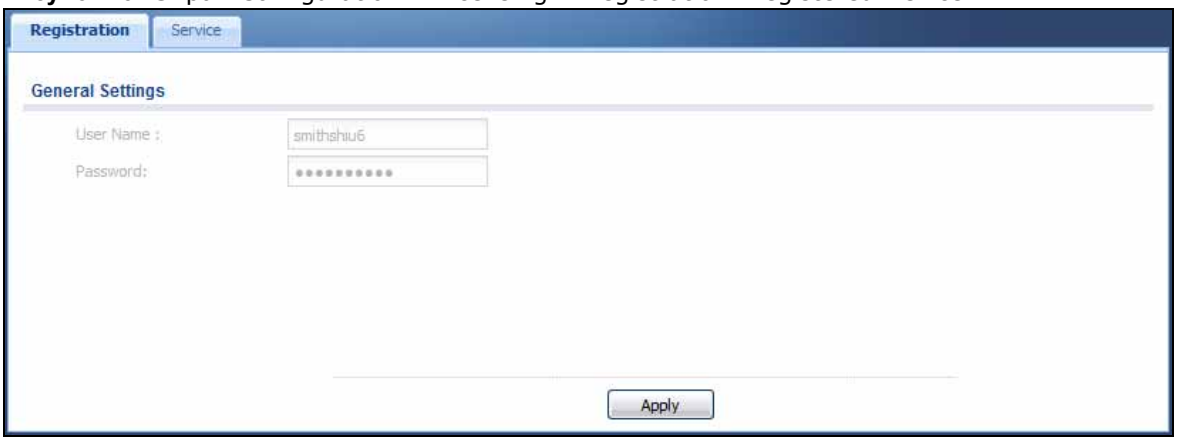
ПОЛЕ	ОПИСАНИЕ
General Settings	Если выбрать **existing myZyXEL.com account** (существующая учетная запись myZyXEL.com), на экране будут видны только поля **User Name** и **Password**.
new myZyXEL.com account	Если у вас еще нет учетной записи на сайте myZyXEL.com, выберите эту опцию и заполните следующие поля, чтобы создать учетную запись и зарегистрировать устройство NXC.
existing myZyXEL.com account	Если у вас уже есть учетная запись myZyXEL.com, выберите эту опцию и введите имя пользователя/пароль в полях ниже, чтобы зарегистрировать устройство NXC.
UserName	Введите имя пользователя для учетной записи myZyXEL.com. Длина имени должна составлять от шести до 20 символов. В имени можно использовать алфавитно-цифровые символы и знак подчеркивания. Использование пробелов в имени не допускается.
Check	Нажмите эту кнопку, если необходимо проверить, не существует ли уже в базе myZyXEL.com выбранное имя пользователя.
Password	Введите пароль. Длина пароля должна составлять от шести до 20 символов. В пароле можно использовать алфавитно-цифровые символы и знак подчеркивания. Использование пробелов в имени не допускается.
Confirm Password	Введите пароль еще раз для подтверждения.
E-Mail Address	Введите адрес электронной почты. В этом поле можно ввести строку длиной до 80 символов. Разрешается использовать алфавитно-цифровые символы, точки и подчеркивания, использование пробелов не допускается.

Таблица 45 Экран Configuration > Licensing > Registration (продолжение)

ПОЛЕ	ОПИСАНИЕ
Country	Выберите страну из выпадающего списка.
Seller Details	Этот раздел служит для ввода информации о продавце.
Seller's Name	Введите имя продавца.
Seller's E-mail	Введите адрес электронной почты продавца.
Seller's Contact Number	Введите номер телефона продавца.
VAT Number	Укажите номер плательщика НДС продавца, если устройство NXC было приобретено в Европе.
I accept the terms in the Privacy Policy	При согласии с условиями политики конфиденциальности, изложенными в тексте над этим полем, установите данный переключатель.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.

Примечание: В случае успешной регистрации устройства NXC этот экран будет доступен только для чтения. Чтобы обновить состояние подписки на службы, воспользуйтесь экраном **Service**.

Рисунок 43 Экран Configuration > Licensing > Registration: Registered Device



6.2.2 NXC5500

Щелкните по ссылке на этом экране, чтобы зарегистрировать устройство NXC на сайте myZyXEL.com. Перед тем, как начать процедуру регистрации, убедитесь, что устройство NXC имеет доступ к Интернету. Чтобы открыть экран, показанный ниже, выберите в меню навигационной панели **Configuration > Licensing > Registration**.

Рисунок 44 Экран Configuration > Licensing > Registration

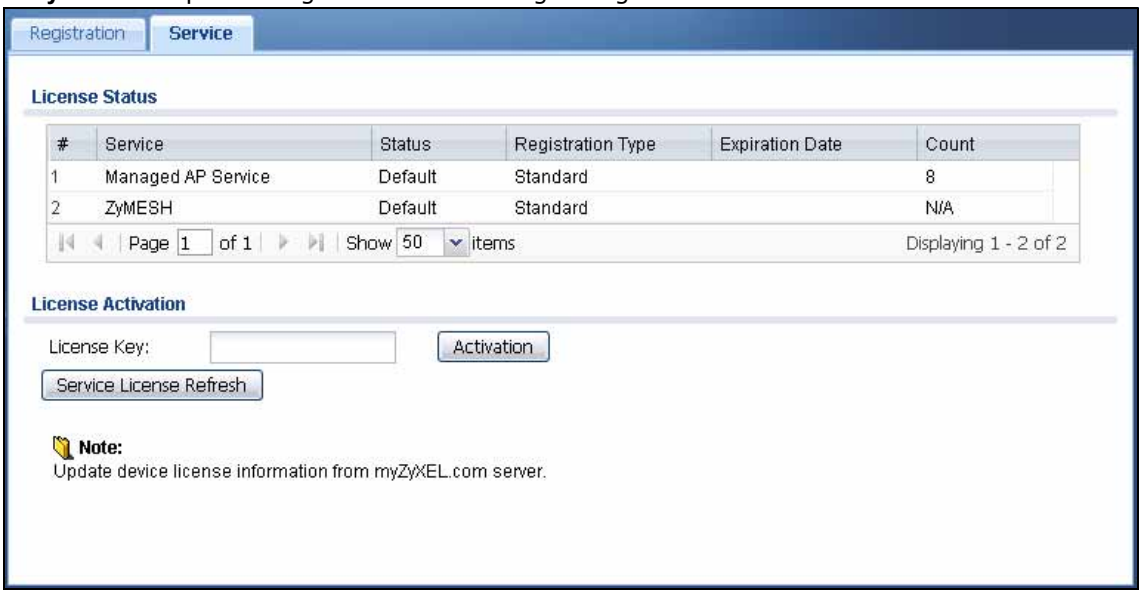
6.3 Экран Service

Внешний вид этого экрана зависит от используемой модели устройства NXC.

6.3.1 NXC2500

Этот экран служит для отображения состояния регистраций служб и обновления лицензий. Чтобы активировать или продлить стандартную подписку на службу, купите iCard и введите PIN-код iCard (лицензионный ключ) на этом экране.Чтобы открыть экран, показанный ниже, выберите в меню навигационной панели **Configuration > Licensing > Registration** > **Service**.

Рисунок 45 Экран Configuration > Licensing > Registration > Service



Поля экрана описаны в следующей таблице.

Таблица 46 Экран Configuration > Licensing > Registration > Service

ПОЛЕ	ОПИСАНИЕ
License Status	
#	В этом поле показана позиция записи в списке.
Service	Это поле показывает список служб, доступных на устройстве NXC.
Status	Это поле указывает на состояние службы: служба по умолчанию (**Default**) или активированное обновление лицензии (**Licensed**).
Registration Type	В этом поле отображается значение «**standard**», если служба была зарегистрирована с использованием PIN-кода iCard.
Expiration Date	Это поле показывает дату окончания срока действия службы.
Count	В этом поле отображается количество точек управляемых точек доступа, которые данное устройство NXC способно поддерживать при текущей лицензии. Это поле не применимо для других служб.
License Activation	

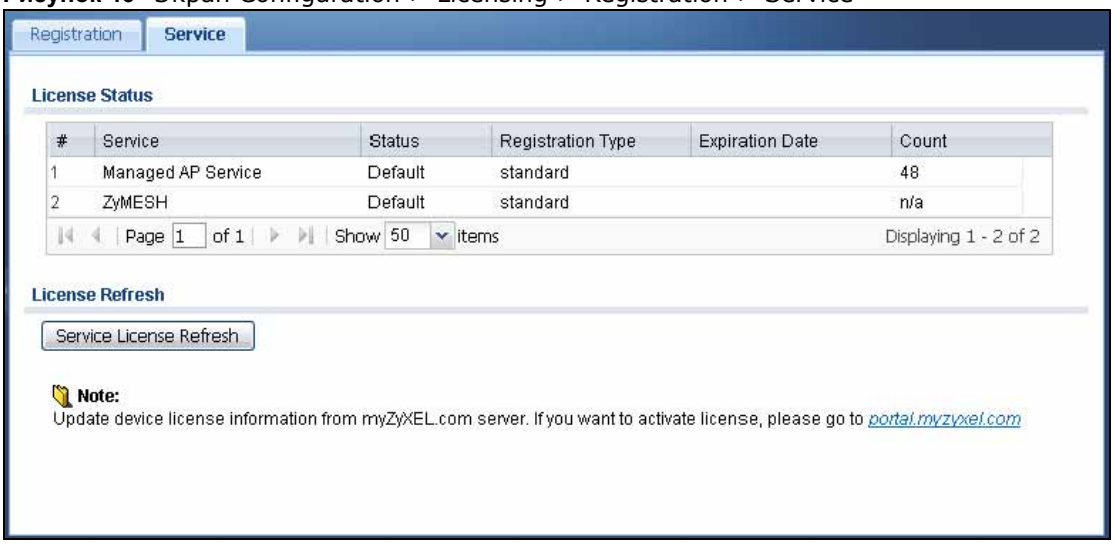
Таблица 46 Экран Configuration > Licensing > Registration > Service (продолжение)

ПОЛЕ	ОПИСАНИЕ
License Key	Введите PIN-код iCard и нажмите кнопку **Activation**, чтобы активировать или продлить стандартную подписку на службу. Если срок действия стандартной подписки на службу истек, необходимо приобрести новую iCard (для конкретного устройства NXC) и ввести новый PIN-код для продления службы.
Service License Refresh	Нажмите эту кнопку, чтобы обновить информацию о лицензии на данную службу (в частности, сведения о состоянии регистрации и дате окончания срока действия).

6.3.2 NXC5500

Этот экран служит для отображения состояния регистраций служб и обновления лицензий. Чтобы активировать или продлить стандартную подписку на службу, купите iCard и введите PIN-код iCard (лицензионный ключ) на этом экране. Чтобы открыть экран, показанный ниже, выберите в меню навигационной панели **Configuration > Licensing > Registration** > **Service**.

Рисунок 46 Экран Configuration > Licensing > Registration > Service



Поля экрана описаны в следующей таблице.

Таблица 47 Экран Configuration > Licensing > Registration > Service

ПОЛЕ	ОПИСАНИЕ
License Status	
#	В этом поле показана позиция записи в списке.
Service	Это поле показывает список служб, доступных на устройстве NXC.
Status	Это поле указывает на состояние службы: служба по умолчанию (**Default**) или активированное обновление лицензии (**Licensed**).
Registration Type	В этом поле отображается значение «**standard**», если служба была зарегистрирована с использованием PIN-кода iCard.
Expiration Date	Это поле показывает дату окончания срока действия службы.
Count	В этом поле отображается количество точек управляемых точек доступа, которые данное устройство NXC способно поддерживать при текущей лицензии. Это поле не применимо для других служб.

Таблица 47 Экран Configuration > Licensing > Registration > Service (продолжение)

ПОЛЕ	ОПИСАНИЕ
License Refresh	
Service License Refresh	Нажмите эту кнопку, чтобы обновить информацию о лицензии на данную службу (в частности, сведения о состоянии регистрации и дате окончания срока действия).

7

Беспроводные устройства

7.1 Обзор

С помощью экранов группы **Wireless** можно управлять параметрами взаимодействия устройства NXC с подключающимися к нему точками доступа.

7.1.1 О чем рассказывается в этой главе

- Экран **Controller** (разд. 7.2 на стр. 100) содержит параметры, описывающие правила подключения новых точек доступа к сети через устройство NXC.
- Экран **AP Management** (разд. 7.3 на стр. 101) описывает параметры управления всеми точками доступа, подключенными к устройству NXC.
- Экран **MON Mode** (разд. 7.4 на стр. 108) позволяет включать соответствующие точки доступа в список мошеннических или дружественных точек доступа.
- Экран **Load Balancing** (разд. 7.5 на стр. 111) описывает параметры балансировки сетевого трафика между точками доступа и устройством NXC.
- Экран **DCS** (разд. 7.6 на стр. 113) описывает параметры динамического выбора радиоканала для управляемых точек доступа.
- Экран **Auto Healing** (разд. 7.7 на стр. 116) позволяет включить функцию автоматического восстановления работоспособности (auto healing) для расширения беспроводной зоны покрытия группы управляемых точек доступа в случае сбоя одной из них.

7.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Станция / беспроводной клиент

Станцией или беспроводным клиентом называют любое устройство с поддержкой функций беспроводной связи, которое может подключаться к точке доступа по радиоканалу.

Динамический выбор канала

Динамический выбор канала (Dynamic Channel Selection, DCS) – это функция, которая позволяет точке доступа автоматически выбирать радиоканал для широковещательной передачи. Для этого она сканирует окружающее пространство и определяет, какие каналы в настоящее время задействованы другими устройствами.

Балансировка нагрузки (беспроводная)

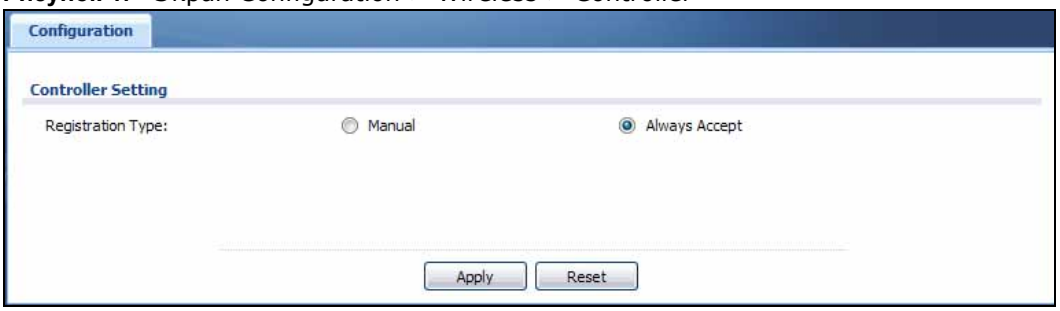
Балансировка нагрузки в беспроводной сети – это процесс ограничения количества соединений, разрешенных для данной беспроводной точки доступа, или объема входящего/

исходящего беспроводного трафика. Балансировка нагрузки позволяет защитить точку доступа от перегрузки.

7.2 Экран Controller

С помощью этого экрана можно настроить параметры, описывающие правила подключения новых точек доступа к сети через устройство NXC. Чтобы перейти к этому экрану, выберите в меню **Configuration > Wireless > Controller**.

Рисунок 47 Экран Configuration > Wireless > Controller



Описание каждого из полей приведено в таблице ниже.

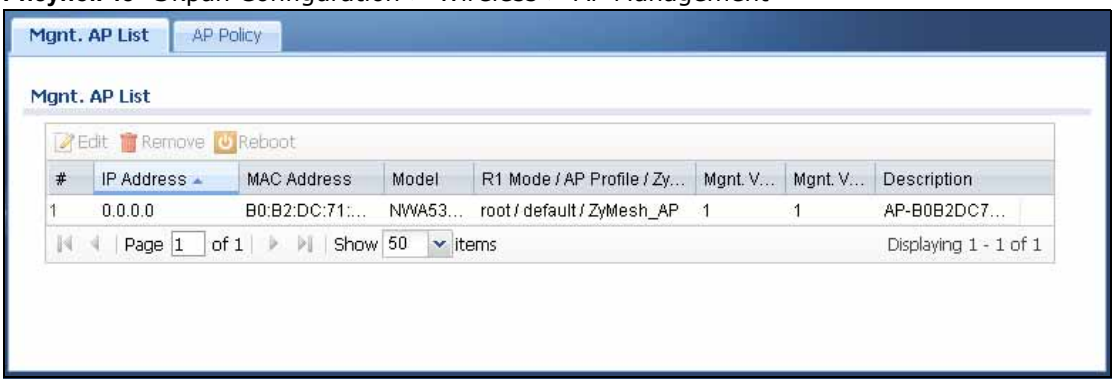
Таблица 48 Экран Configuration > Wireless > Controller

ПОЛЕ	ОПИСАНИЕ
Registration Type	Выберите опцию **Manual**, если необходимо добавлять каждую новую точку доступа на устройстве NXC вручную, или опцию **Always Accept**, чтобы регистрация новых точек доступа на устройстве NXC происходила автоматически. Примечание: Выберите опцию **Manual** для управления определенной группой точек доступа. Эта опция является рекомендуемой, поскольку механизм регистрации не может автоматически отличать дружественные точки доступа от мошеннических. Более подробную информацию о том, как поступать с мошенническими точками доступа, можно найти в разд. 5.15 на стр. 85. Точи доступа должны быть подключены к устройству NXC по проводному соединению или сети.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

7.3 Экран AP Management

С помощью этого экрана можно управлять всеми точками доступа, подключенными к устройству NXC. Чтобы перейти к этому экрану, выберите в меню **Configuration > Wireless > AP Management**.

Рисунок 48 Экран Configuration > Wireless > AP Management



Описание каждого из полей приведено в таблице ниже.

Таблица 49 Экран Configuration > Wireless > AP Management

ПОЛЕ	ОПИСАНИЕ
Edit	Выберите нужную точку доступа и нажмите эту кнопку, чтобы изменить ее параметры.
Remove	Выберите нужную точку доступа и нажмите эту кнопку, чтобы удалить ее из списка. Примечание: Если на экране **Configuration > Wireless > Controller** для параметра **Registration Type** установлено значение **Always Accept**, то после удаления точки доступа из списка она заново подключится к устройству.
Reboot	Выберите нужную точку доступа и нажмите эту кнопку, чтобы произвести ее принудительную перезагрузку.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо интерфейсом.
IP-адрес	В этом поле отображается IP-адрес данной точки доступа.
MAC Address	В этом поле отображается MAC-адрес данной точки доступа.
Model	Это поле содержит сведения о модели аппаратного обеспечения данной точки доступа. Значение **N/A** (не применимо) отображается в этом поле только в случае отключения точки доступа от устройства NXC и, как следствие, недоступности информации о ее модели.
R1 Mode / AP Profile / ZyMesh Profile	Это поле содержит сведения о режиме работы (**AP** [точка доступа], **MON** [мониторинг], **root** [корневая точка доступа] или **repeater** [повторитель]), имени радиопрофиля точки доступа и имени профиля ZyMesh для радиомодуля 1 (Radio 1). Вместо описания профиля точки доступа или профиля ZyMesh в этом поле отображается «**n/a**», если радиомодуль не использует соответственно профиль точки доступа или профиль ZyMesh.
R2 Mode / AP Profile / ZyMesh Profile	Это поле содержит сведения о режиме работы (**AP** [точка доступа], **MON** [мониторинг], **root** [корневая точка доступа] или **repeater** [повторитель]), имени радиопрофиля точки доступа и имени профиля ZyMesh для радиомодуля 2 (Radio 1). Вместо описания радиопрофиля точки доступа или профиля ZyMesh в этом поле отображается «**n/a**», если радиомодуль не использует соответственно радиопрофиль точки доступа или профиль ZyMesh.

Таблица 49 Экран Configuration > Wireless > AP Management (продолжение)

ПОЛЕ	ОПИСАНИЕ
Mgnt. VLAN ID(AC)	Это поле показывает идентификатор сети VLAN управления для данной точки доступа, установленный на контроллере доступа (устройства NXC).
Mgnt. VLAN ID(AP)	Это поле показывает идентификатор сети VLAN управления времени выполнения, установленный на точке доступа. **Значение VLAN Conflict** отображается в том случае, если идентификатор сети VLAN управления, установленный на точке доступа, не совпадает с идентификатором в поле **Mgnt. VLAN ID(AC)**. В этом поле отображается значение «**n/a**», если устройство NXC не может получить информацию о сети VLAN от точки доступа.
Description	Это поле содержит описание точки доступа. Чтобы его изменить, нужно выбрать нужную точку доступа и нажать кнопку **Edit**.

7.3.1 Экран Edit AP List

Чтобы открыть этот экран, выберите нужную точку доступа, а затем нажмите кнопку **Edit** в таблице **Configuration > Wireless > AP Management**.

Рисунок 49 Экран Configuration > Wireless > AP Management > Edit AP List

Описание каждого из полей приведено в таблице ниже.

Таблица 50 Экран Configuration > Wireless > AP Management > Edit AP List

ПОЛЕ	ОПИСАНИЕ
Create new Object	С помощью этого меню можно создать новый объект типа **Radio Profile**, **MON Profile** или **ZyMesh Profile**, который необходимо ассоциировать с данной точкой доступа.
MAC	Это поле показывает MAC-адрес выбранной точки доступа.

Таблица 50 Экран Configuration > Wireless > AP Management > Edit AP List (продолжение)

ПОЛЕ	ОПИСАНИЕ
Model	Это поле содержит сведения о модели аппаратного обеспечения данной точки доступа. Значение **N/A** (не применимо) отображается в этом поле только в случае отключения точки доступа от устройства NXC и, как следствие, недоступности информации о ее модели.
Description	Введите описание для данной точки доступа. Длина описания может составлять не более 31 символа, можно использовать пробелы и подчеркивания.
Radio 1/2 OP Mode	Выберите режим работы для радиомодуля 1 или радиомодуля 2. Значение **AP Mode** указывает на то, что данная точка доступа может принимать соединения, инициированные беспроводными клиентами, и передавать их трафик данных для управления на устройство NXC (или на следующий шлюз более высокого уровня). Значение **MON Mode** свидетельствует о том, что данная точка доступа AP отслеживает зону широковещательной передачи на предмет наличия других точек доступа, а затем передает информацию о них устройству NXC, которое определяет, является ли данная точка доступа дружественной или мошеннической. Точка доступа, работающая в режиме мониторинга (MON Mode), не может принимать входящие соединения от беспроводных клиентов. Значение **Root AP** говорит о том, что радиомодуль выступает в качестве точки доступа и поддерживает беспроводные подключения с другими точками доступа (в режиме повторителя) с целью формирования сети ZyMesh/WDS для увеличения зоны покрытия беспроводной сети. Значение **Repeater AP** говорит о том, что данный радиомодуль может устанавливать беспроводные соединения с другими точками доступа (либо в режиме корневой точки доступа, либо в режиме повторителя). Примечание: Чтобы исключить образование мостовых петель, не устанавливайте режим **Repeater AP** на обоих радиомодулях управляемой точки доступа. Примечание: При изменении режима работы управляемую точку доступа необходимо перезагрузить.
Radio 1/2 AP Profile	Выберите профиль точки доступа из списка. Если профиля нет, его можно создать с помощью меню **Create new Object**.
Radio 1/2 Profile	Выберите профиль режима мониторинга из списка. Если профиля нет, его можно создать с помощью меню **Create new Object**.
Radio 1/2 ZyMesh Profile	Это поле доступно только в том случае, если для радиомодуля установлен режим **Root AP** или **Repeater AP**. Выберите профиль ZyMesh, который радиомодуль будет использовать для подключения к корневой точке доступа или повторителю.
Force Overwrite VLAN Config	Установите этот переключатель, чтобы устройство NXC принудительно меняло управляющую сеть, заданную для данной точки доступа, для приведения ее в соответствие с конфигурацией, показанной на экране.
Management VLAN ID	Введите идентификатор сети VLAN для данной точки доступа.
As Native VLAN	Выберите эту опцию, чтобы сеть VLAN с данным идентификатором рассматривалась как сеть, созданная на устройстве NXC, а не как сеть, назначенная ему извне.
Port Setting	
#	В этом поле указан последовательный номер порта в списке.
Status	Это поле указывает на состояние порта – активирован он или нет.
Port	В этом поле отображается название физического порта Ethernet на управляемой точке доступа.

Таблица 50 Экран Configuration > Wireless > AP Management > Edit AP List (продолжение)

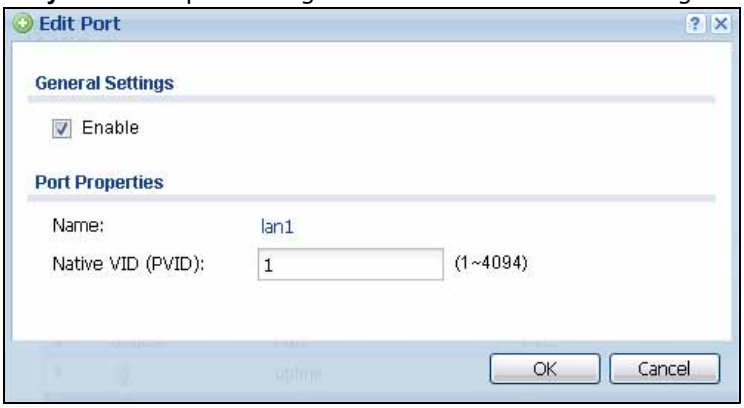
ПОЛЕ	ОПИСАНИЕ
PVID	Это поле показывает кадр приоритета (PVID) порта. PVID (идентификатор сети VLAN порта) – это тег, которым помечаются входящие кадры без тегов, принимаемые портом, с тем, чтобы потом перенаправить эти кадры в группу VLAN, которую определяет данный тег.
VLAN Configuration	
#	Это последовательный номер данной сети VLAN в этом списке.
Status	В этом поле отображается состояние сети VLAN: активирована или нет.
Name	Это поле показывает имя сети VLAN.
VID	Это поле показывает идентификатор сети VLAN.
Member	Это поле содержит список портов Ethernet, входящих в данную сеть VLAN.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, если необходимо закрыть окно без сохранения изменений.

7.3.2 Экран Port Setting Edit

С помощью этого экрана можно включить или отключить определенный порт на управляемой точке доступа и задать кадр приоритета (PVID) для порта.

Чтобы открыть этот экран, выберите нужный порт и нажмите кнопку **Edit** в таблице **Port Setting** на экране **Configuration > Wireless > AP Management > Edit AP List**.

Рисунок 50 Экран Configuration > Wireless > AP Management > Edit AP List > Edit Port



Описание каждого из полей приведено в таблице ниже.

Таблица 51 Экран Configuration > Wireless > AP Management > Edit AP List > Edit Port

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы активировать порт. В противном случае снимите выделение с переключателя.
Name	Это поле показывает наименование порта.
Native VID (PVID)	PVID (идентификатор сети VLAN порта) – это тег, которым помечаются входящие кадры без тегов, принимаемые портом, с тем, чтобы потом перенаправить эти кадры в группу VLAN, которую определяет данный тег. Введите значение PVID для данного порта из диапазона от 1 до 4094.

Таблица 51 Экран Configuration > Wireless > AP Management > Edit AP List > Edit Port

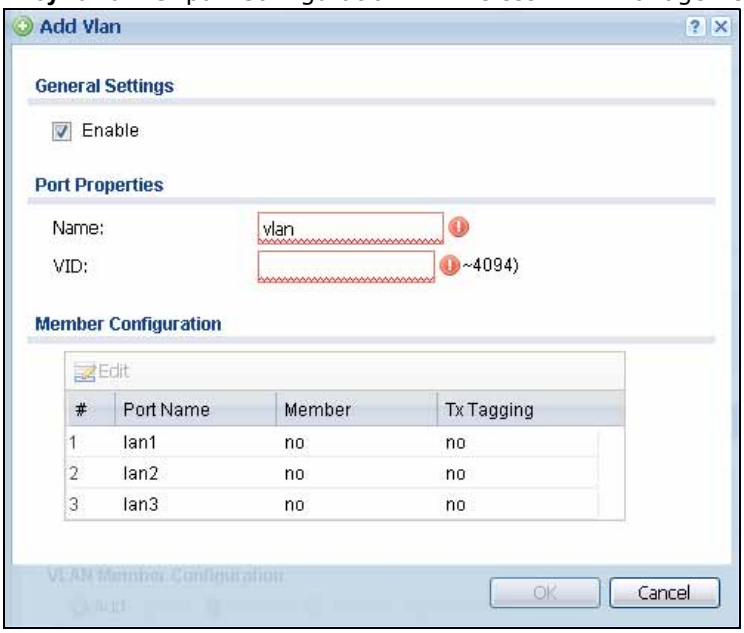
ПОЛЕ	ОПИСАНИЕ
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, если необходимо закрыть окно без сохранения изменений.

7.3.3 Экран VLAN Add/Edit

С помощью этого экрана можно создать новую сеть VLAN или настроить параметры существующей сети VLAN на устройстве NXC.

Чтобы открыть этот экран, нажмите кнопку **Add** или выберите нужную сеть VLAN и нажмите кнопку **Edit** в таблице **VLAN Member Configuration** на экране **Configuration > Wireless > AP Management > Edit AP List**.

Рисунок 51 Экран Configuration > Wireless > AP Management > Edit AP List > Edit VLAN



Описание каждого из полей приведено в таблице ниже.

Таблица 52 Экран Configuration > Wireless > AP Management > Edit AP List > Edit VLAN

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы активировать данную сеть VLAN. В противном случае снимите выделение с переключателя.
Name	При изменении настроек существующей сети VLAN это поле доступно только для чтения. Введите номер для данной сети VLAN. Номер можно выбрать из диапазона от 0 до 4095. Например, vlan0, vlan8 и т.д.
VID	Введите идентификатор сети VLAN (VLAN ID). Это 12-разрядное число уникальным образом идентифицирует каждую сеть VLAN. Допустимые значения выбираются из диапазона от 1 до 4094. (значения 0 и 4095 зарезервированы)
Member Configuration	С помощью настроек этой группы можно назначить порты участниками данной сети VLAN.

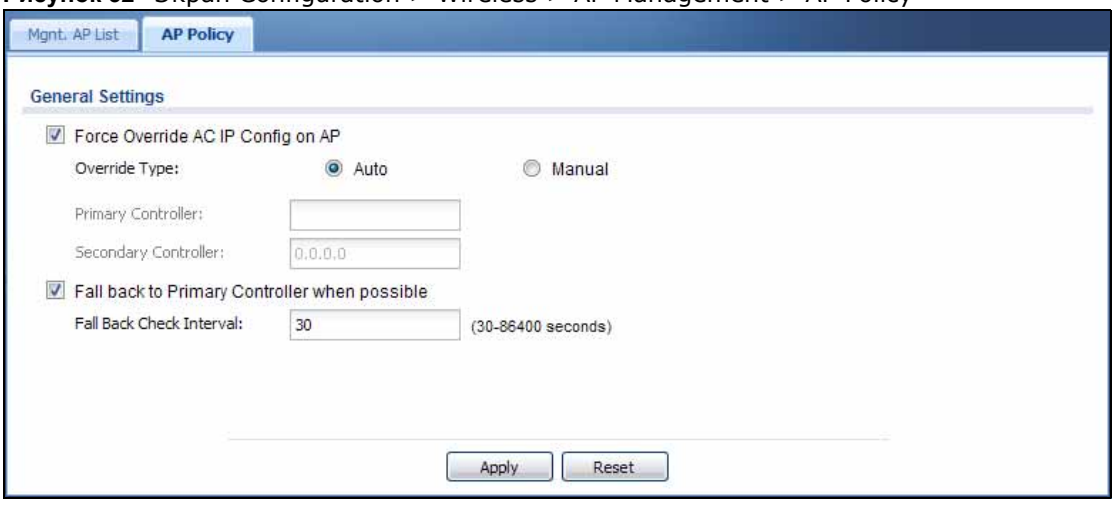
Таблица 52 Экран Configuration > Wireless > AP Management > Edit AP List > Edit VLAN

ПОЛЕ	ОПИСАНИЕ
Edit	Нажмите эту кнопку, чтобы изменить параметры участия выбранного порта в сети VLAN.
#	Это поле содержит последовательный указатель номера порта.
Port Name	Это поле показывает имя порта.
Member	Это поле указывает, является ли выбранный порт участником сети VLAN, параметры которой редактируются в настоящий момент. Щелкните по этому полю, чтобы изменить значение в нем.
Tx Tagging	Это поле указывает на то, помечает ли выбранный порт исходящий трафик тегами, содержащими идентификатор этой сети VLAN. Щелкните по этому полю, чтобы изменить значение в нем.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, если необходимо закрыть окно без сохранения изменений.

7.3.4 Экран AP Policy

С помощью этого экрана можно выполнить настройку IP-адреса контроллера точек доступа на управляемых точках доступа и описать действия, которые должны предпринять управляемые точки доступа в случае сбоя текущего контроллера. Чтобы открыть этот экран, выберите в меню **Configuration > Wireless > AP Management > AP Policy**.

Рисунок 52 Экран Configuration > Wireless > AP Management > AP Policy



Описание каждого из полей приведено в таблице ниже.

Таблица 53 Экран Configuration > Wireless > AP Management > AP Policy

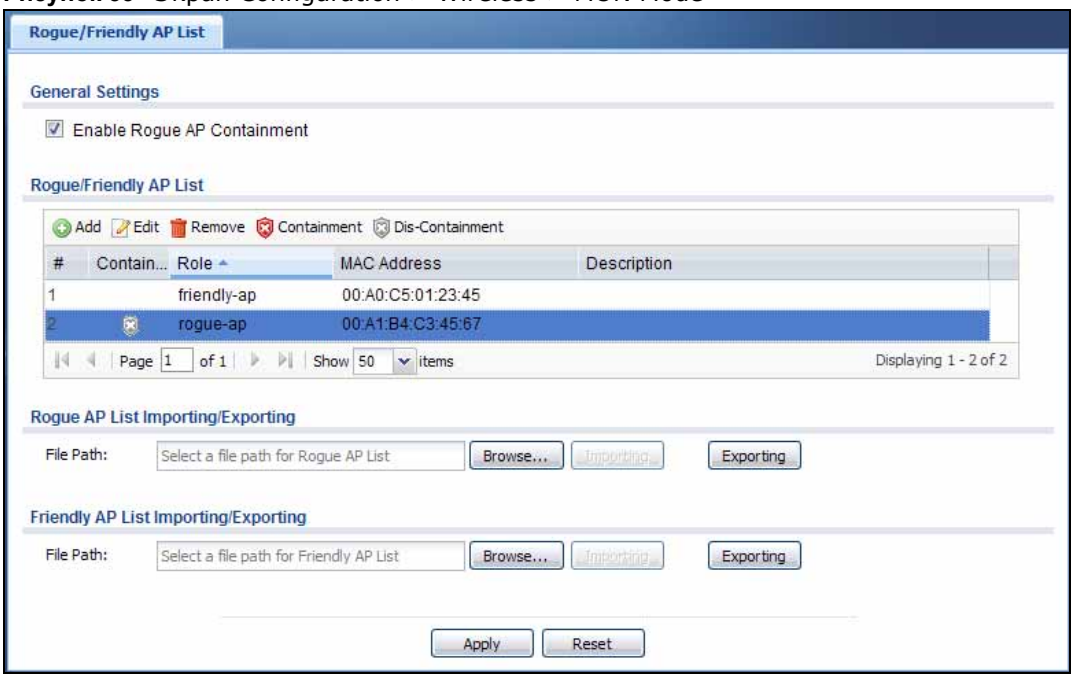
ПОЛЕ	ОПИСАНИЕ
Force Override AC IP Config on AP	Установите этот переключатель, чтобы устройство NXC принудительно меняло IP-адрес контроллера точек доступа на управляемых точках доступа для приведения его в соответствие с конфигурацией, показанной на экране.
Override Type	Выберите опцию **Auto**, чтобы управляемые точки доступа автоматически направляли широковещательные пакеты для поиска любых доступных контроллеров точек доступа. Выберите опцию **Manual**, если необходимо заменить IP-адрес контроллера точек доступа, установленный на управляемых точках доступа, на IP-адрес (или адреса), указанный в поле ниже.
Primary Controller	Укажите IP-адрес основного контроллера точек доступа, если в поле **Override Type** выбрано значение **Manual**.
Secondary Controller	Укажите IP-адрес дополнительного контроллера точек доступа, если в поле **Override Type** выбрано значение **Manual**.
Fall back to Primary Controller when possible	Установите этот переключатель, чтобы управляемая точка доступа переключалась на основной контроллер сразу же после восстановления его доступности.
Fall Back Check Interval	Этот параметр определяет, с какой периодичностью управляемая точка доступа проверяет доступность основного контроллера точек доступа.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

7.4 Экран MON Mode

Этот экран позволяет включить точки доступа либо в список мошеннических точек доступа, либо в список дружественных точек доступа. Мошенническая точка доступа – это беспроводная точка доступа, которая действует в зоне покрытия сети и при этом не контролируется администратором сети. Такая точка доступа представляет собой потенциальную угрозу для безопасности сети.

Чтобы перейти к этому экрану, выберите в меню **Configuration > Wireless > MON Mode**.

Рисунок 53 Экран Configuration > Wireless > MON Mode



Описание каждого из полей приведено в таблице ниже.

Таблица 54 Экран Configuration > Wireless > MON Mode

ПОЛЕ	ОПИСАНИЕ
General Settings	
Enable Rogue AP Containment	Установите этот переключатель, чтобы включить функцию сдерживания мошеннических точек доступа.
Rogue/Friendly AP List	
Add	Нажмите эту кнопку, чтобы добавить данную точку доступа в список и назначить ей статус мошеннической или дружественной.
Edit	Выберите в списке нужную точку доступа и поменяйте ее статус.
Remove	Выберите в списке точку доступа, которую необходимо удалить.
Containment	Нажмите эту кнопку, чтобы поместить выбранную точку доступа в карантин. Точка доступа, находящаяся на карантине, не может предоставлять доступ к каким-либо сетевым службам. Любые станции, которые пытаются подключиться к точке доступа, находящейся на карантине, отключаются автоматически.
Dis-Containment	Нажмите эту кнопку, чтобы вывести выбранную точку доступа из карантина. Точка доступа, выведенная из карантина, получает нормальный доступ к сети.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо интерфейсом.
Containment	Это поле указывает на статус сдерживания выбранной точки доступа.
Role	Это поле указывает, является ли выбранная точка доступа мошеннической или дружественной. Чтобы изменить роль точки доступа, нажмите кнопку **Edit**.
MAC Address	Это поле показывает MAC-адрес радиомодуля точки доступа.
Description	В этом поле отображается описание точки доступа. Чтобы изменить содержимое этого поля, нажмите кнопку **Edit**.

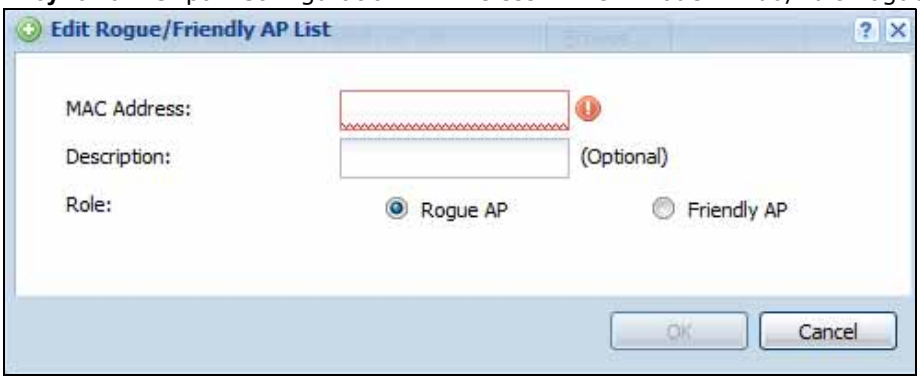
Таблица 54 Экран Configuration > Wireless > MON Mode (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rogue/Friendly AP List Importing/Exporting	Эти кнопки позволяют экспортировать текущие списки мошеннических и дружественных точек доступа или импортировать существующие списки.
File Path / Browse / Importing	Введите имя файла и путь к списку, который необходимо импортировать, или нажмите кнопку, чтобы выбрать его в файловой системе. После заполнения поля **File Path** нажмите кнопку **Importing**, чтобы загрузить список в устройство NXC.
Exporting	Нажмите эту кнопку, чтобы экспортировать текущий список мошеннических или дружественных точек доступа.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

7.4.1 Экран Add/Edit Rogue/Friendly List

Чтобы открыть этот экран, выберите нужную точку доступа и нажмите кнопку **Edit** в таблице **Configuration > Wireless > MON Mode**.

Рисунок 54 Экран Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly



Описание каждого из полей приведено в таблице ниже.

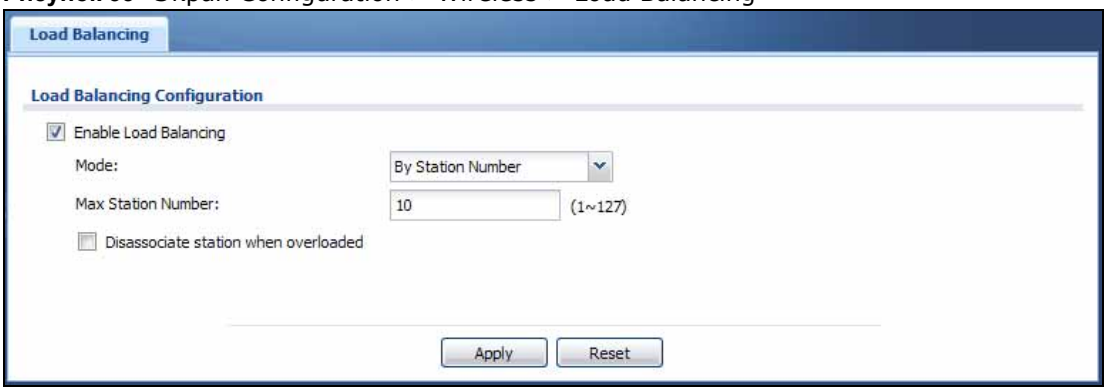
Таблица 55 Экран Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly

ПОЛЕ	ОПИСАНИЕ
MAC Address	Введите MAC-адрес точки доступа, которую необходимо добавить в список. MAC-адрес – это уникальный аппаратный идентификатор, представленный в следующем шестнадцатеричном формате: xx:xx:xx:xx:xx:xx, где xx – это шестнадцатеричное число, в котором в качестве разделителя используются двоеточия.
Description	Введите описание точки доступа (не более 60 символов). Допускается использование символов пробела и подчеркивания.
Role	Выберите роль для данной точки доступа: **Rogue AP** (мошенническая) или **Friendly AP** (дружественная).
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, если необходимо закрыть окно без сохранения изменений.

7.5 Экран Load Balancing

С помощью этого экрана можно описать параметры балансировки нагрузки сетевого трафика между точками доступа в сети. Чтобы перейти к этому экрану, выберите в меню **Configuration > Wireless > Load Balancing**.

Рисунок 55 Экран Configuration > Wireless > Load Balancing



Описание каждого из полей приведено в таблице ниже.

Таблица 56 Экран Configuration > Wireless > Load Balancing

ПОЛЕ	ОПИСАНИЕ
Enable Load Balancing	Установите этот переключатель, если необходимо включить балансировку нагрузки на устройстве NXC.
Mode	Выберите режим балансировки нагрузки. Выберите опцию **By Station Number**, если необходимо выполнять балансировку исходя из количества указанных станций, подключенных к точке доступа. Выберите опцию **By Traffic Level**, если необходимо выполнять балансировку сетевого трафика исходя из объема трафика, сгенерированного станциями, подключенными к точке доступа. При достижении порогового значения (либо максимального количества станций, либо максимального объема трафика) данная точка доступа временно прекращает принимать запросы на ассоциацию и пакеты с запросами на аутентификацию от любой новой станции, которая пытается установить с ней соединение. Это дает возможность станции автоматически попробовать подключиться к другой, менее нагруженной точке доступа, если таковая имеется.
Max Station Number	Введите пороговое количество станций, при достижении которого точка доступа начинает балансировать нагрузку, временно отклоняя попытки подключений.
Traffic Level	Введите пороговое значение объема трафика, при достижении которого точка доступа начинает балансировать нагрузку, временно отклоняя попытки подключений (низкий, средний, высокий уровни).

Таблица 56 Экран Configuration > Wireless > Load Balancing (продолжение)

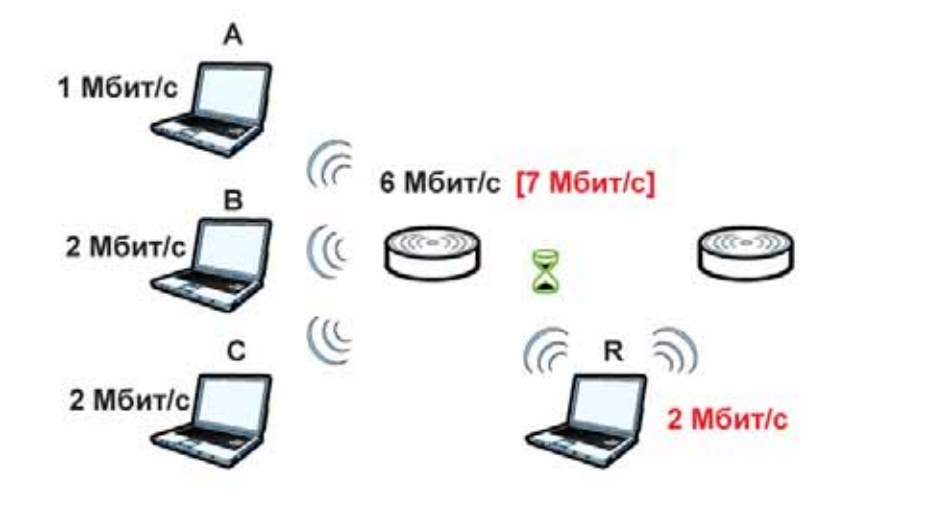
ПОЛЕ	ОПИСАНИЕ
Disassociate station when overloaded	Установите этот переключатель, чтобы удалить ассоциации с беспроводными клиентами, подключенными к данной точке доступа, когда она входит в состояние перегрузки. Если не установить этот переключатель, точка доступа просто временно прекратит устанавливать соединения до тех пор, пока не получит достаточной для этого соединения пропускной способности, или передаст соединение другой точке доступа в пределах радиуса широковещательной передачи. Приоритет удаления ассоциаций устройство NXC определяет автоматически по следующим правилам: • Время неактивности (**Idle Timeout**) – Ассоциации с устройствами, имеющими наиболее продолжительный период неактивности, будут удалены в первую очередь. Если все подключенные устройства активны, то приоритет определяется по силе сигнала. • Сила сигнала (**Signal Strength**) – Ассоциации с устройствами, имеющими наименьшую силу сигнала, будут удалены в первую очередь. Примечание: Перед включением этой функции необходимо удостовериться, что в пределах радиуса широковещательной передачи существуют две и более точек доступа, способных принять отвергнутые соединения, запрашиваемые беспроводными клиентами; в противном случае беспроводной клиент, пытающийся подключиться к перегруженной точке доступа, будет постоянно получать отказ в соединении и в конечном итоге так и не сможет подключиться к сети.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

7.5.1 Удаление ассоциаций и временный отказ в соединениях

В случае перегрузки точка доступа может реагировать двумя основными способами. Первый способ – это «временный отказ» в установлении соединения с клиентом. Это означает, что точка доступа «задерживает» соединение до тех пор, пока либо не упадет интенсивность потребления ресурсов полосы пропускания, либо другая точка доступа не подхватит это соединение. Если клиент подхвачен другой точкой доступа, исходная точка доступа не может возобновить соединение с ним.

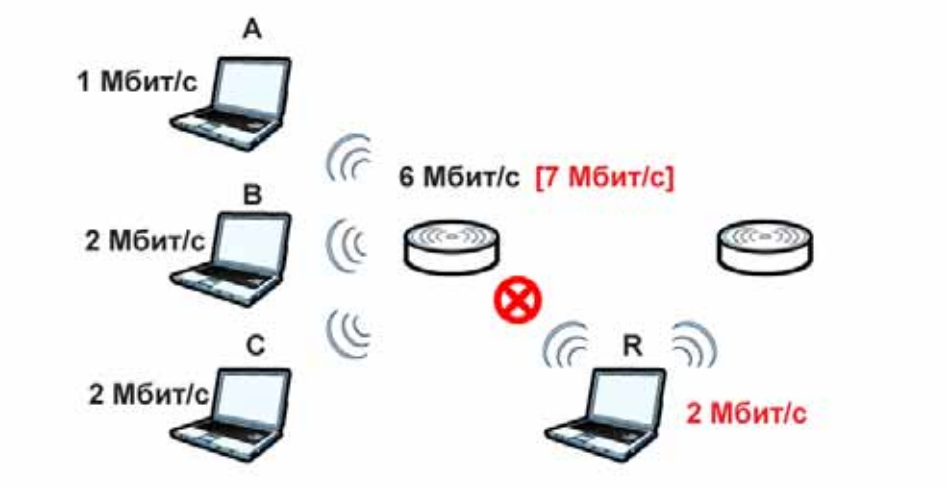
К примеру, у нас имеется точка доступа со сбалансированным выделением полосы пропускания в объеме 6 Мбит/с. Если к ней подключается ноутбук **R**, и это подключение требует ресурсов, выходящих за указанные рамки, скажем, 7 Мбит/с, то эта точка доступа временно отклоняет соединение с ноутбуком R до того момента, пока не будут высвобождены соответствующие ресурсы полосы пропускания, или этот ноутбук не «подхватит» другая точка доступа, располагающая достаточными ресурсами полосы пропускания.

Рисунок 56 Временный отказ в соединении



Точка доступа может отреагировать еще одним способом – прервать соединения, требования которых выходят за рамки установленного лимита сбалансированной полосы пропускания.

Рисунок 57 Разрыв соединения



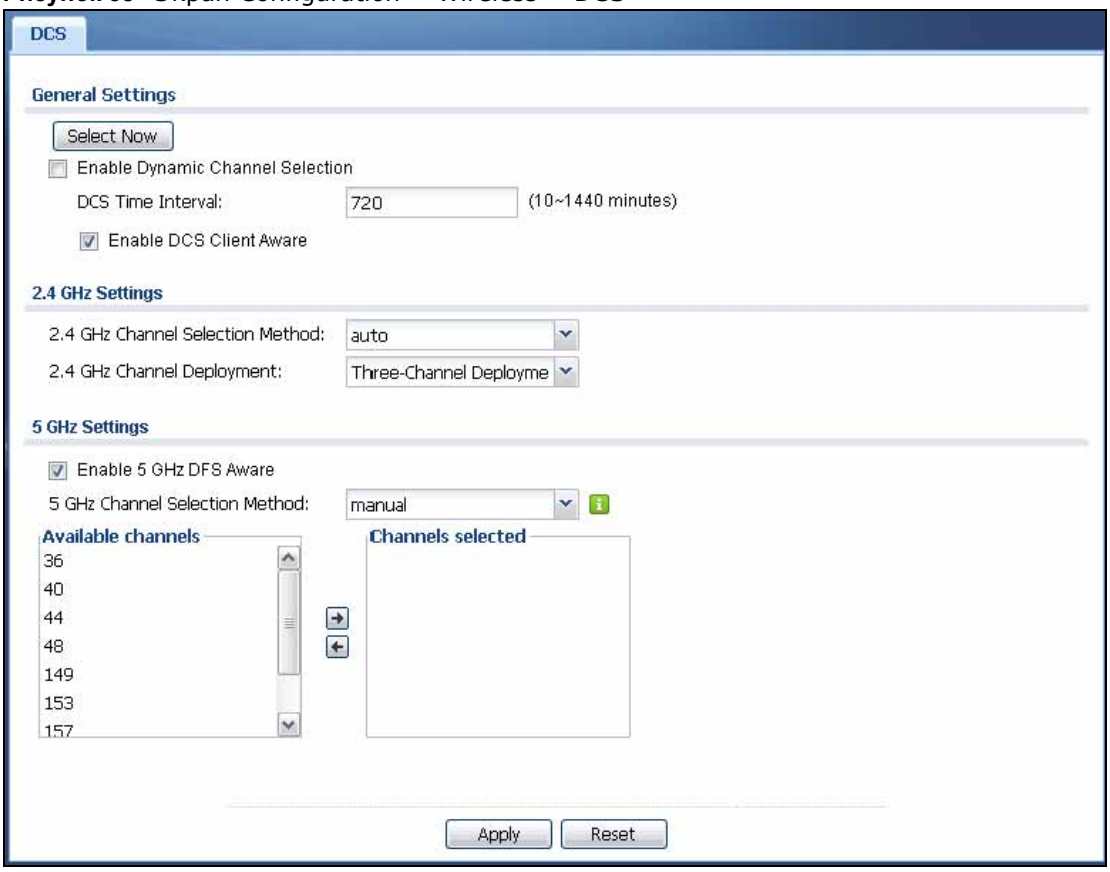
Разрыв соединений осуществляется на основе таких критериев, как время неактивности и сила сигнала. В первую очередь устройство NXC выбирает устройства с наибольшим периодом неактивности, а затем начинает отключать их (чем дольше период неактивности, тем раньше в списке на отключение встанет беспроводной клиент). Если неактивные соединения отсутствуют, устройство NXC анализирует следующий критерий – силу сигнала. Устройства с наименьшей силой сигнала будут отключены первыми.

7.6 Динамический выбор канала

Если в определенной зоне работает множество точек доступа, и существует вероятность возникновения помех, рекомендуется использовать функцию динамического выбора канала (DCS, Dynamic Channel Selection). Функция DCS позволяет точкам доступа автоматически находить в описанных условиях наименее задействованный канал. Используйте этот экран

для настройки параметров динамического выбора канала на управляемых точках доступа. Чтобы перейти к этому экрану, выберите в меню **Configuration > Wireless > DCS**.

Рисунок 58 Экран Configuration > Wireless > DCS



Описание каждого из полей приведено в таблице ниже.

Таблица 57 Экран Configuration > Wireless > DCS

ПОЛЕ	ОПИСАНИЕ
General Settings	
Select Now	Нажмите эту кнопку, чтобы управляемые точки доступа просканировали прилегающую зону широковещательной передачи и немедленно выбрали доступный канал.
Enable Dynamic Channel Selection	Установите этот переключатель, чтобы включить функцию динамического выбора канала для точек доступа, находящихся под управлением устройства NXC.
DCS Time Interval	Введите количество минут. Этот параметр определяет, с какой частотой устройство NXC проводит опрос других точек доступа, находящихся в радиусе широковещательной передачи. Если на канале, на котором данная точка доступа в настоящий момент осуществляет широковещательную передачу, вдруг начинает работать другая точка доступа, то устройство NXC в динамическом режиме выберет следующий доступный чистый канал или канал с минимальными помехами.
Enable DCS Client Aware	Установите этот переключатель, чтобы перед переключением на другой канал точка доступа всегда ожидала отключения всех подключенных клиентов. Если не устанавливать этот переключатель, то точка доступа будет переключаться с одного канала на другой немедленно, независимо от наличия клиентских подключений. В данном примере при переключении каналов точкой доступа происходит отключение всех клиентских соединений.

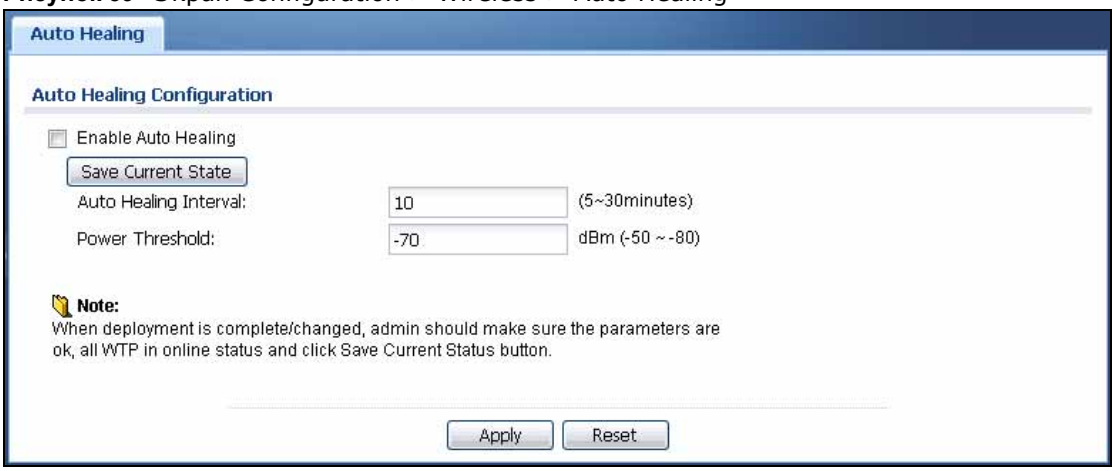
Таблица 57 Экран Configuration > Wireless > DCS (продолжение)

ПОЛЕ	ОПИСАНИЕ
2.4 GHz Settings	
2.4 GHz Channel Selection Method	Выберите опцию **auto**, чтобы точка доступа автоматически искала доступные каналы в диапазоне 2,4 ГГц. Перечень доступных каналов будет зависеть от опции, выбранной в поле **2.4 GHz Channel Deployment**. Выберите опцию **manual** и укажите самостоятельно каналы, которые данная точка доступа будет использовать в диапазоне 2,4 ГГц.
Available channels	Это текстовое поле содержит список каналов, доступных в диапазоне 2,4 ГГц. Выберите каналы для данной точки доступа и нажмите кнопку со стрелкой вправо, чтобы их добавить.
Channels selected	Это текстовое поле содержит список каналов, использование которых необходимо разрешить данной точке доступа. Выберите каналы, которые необходимо исключить из использования для данной точки доступа, и нажмите кнопку со стрелкой влево, чтобы убрать их из списка.
2.4 GHz Channel Deployment	Это поле доступно только в том случае, если в поле **2.4 GHz Channel Selection Method** выбрана опция **auto**. Выберите опцию **Three-Channel Deployment**, если необходимо ограничить перечень для переключения каналами 1, 6 и 11, тремя каналами, обладающими достаточным затуханием, чтобы практически полностью исключить влияние друг на друга. Другими словами, это позволяет минимизировать взаимные помехи между каналами за счет ограничения перечня каналов, доступных для переключения, этими тремя «безопасными» каналами. Выберите опцию **Four-Channel Deployment**, если необходимо ограничить перечень для переключения четырьмя каналами. В зависимости от страны, если единственными доступными каналами являются каналы в диапазоне от 1 до 11, устройство NXC использует в этой конфигурации каналы 1, 4, 7 и 11; в противном случае устройство NXC использует в этой конфигурации каналы 1, 5, 9 и 13. Опция Four channel deployment позволяет расширить пул возможных каналов, сохранив при этом минимальный уровень межканальных помех.
5 GHz Settings	
Enable 5 GHz DFS Aware	Установите этот переключатель, если на территории, где функционируют точки доступа, одновременно работают радарные установки. Эта опция позволяет устройству снизить частоту, перейти в диапазон ниже 5 ГГц при обнаружении сигнала от радара и таким образом избежать взаимных помех с этим сигналом. Если установить этот переключатель, точка доступа обязательно будет выбирать канал, не являющийся DFS-каналом.
5 GHz Channel Selection Method	Выберите опцию **auto**, чтобы точка доступа автоматически искала доступные каналы в диапазоне 5 ГГц. Выберите опцию **manual** и укажите самостоятельно каналы, которые данная точка доступа будет использовать в диапазоне 5 ГГц.
Available channels	Это текстовое поле содержит список каналов, доступных в диапазоне 5 ГГц. Выберите каналы для данной точки доступа и нажмите кнопку со стрелкой вправо, чтобы их добавить.
Channels selected	Это текстовое поле содержит список каналов, использование которых необходимо разрешить данной точке доступа. Выберите каналы, которые необходимо исключить из использования для данной точки доступа, и нажмите кнопку со стрелкой влево, чтобы убрать их из списка.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

7.7 Экран Auto Healing

С помощью этого экрана можно включить функцию автоматического восстановления работоспособности (auto healing), которая позволяет расширить зону покрытия группы управляемых точек доступа в случае сбоя одной из них. Чтобы перейти к этому экрану, выберите в меню **Configuration > Wireless > Auto Healing**.

Рисунок 59 Экран Configuration > Wireless > Auto Healing



Описание каждого из полей приведено в таблице ниже.

Таблица 58 Экран Configuration > Wireless > Auto Healing

ПОЛЕ	ОПИСАНИЕ
Enable Auto Healing	Установите этот переключатель, чтобы включить функцию auto healing.
Save Current State	Нажмите эту кнопку, чтобы все управляемые точки доступа немедленно просканировали соседства три раза подряд и обновили списки соседств на контроллере точек доступа (устройстве NXC).
Auto Healing Interval	В этом поле задается интервал (в минутах), через который управляемые точки доступа сканируют окружение и сообщают состояние соседних точек доступа контроллеру точек доступа (устройству NXC). Точка доступа считается неисправной, если контроллер точек доступа три раза получает одинаковый результат сканирования, говорящий о том, что данная точка доступа отсутствует в списках соседств у других точек доступа.
Power Threshold	Установите уровень мощности (в дБм), до которого соседние по отношению к неисправной точки доступа увеличивают выходную мощность, чтобы расширить собственные беспроводные зоны покрытия. После того, как неисправная точка доступа возвращается в рабочее состояние, соседние по отношению к ней точки доступа уменьшают выходную мощность до исходного уровня.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

7.8 Справочная техническая информация

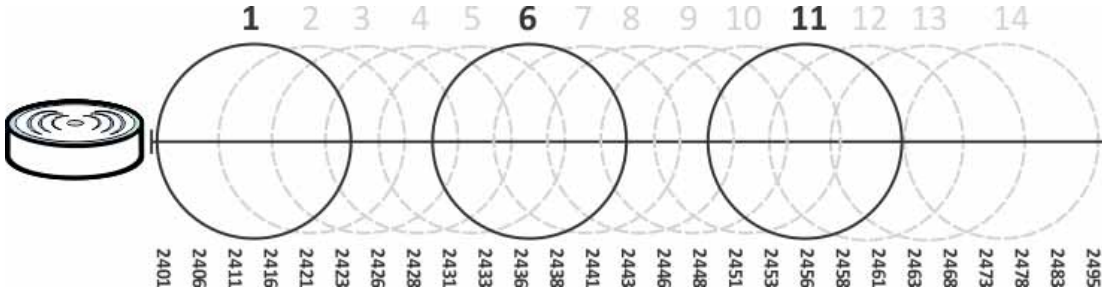
В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

7.8.1 Динамический выбор каналов

Если достаточно большое количество точек доступа ведут широковещательную передачу в определенной зоне, это создает риск повышения радиопомех, особенно, если все или некоторые из них работают на одном радиоканале. Если уровень помех становится слишком большим, сетевой администратор должен открыть настройки соответствующей точки доступа и вручную поменять действующий канал на другой, который не используют другие точки доступа (или, по крайней мере, на канал с более низким уровнем помех), чтобы обеспечить минимальный уровень помех для подключенных станций. Динамический выбор каналов освобождает сетевого администратора от этой нагрузки, поскольку позволяет точкам доступа выполнять смену канала автоматически. Точка доступа может сканировать окружающую территорию в поисках канала с наименьшим уровнем помех.

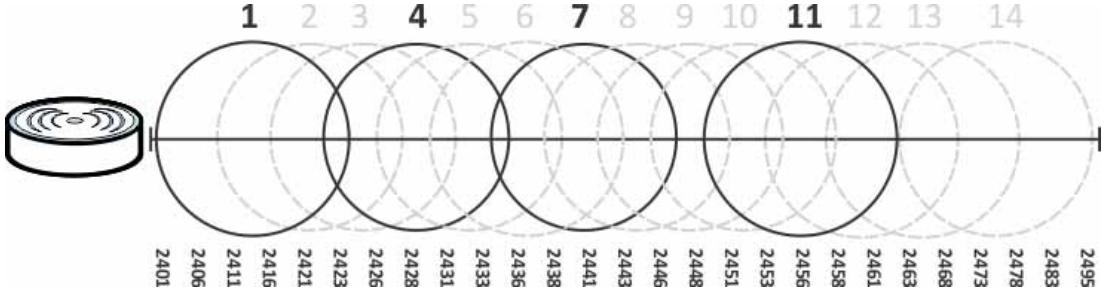
В диапазоне 2,4 ГГц каждый канал с номером с 1 по 13 разбит на дискретные сегменты шириной 22 МГц, отстоящие друг от друга на 5 МГц. Канал 1 зацентрован на частоте 2,412 ГГц, а канал 13 – на частоте 2,472 ГГц.

Рисунок 60 Пример трехканальной реализации



Три канала располагаются относительно друг друга таким образом, что при их исключительном использовании взаимные помехи практически отсутствуют: 1, 6 и 11. Если какая-либо точка доступа ведет широковещательную передачу на любом из указанных трех каналов, то она не должна создавать помехи для соседних точек доступа, если они тоже работают на каналах из этой троицы.

Рисунок 61 Пример четырехканальной реализации

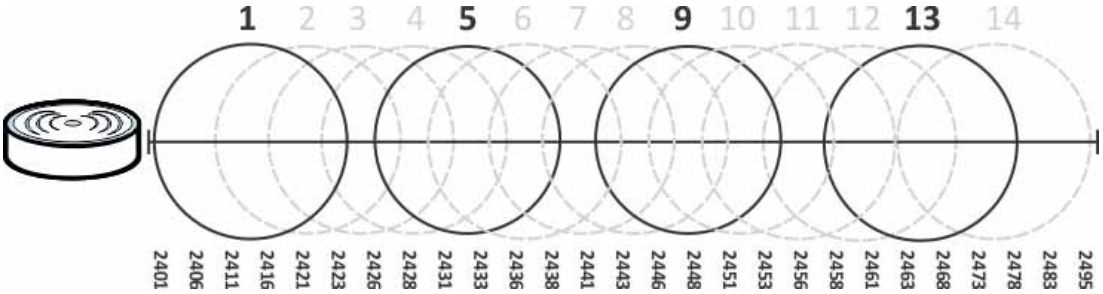


В некоторых регионах, однако, существуют требования об использовании других каналов, и в этом случае часто используется безопасная схема со следующими четырьмя каналами: 1, 4, 7

и 11. Тот факт, что они расположены относительно близко друг к другу и трем так называемым «безопасным» каналам (1, 6 и 11), делает помехи неизбежными. Уровень помех в этом случае зависит от других факторов: близость точки доступа, на которую влияют помехи, сила сигнала, активность и т.д.

Существует также альтернативная четырехканальная схема для ETSI, включающая в себя каналы 1, 5, 9 и 13. Эта схема обеспечивает существенно меньшее наложение каналов.

Рисунок 62 Альтернативная схема четырехканальной реализации



7.8.2 Балансировка нагрузки

Из-за жестких верхних ограничений на полосу пропускания беспроводных точек доступа механизм балансировки нагрузки может сыграть крайне важную роль в зонах с большим количеством пользователей беспроводных устройств. Вместо того, чтобы давать каждому пользователю подключаться и в конечном счете уменьшить доступные ресурсы полосы пропускания, когда каждому подключающемуся устройству достается мизерная пропускная способность, точка доступа с включенной функцией балансировки нагрузки ограничивает входящие соединения и таким образом защищает ресурсы полосы пропускания от дефицита.

Устройство NXC поддерживает два способа балансировки нагрузки:

Балансировка нагрузки по количеству станций ограничивает количество устройств, которым разрешено подключение к точке доступа. Если точно известно, скольким станциям необходимо разрешить одновременное подключение к точке доступа, выберите эту опцию.

Например, если в компании есть группа, занимающаяся графическим дизайном, у нее имеется собственная точка доступа и в этой группе – 10 компьютеров, то можно включить балансировку нагрузки на 10 устройств. Если какой-то сотрудник, к примеру, из отдела продаж, приедет в офис группы графических дизайнеров на совещание и попытается получить доступ к сети, его запрос на соединение будет временно отклонен с тем, чтобы он смог подключиться к другой, соседней точке доступа. Если же этот сотрудник все равно подключается к данной точке доступа, невзирая на задержку, то эта точка доступа может перегрузить других, уже подключенных сотрудников, чтобы создать ассоциацию с новым соединением.

Балансировка нагрузки по уровню трафика ограничивает число подключений к точке доступа исходя из максимально доступной полосы пропускания. Если не известно наверняка, какое количество подключений к точке доступа следует разрешить, можно выбрать эту опцию. Устанавливая предельное верхнее значение полосы пропускания, можно разрешить подключение к точке доступа практически любому количеству устройств – до тех пор, пока совокупный объем потребляемых ими ресурсов полосы пропускания не превысит установленное этим параметром пороговое значение. Как только порог будет

превышен, точка доступа будет отбрасывать все новые соединения или временно их запрещать при условии, что по соседству есть другие точки доступа.

Представьте себе кофейню в офисном центре, которая предлагает своим клиентам бесплатный доступ к беспроводной сети. Хозяин кофейни, вероятно, не может знать, сколько клиентов захочет подключиться к его точке доступа в каждый конкретный момент. Соответственно, он решает установить ограничение не по количеству доступных соединений, а по объему полосы пропускания, доступной клиентам. Это означает, что любой пользователь может подключиться к его беспроводной сети при условии наличия достаточного объема пропускной способности. Если к точке доступа подключилось слишком много пользователей, и достигнут верхний порог для полосы пропускания, то всем пользователям, которые захотят подключиться к точке доступа с этого момента фактически придется либо подождать своей очереди, либо подключиться к ближайшей идентичной точке доступа.

8

Интерфейсы

8.1 Обзор интерфейсов

Эти экраны служат для настройки интерфейсов устройства NXC.

- **Портами** называют физические порты, к которым подключаются кабели.
- **Интерфейсы** используются внутри системы для выполнения различных операций. С их помощью настраиваются разнообразные функции. Кроме того, интерфейс служит для описания сети, к которой непосредственно подключается устройство NXC. Например, через интерфейс осуществляется подключение к локальной сети.
- **Зоны** представляют собой группы интерфейсов. Наличие зон облегчает настройку политик безопасности.

8.1.1 О чем рассказывается в этой главе

- Экраны **Ethernet** (разд. 8.2 на стр. 121) служат для настройки интерфейсов Ethernet. Интерфейсы Ethernet образуют основу для всех прочих интерфейсов и сетевых политик.
- Экраны **VLAN** (разд. 8.3 на стр. 135) позволяют разделить одну физическую сеть на несколько логических. Интерфейсы VLAN получают и отправляют кадры с тегами. Устройство NXC автоматически добавляет или удаляет теги по мере необходимости.

8.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Характеристики интерфейсов

Как правило, интерфейсы имеют следующие характеристики (при этом надо помнить, что не все перечисленные характеристики применимы ко всем типам интерфейсов).

- Интерфейс – это логическая сущность, через которую проходят пакеты третьего уровня.
- Интерфейс привязан к физическому порту или другому интерфейсу.
- Несколько интерфейсов могут иметь общий физический порт.
- Интерфейс может входить только в одну зону.
- Несколько интерфейсов могут принадлежать к одной зоне.

Типы интерфейсов

На устройстве NXC можно создавать интерфейсы нескольких типов.

- **Интерфейсы Ethernet** являются основой для описания других интерфейсов и сетевых политик.

- **Интерфейсы VLAN** получают и отправляют кадры с тегами. Устройство NXC автоматически добавляет или удаляет теги по мере необходимости.

8.2 Сводный экран интерфейсов Ethernet

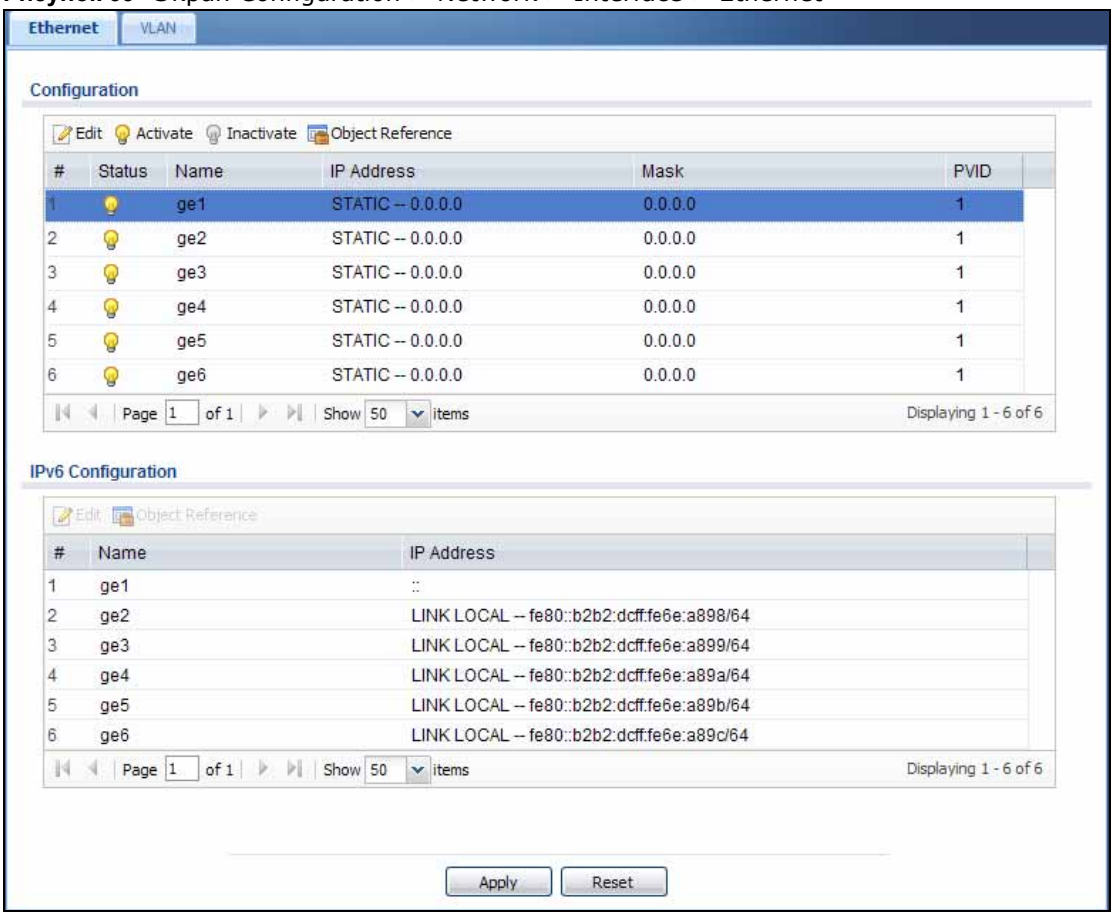
Этот экран содержит список всех интерфейсов Ethernet. Если на экране **Configuration > System > IPv6** была включена поддержка протокола IPv6, на этом экране можно будет настроить параметры интерфейсов VLAN, используемых сетями IPv6. Чтобы открыть этот экран, выберите в меню **Configuration > Network** > **Interface**.

В отличие от интерфейсов других типов, создавать новые интерфейсы Ethernet и удалять существующие невозможно. Если интерфейсу Ethernet не назначен ни один физический порт, то устройство NXC фактически удаляет его, хотя сохраняется возможность настраивать его параметры.

Интерфейсы Ethernet во многих отношениях напоминают интерфейсы других типов. У них есть IP-адрес, маска подсети и шлюз, используемый для принятия решений о маршрутизации. Они ограничивают полосу пропускания и размер пакета. Они могут предоставлять службы DHCP и проверять доступность шлюза.

С помощью интерфейсов Ethernet можно управлять тем, какие физические порты обмениваются маршрутной информацией с другими маршрутизаторами, а также перечнем информации, подлежащим обмену на каждом порту. Чем больше объем маршрутной информации, предназначенный для обмена, тем более эффективными должны быть маршрутизаторы. Следует учесть, однако, что в этом случае маршрутизаторы генерируют больше сетевого трафика, а некоторые протоколы маршрутизации требуют существенных усилий по настройке и управлению.

Рисунок 63 Экран Configuration > Network > Interface > Ethernet



Описание каждого из полей приведено в таблице ниже.

Таблица 59 Экран Configuration > Network > Interface > Ethernet

ПОЛЕ	ОПИСАНИЕ
Configuration/IPv6 Configuration	С помощью раздела **Configuration** можно настроить параметры протокола IPv4. С помощью раздела **IPv6 Configuration** можно настроить параметры протокола IPv6, если устройство NXC подключается к сети IPv6. В обоих разделах присутствуют схожие поля, которые описаны ниже.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Activate	Чтобы включить интерфейс, выберите его и нажмите кнопку **Activate**.
Inactivate	Чтобы выключить интерфейс, выберите его и нажмите кнопку **Inactivate**.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо интерфейсом.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Name	В этом поле отображается наименование данного интерфейса.

Таблица 59 Экран Configuration > Network > Interface > Ethernet (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Address	В этом поле отображается текущий IP-адрес интерфейса. если в поле IP-адреса отображается значение 0.0.0.0 (в сети IPv4) или значение :: (в сети IPv6), то это означает, что IP-адрес интерфейсу еще не назначен. Для сети IPv4 на этом экране также присутствуют сведения о том, является ли данный IP-адрес статическим (**STATIC**) или динамическим (**DHCP**). Для сети IPv6 этот экран показывает еще и информацию о том, является ли IP-адрес статическим (**STATIC**), относящимся к локальному соединению (**LINK LOCAL**), динамически назначенным (**DHCP**) или IP-адресом IPv6 **SLAAC** (StateLess Address AutoConfiguration).Дополнительную информацию об IPv6 можно найти в прил. E на стр. 477.
Mask	Это поле показывает маску подсети данного интерфейса в точечно-десятичной нотации.
PVID	Это поле показывает кадр приоритета (PVID) для данного интерфейса.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

8.2.1 Экран Edit Ethernet

С помощью этого экрана можно задать параметры назначения IP-адресов и настройки интерфейсов. Чтобы открыть этот экран, выберите нужный интерфейс и нажмите на пиктограмме **Edit** на экране **Ethernet**.

Примечание: Если объект IP-адреса создан на основе IP-адреса, маски подсети или шлюза определенного интерфейса, устройство NXC автоматически обновляет все правила и настройки, которые используют этот объект, при любом изменении настроек IP-адреса данного интерфейса. Например, если изменить IP-адрес локальной сети, устройство NXC автоматически внесет изменения в соответствующий объект адреса локальной подсети на основе интерфейса.

Рисунок 64 Экран Configuration > Network > Interface > Ethernet > Edit (general)

Поля этого экрана описаны в таблице ниже.

Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit

ПОЛЕ	ОПИСАНИЕ
IPv4/IPv6 View / IPv4 View / IPv6 View	С помощью этой кнопки можно вывести на экран поля настроек для протоколов IPv4 и IPv6, только для протокола IPv4 и только для протокола IPv6.
Show / Hide Advanced Settings	С помощью этой кнопки можно показать или скрыть на экране дополнительные поля настроек.
Create New Object	Используйте эту кнопку для создания объекта запроса DHCPv6, который можно использовать для работы с настройками DHCPv6 на этом экране.
General Settings	
Enable Interface	Установите этот переключатель, чтобы включить данный интерфейс. Снимите выделение переключателя, чтобы отключить данный интерфейс.
Interface Properties	
Interface Type	Выберите тип сети, к которой необходимо подключить этот интерфейс. В зависимости от выбранной опции – **internal** или **external** – меняется состав остальных опций, отображаемых на экране. Устройство NXC автоматически добавляет маршрут по умолчанию и настройки SNAT для трафика, который оно пересылает с внутренних интерфейсов на внешние; например, трафика, идущего из локальной сети в сеть WAN. Выберите опцию **internal**, чтобы подключиться к локальной сети. Другие соответствующие опции конфигурации: DHCP server и DHCP relay. Устройство NXC автоматически добавляет параметры SNAT по умолчанию для трафика, пересылаемого с этого интерфейса на внешний интерфейс. Выберите опцию **external**, чтобы подключиться ко внешней сети (например, сети Интернет). Если выбрать опцию **general**, то автоматическая перенастройка опций на остальной части экрана не произойдет, и необходимо будет вручную настроить политику для добавления правил маршрутизации и настроек SNAT для данного интерфейса.
Interface Name	Укажите в этом поле название интерфейса. Длина названия должна быть не более 11 символов, оно может содержать алфавитно-цифровые символы, символы дефиса и подчеркивания.
Port	Это поле указывает на порт, настройки которого редактируются в данный момент.
PVID	PVID (идентификатор сети VLAN порта) – это тег, которым помечаются входящие кадры без тегов, принимаемые портом, с тем, чтобы потом перенаправить эти кадры в группу VLAN, которую определяет данный тег. Выберите значение PVID для данного порта из диапазона (1~4094).
Zone	Выберите зону, с которой необходимо ассоциировать данный порт.
MAC Address	Это поле доступно только для чтения. В этом поле отображается MAC-адрес, который использует интерфейс Ethernet.
Description	Введите описание для данного интерфейса. Больше это поле нигде не используется. В тексте описания можно использовать алфавитно-цифровые символы, а также символы `()+/:=?!*#@$_%-`, длина описания не может быть больше 60 символов.
IP Address Assignment	Значения в этих полях определяют параметры IP-адреса на самом интерфейсе. Если изменить этот IP-адрес на данном интерфейсе, то вам, возможно, потребуется изменить связанный адресный объект для сети, подключенной к данному интерфейсу. К примеру, если поменять на этом экране IP-адрес интерфейса локальной сети, то необходимо будет также поменять адресный объект подсети соответствующей локальной сети.

Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Get Automatically	Эта опция появляется на экране в том случае, если выбрать в поле **Interface Type** опцию **external** или **general**. Установите этот переключатель, если необходимо сделать данный интерфейс DHCP-клиентом и автоматически получать IP-адрес, маску подсети и адрес шлюза с DHCP-сервера.
Use Fixed IP Address	Эта опция появляется на экране в том случае, если выбрать в поле **Interface Type** опцию **external** или **general**. Установите этот переключатель, если необходимо вручную указать IP-адрес, маску подсети и шлюз.
IP Address	Это поле становится доступным, если выбрать в поле **Interface Type** опцию **internal** или выбрать опцию **Use Fixed IP Address**. Введите IP-адрес для данного интерфейса.
Subnet Mask	Это поле становится доступным, если выбрать в поле **Interface Type** опцию **internal** или выбрать опцию **Use Fixed IP Address**. Введите маску подсети для данного интерфейса в точечно-десятичной нотации. Маска подсети указывает на то, какая часть IP-адреса является одинаковой для всех компьютеров в данной сети.
Gateway	Это поле становится доступным при выборе опции **Use Fixed IP Address**. Введите IP-адрес шлюза. Устройство NXC отправляет пакеты на шлюз в том случае, когда не знает, каким образом доставить пакет по адресу назначения. Шлюз должен принадлежать той же сети, что и интерфейс.
Metric	Это поле становится доступным, если выбрать в поле **Interface Type** опцию **external** или **general**, а также установить переключатель **Get Automatically**. Укажите приоритет шлюза (если таковой имеется) на данном интерфейсе. Устройство NXC решает, какой шлюз использовать исходя из приоритета. Чем меньше число, тем выше приоритет. Если два и более шлюзов имеют одинаковый приоритет, устройство NXC использует тот из них, который был сконфигурирован первым.
IPv6 Address Assignment	Значения в этих полях определяют параметры адреса IPv6 на самом интерфейсе.
Enable Stateless Address Auto-configuration (SLAAC)	Установите этот переключатель, чтобы включить функцию автоматической настройки параметров IPv6 на этом интерфейсе без сохранения состояния. Интерфейс самостоятельно сгенерирует адрес IPv6 на основе префикса, полученного от маршрутизатора IPv6 в сети.
Link-Local Address	Это поле показывает IPv6-адрес link-local и сетевой префикс, который устройство NXC самостоятельно генерирует для данного интерфейса.
IPv6 Address/ Prefix Length	Введите IPv6-адрес и длину префикса для данного интерфейса, если необходимо использовать статический IP-адрес. Данное поле является необязательным. Длина префикса определяет, какая часть IP-адреса (если смотреть слева) совпадает для всех компьютеров в данной сети, то есть является адресом сети.
Gateway	Введите IPv6-адрес исходящего шлюза по умолчанию с использованием шестнадцатеричной нотации и двоеточия (:) в качестве разделителя.
Metric	Укажите приоритет шлюза (если таковой имеется) на данном интерфейсе. Устройство NXC решает, какой шлюз использовать, исходя из приоритета. Чем меньше число, тем выше приоритет. Если два и более шлюзов имеют одинаковый приоритет, устройство NXC использует тот из них, который был сконфигурирован первым.
DHCPv6 Setting	
DHCPv6	Выберите опцию **N/A**, если использовать DHCPv6 не требуется. Выберите опцию **Client**, чтобы данный интерфейс выступал в качестве клиента DHCPv6.

Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
DUID	Это поле отображает идентификатор DUID (DHCP Unique IDentifier) данного интерфейса, который является уникальным и используется для идентификации интерфейса в процессе обмена сообщениями DHCPv6 с другими интерфейсами. Дополнительную информацию можно найти в прил. E на стр. 477.
DUID as MAC	Выберите эту опцию, чтобы устройство генерировало идентификатор DUID на основе MAC-адреса интерфейса по умолчанию.
Customized DUID	Если необходимо выбрать идентификатор DUID самостоятельно, введите его в этом поле.
Enable Rapid Commit	Выберите эту опцию, если необходимо сократить процесс обмена сообщениями DHCPv6 с четырех шагов до двух. Эта функция позволяет уменьшить высокую нагрузку, создаваемую сетевым трафиком. Примечание: Для того, чтобы функция быстрого подтверждения транзакций (rapid commit) работала, необходимо включить ее на сервере DHCPv6.
Request Address	Выберите эту опцию, если необходимо получать адрес IPv6 для этого интерфейса с DHCP-сервера. Снимите выделение с этого переключателя, чтобы отказаться от получения какой-либо информации об IP-адресе через DHCPv6.
DHCPv6 Request Options	Ели данный интерфейс является клиентом DHCPv6, то в этом разделе можно настроить параметры запросов DHCPv6, которые определяют объем дополнительной информации, получаемой с сервера DHCPv6.
Add	Нажмите эту кнопку, чтобы создать запись в таблице. Дополнительную информацию можно найти в разд. 8.2.3 на стр. 132.
Remove	Выберите требуемую запись и нажмите эту кнопку, чтобы удалить ее из таблицы.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись. Пример можно найти в разд. 8.2.2 на стр. 131.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
Name	Это поле отображает имя объекта запроса DHCPv6.
Type	Это поле показывает тип объекта.
Value	Это поле показывает IPv6-адрес, полученный устройством NXC от агрегирующего маршрутизатора.
Interface Parameters	
Egress Bandwidth	Укажите максимальный объем трафика (в килобитах в секунду), который устройство NXC может отправлять в сеть через этот интерфейс. Значения можно выбирать из диапазона от 0 до 1048576.
Ingress Bandwidth	Это поле зарезервировано для использования в будущем. Укажите максимальный объем трафика (в килобитах в секунду), который устройство NXC может принимать из сети через этот интерфейс. Значения можно выбирать из диапазона от 0 до 1048576.
MTU	Maximum Transmission Unit. Укажите максимальный размер каждого пакета данных (в байтах), который может перемещаться через этот интерфейс. Если на интерфейс приходит пакет большего размера, устройство NXC разбивает его на более мелкие фрагменты. Значения можно выбирать из диапазона от 576 до 1500. Обычно выбирают значение 1500.

Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connectivity Check	Эта группа полей появляется на экране, если выбрать в поле **Interface Type** опцию **External** или опцию **General**. Интерфейс может регулярно проверять доступность соединения с указанным шлюзом. Можно также указать, с какой периодичностью интерфейс должен проверять соединение, как долго следует ожидать ответа, прежде, чем расценить проверку как неудачную, и сколько неудачных попыток подряд должно произойти прежде, чем устройство NXC прекратит направлять трафик на этот шлюз. Устройство NXC возобновляет отправку трафика на указанный шлюз после первой удачной проверки доступности соединения.
Enable Connectivity Check	Выберите эту опцию, чтобы включить проверку доступности соединения.
Check Method	Выберите метод проверки, который можно использовать для данного шлюза. Выберите опцию **icmp**, чтобы устройство NXC регулярно отправляло пакеты типа ping на шлюз, чтобы убедиться в его доступности. Выберите опцию **tcp**, чтобы устройство NXC регулярно выполняло процедуру согласования параметров TCP (TCP handshake) со шлюзом, чтобы убедиться в его доступности.
Check Period	Укажите интервал опроса с целью проверки соединения (в секундах).
Check Timeout	Укажите, сколько должно длиться ожидание в секундах, прежде чем попытка проверки доступности соединения будет расценена как неудачная.
Check Fail Tolerance	Укажите, сколько неудачных попыток подряд должно совершить устройство NXC до того, как оно перестанет направлять трафик на этот шлюз.
Check Default Gateway	Выберите эту опцию, если необходимо проверять доступность шлюза по умолчанию.
Check this address	Выберите эту опцию, если необходимо проверять доступность определенного доменного имени или IP-адреса. В поле рядом введите имя домена или IP-адрес для проверки.
Check Port	Это поле отображается на экране только в том случае, если в поле **Check Method** выбрана опция **tcp**. Укажите номер порта, используемого при проверке соединения TCP.
DHCP Setting	Эти поля отображаются на экране в том случае, если в поле **Interface Type** выбраны опции **Internal** или **General**.
DHCP	Выберите тип службы DHCP, которую устройство NXC предоставляет сети. Возможные варианты: **None** – устройство NXC не предоставляет никаких служб DHCP. В сети уже есть DHCP-сервер. **DHCP-ретранслятор** – устройство NXC направляет DHCP-запросы на один или несколько указанных DHCP-серверов. DHCP-сервер (-ы) может(-гут) находиться в другой сети. **DHCP Server** – устройство NXC назначает IP-адреса, выдает маску подсети, адрес шлюза и информацию о DNS-серверах сетевым устройствам. В этом случае устройство NXC выполняет в сети функции DHCP-сервера.
	Эти поля появляются на экране, если выбрать для устройства NXC роль **DHCP Relay**.
Relay Server 1	Укажите IP-адрес DHCP-сервера в сети.
Relay Server 2	Данное поле является необязательным. Укажите IP-адрес другого DHCP-сервера в сети.
	Эти поля появятся на экране, если выбрать для устройства NXC роль **DHCP Server**.

Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Pool Start Address	Укажите IP-адрес, с которого устройство NXC начинает раздачу IP-адресов. Если необходимо назначить определенному компьютеру статический IP-адрес, выберите опцию **Static DHCP Table**. При отсутствии значения в этом поле поле **Pool Size** также необходимо оставить пустым. В этом случае устройство NXC может назначить каждый IP-адрес, разрешенный параметрами IP-адреса и маски подсети данного интерфейса, за исключением первого адреса (сетевого адреса), последнего адреса (широковещательного адреса) и IP-адреса самого интерфейса.
Pool Size	Укажите количество выделяемых IP-адресов. Значение в этом поле не может быть меньше единицы; верхний предел указываемого значения ограничен маской **Subnet Mask** подсети данного интерфейса. Например, если в поле **Subnet Mask** указано значение 255.255.255.0, а в поле **IP Pool Start Address** – значение 10.10.10.10, то устройство NXC может выделять адреса из диапазона от 10.10.10.10 до 10.10.10.254, то есть 245 IP-адресов. Если это поле пусто, то поле **IP Pool Start Address** также должно быть пустым. В этом случае устройство NXC может назначить каждый IP-адрес, разрешенный параметрами IP-адреса и маски подсети данного интерфейса, за исключением первого адреса (сетевого адреса), последнего адреса (широковещательного адреса) и IP-адреса самого интерфейса.
First DNS Server, Second DNS Server, Third DNS Server	Укажите IP-адреса DNS-сервером (не более трех), к которым могут обращаться DHCP-клиенты. Для этого можно воспользоваться следующими опциями. **Custom Defined** – укажите статический IP-адрес. **From ISP** – выберите DNS-сервер, сведения о котором другой интерфейс получил от своего DHCP-сервера. **EnterpriseWLAN** – DHCP-клиенты используют IP-адрес данного интерфейса, а устройство NXC выступает в качестве DNS-ретранслятора.
First WINS Server, Second WINS Server	Укажите IP-адрес сервера WINS (Windows Internet Naming Service), который необходимо рассылать DHCP-клиентам. Сервер WINS хранит таблицу соответствий имен компьютеров в сети и IP-адресов, назначенных им на текущий момент.
Default Router	Если решено использовать этот интерфейс в роли **DHCP-сервера**, можно либо выбрать **gex IP** (где x – номер интерфейса) в качестве IP-адреса интерфейса, либо использовать другой IP-адрес в качестве адреса маршрутизатора по умолчанию. Маршрутизатор по умолчанию станет шлюзом по умолчанию для DHCP-клиентов. Чтобы использовать другой IP-адрес в качестве маршрутизатора по умолчанию, выберите опцию **Custom Defined** и введите нужный IP-адрес.
Lease time	Укажите, в течение какого времени каждый компьютер может использовать эту информацию (особенно IP-адрес), прежде, чем запросить ее снова. Возможные варианты: **infinite** – срок действия IP-адресов бесконечен. **days** (дней), **hours** (часов) и **minutes** (минут) – выберите вариант и укажите, как долго длится аренда IP-адресов.
Extended Options	Эта таблица становится доступной, если данное устройство будет использоваться в качестве DHCP-сервера (**DHCP server**). Настройте параметры в этой таблице, если необходимо посылать дополнительную информацию DHCP-клиентам через пакеты DHCP.
Add	Нажмите эту кнопку, чтобы создать запись в таблице. См. разд. 8.2.4 на стр. 132.
Edit	Выберите нужную запись в таблице и нажмите эту кнопку, чтобы изменить ее.
Remove	Выберите нужную запись в таблице и нажмите эту кнопку, чтобы удалить ее.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.

Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name	Это название опции DHCP.
Code	Это кодовый номер опции DHCP.
Type	Это тип значения, задаваемого для данной опции DHCP.
Value	Это значение, задаваемое для опции DHCP.
Enable IP/MAC Binding	Выберите эту опцию, чтобы данный интерфейс в обязательном порядке устанавливал связь между определенными IP-адресами и определенными MAC-адресами. Это позволит исключить возможность ручной привязки связанного IP-адреса к другому устройству, подключенному к данному интерфейсу. Воспользуйтесь этой опцией, если необходимо разрешить использование определенных IP-адресов только определенным пользователям.
Enable Logs for IP/MAC Binding Violation	При выборе этой опции устройство NXC будет генерировать сообщение в журнале каждый раз, когда устройство, подключенное к данному интерфейсу, попытается использовать IP-адрес, привязанный к MAC-адресу другого устройства.
Static DHCP Table	Создайте список статических IP-адресов, которые устройство NXC назначит компьютерам, подключенным к данному интерфейсу. В противном случае устройство NXC выберет динамические IP-адреса, используя значения, указанные в полях **IP Pool Start Address** и **Pool Size** для данного интерфейса.
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Выберите нужную запись и нажмите эту кнопку, чтобы изменить ее.
Remove	Выберите нужную запись и нажмите эту кнопку, чтобы удалить ее.
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
IP-адрес	Введите IP-адрес, который необходимо назначить устройству с MAC-адресом, указанным в этой записи.
MAC	Введите MAC-адрес, который необходимо связать с IP-адресом, указанным в этой записи.
Description	Введите описание, которое поможет идентифицировать эту статическую запись DHCP. В тексте описания можно использовать алфавитно-цифровые символы, а также символы `()+/:=?!*#@$_%-`, длина описания не может быть больше 60 символов.
MAC Address Setting	Эта группа полей появляется на экране, если выбрать в поле **Interface Type** опцию **External** или опцию **General**. Данный интерфейс может использовать заводской MAC-адрес, установленный по умолчанию, MAC-адрес, указанный вручную или MAC-адрес, склонированный с другого компьютера или устройства.
Use Default MAC Address	При выборе этой опции данный интерфейс будет использовать заводской MAC-адрес, назначенный ему по умолчанию. По умолчанию устройство NXC использует для собственной идентификации именно MAC-адрес, установленный на заводе-изготовителе.
Overwrite Default MAC Address	Эта опция позволяет выбрать для данного интерфейса другой MAC-адрес. Можно либо ввести MAC-адрес в соответствующих полях, либо нажать кнопку **Clone by host** и указать IP-адрес устройства или компьютера, чей MAC-адрес необходимо склонировать. В случае успешной настройки этот адрес будет скопирован в файл конфигурации. Он не изменится до тех пор, пока не будет изменено значение этого параметра или на устройство не будет выгружен новый файл конфигурации.
Related Setting	

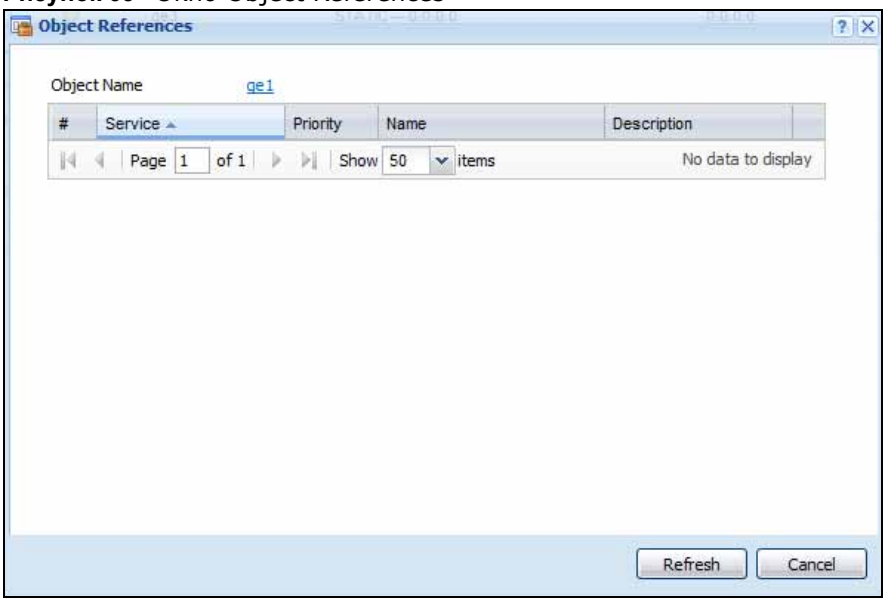
Таблица 60 Экран Configuration > Network > Interface > Ethernet > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Configure Policy Route	Щелкните по ссылке **Policy Route**, чтобы перейти на экран настройки маршрутов на основе политик, с помощью которого можно вручную ассоциировать трафик с данным интерфейсом. Чтобы добавить параметры маршрутизации и настройки SNAT для интерфейса, в настройках которого в поле **Interface Type** выбрана опция **General**, необходимо вручную настроить маршруты на основе политик. Кроме того, можно настроить маршруты на основе политик, заменяющие правила маршрутизации и алгоритмы SNAT по умолчанию для интерфейса, в настройках которого в поле **Interface Type** выбрана опция **Internal** или **External**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

8.2.2 Экран Object References

Если на экране настроек присутствует пиктограмма **Object Reference**, выберите объект конфигурации и нажмите на пиктограмме **Object Reference**, чтобы открыть экран **Object References**. На экране появятся параметры конфигурации, которые ссылаются на выбранный объект. Перечень отображаемых полей зависит от типа объекта.

Рисунок 65 Окно Object References



В приведенной ниже таблице описаны все поля, которые могут появиться на этом экране.

Таблица 61 Окно Object Reference

ПОЛЕ	ОПИСАНИЕ
Object Name	В этом поле приводится идентификатор объекта, который задействован в отображаемых настройках конфигурации. Нажатие на имя объекта позволяет отобразить экран настройки объекта в основном окне.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
Service	Обозначает тип настройки, которая ссылается на выбранный объект. Нажатие на имени службы позволяет отобразить экран настройки службы в основном окне.

Таблица 61 Окно Object Reference (продолжение)

ПОЛЕ	ОПИСАНИЕ
Priority	В данном поле отображается, если это применимо, позиция в списке элемента конфигурации, ссылающегося на объект; в противном случае в этом поле отображается **N/A**.
Name	В данном поле отображается идентификатор элемента конфигурации, ссылающегося на объект.
Description	Если для ссылающегося на объект элемента конфигурации имеется описание, оно отображается в этом поле.
Refresh	Нажатие на эту ссылку позволяет обновить информацию на данном экране.
Cancel	Нажатие на **Cancel** позволяет закрыть окно.

8.2.3 Экран Add DHCPv6 Request Options

В процессе настройки интерфейса в качестве DHCPv6-клиента можно добавить опции DHCPv6-запросов, благодаря которым устройство NXC будет помещать дополнительную информацию в DHCPv6-пакеты. Чтобы перейти к этому экрану. выберите в меню **Configuration > Network > Interface > Ethernet > Edit**, выберите в поле **DHCPv6** опцию **Client** в разделе **DHCPv6 Setting**, а затем нажмите кнопку **Add** в таблице **DHCPv6 Request Options**.

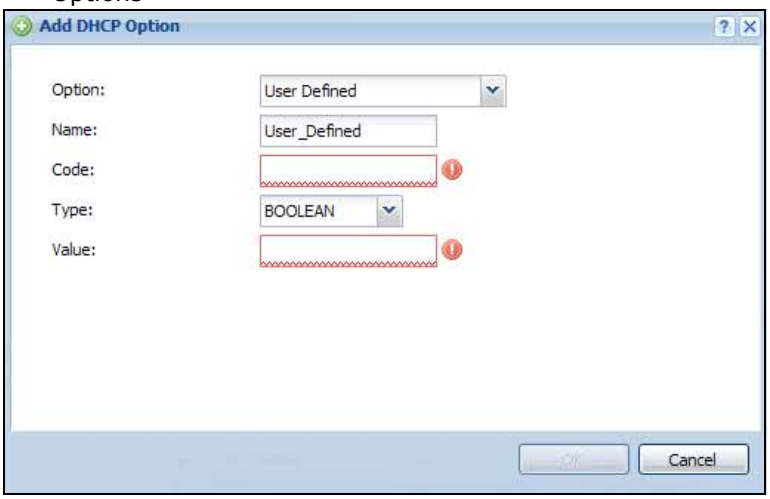
Выберите объект DHCPv6-запроса в поле **Select one object** и нажмите кнопку **OK**, чтобы сохранить его. Нажмите кнопку **Cancel**, чтобы выйти без сохранения изменений.

Рисунок 66 Экран Configuration > Network > Interface > Ethernet > Edit > Add DHCPv6 Request Options

8.2.4 Экран Add/Edit DHCP Extended Options

В процессе настройки интерфейса в качестве DHCPv4-сервера можно добавить расширенные опции DHCP, благодаря которым устройство NXC будет помещать дополнительную информацию в DHCP-пакеты. Доступные поля будут зависеть от типа DHCP-опции, выбранной на экране. Чтобы перейти к этому экрану, выберите в меню **Configuration > Network > Interface > Ethernet > Edit**, выберите опцию **DHCP Server** в разделе **DHCP Setting**, а затем нажмите кнопку **Add** или кнопку **Edit** в таблице **Extended Options**.

Рисунок 67 Экран Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options



В приведенной ниже таблице описаны все поля, которые могут появиться на этом экране.

Таблица 62 Экран Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

ПОЛЕ	ОПИСАНИЕ
Option	Выберите опцию DHCP, которую необходимо добавлять в DHCP-пакеты, посылаемые через этот интерфейс. Дополнительную информацию можно найти в табл. 63 на стр. 134.
Name	Это поле отображает название выбранной опции DHCP. Если в поле **Option** выбрана опция **User Defined**, введите имя-описание для идентификации опции DHCP. Длина имени может составлять не более 16 символов («a-z», «A-Z», «0-9», «-» и «_»), использование пробелов не допускается. Первым в имени должен идти алфавитный символ (a-z, A-Z).
Code	Это поле отображает кодовый номер выбранной опции DHCP. Если в поле Option выбрана опция User Defined, введите номер для этой опции. Это поле является обязательным для заполнения.
Type	Это поле указывает на тип выбранной опции DHCP. Если в поле Option выбрана опция User Defined, выберите соответствующий тип для значения, которое будет введено в следующем поле. Менять значение в поле **User Defined** рекомендуется только опытным пользователям. Неправильно выбранное значение может повлечь блокировку интерфейса.
Value	Введите значение для выбранной опции DHCP. Например, если выбрана опция **TFTP Server Name (66)** и в качестве типа значения указано **TEXT**, в этом поле следует ввести доменное имя TFTP-сервера в DNS. Это поле является обязательным для заполнения.
First IP Address, Second IP Address, Third IP Address	При выборе опций **Time Server (4)**, **NTP Server (42)**, **SIP Server (120)**, **CAPWAP AC (138)** и **TFTP Server (150)** необходимо будет указать в соответствующих полях как минимум один из IP-адресов данных серверов. Серверы должны быть перечислены в списке в порядке предпочтений.
First Enterprise ID, Second Enterprise ID	При выборе одной из опций **VIVC (124)** или **VIVS (125)** необходимо будет ввести 32-разрядный корпоративный номер хотя бы одного производителя в этих полях. Корпоративный номер – это номер, который уникальным образом идентифицирует компанию.
First Class, Second Class	Если выбрана опция **VIVC (124)**, введите сведения об аппаратной конфигурации хоста, на котором работает клиент, или данные о совместимости с нормами отраслевого консорциума.

Таблица 62 Экран Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options (продолжение)

ПОЛЕ	ОПИСАНИЕ
First Information, Second Information	Если выбрана опция **VIVS (125)**, введите в этих полях дополнительную информацию для соответствующего корпоративного номера.
OK	Нажмите эту кнопку, чтобы закрыть экран и обновить значения параметров на предыдущем экране Edit.
Cancel	Нажатие на **Cancel** позволяет закрыть окно.

В таблице ниже приведены все доступные на устройстве NXC дополнительные опции DHCP (описанные в документах RFC). Более подробную информацию можно найти в документах RFC.

Таблица 63 Дополнительные опции DHCP

НАЗВАНИЕ ОПЦИИ	КОД	ОПИСАНИЕ
Time Offset	2	Эта опция описывает временной сдвиг (в секундах) в клиентской подсети относительно часового пояса UTC (Coordinated Universal Time, всеобщее скоординированное время).
Time Server	4	Эта опция описывает список серверов точного времени, доступных клиенту.
NTP Server	42	Эта опция описывает список NTP-серверов, доступных клиенту по IP-адресу.
TFTP Server Name	66	Эту опцию используют для идентификации TFTP-сервера, если поле «sname» в заголовке DHCP задействовано для опций DHCP. Значение не может быть пустым, минимум один символ.
Bootfile	67	Эту опцию используют для идентификации файла загрузки, если поле «file» в заголовке DHCP задействовано для опций DHCP. Значение не может быть пустым, минимум один символ.
SIP Server	120	Эта опция содержит либо адрес IPv4, либо доменное имя в DNS, по которому SIP-клиент будет искать SIP-сервер.
VIVC	124	Опция идентификации производителя по его классу (Vendor-Identifying Vendor Class) С помощью этой опции DHCP-клиент может однозначно идентифицировать производителя аппаратного обеспечения, на котором работает клиент, используемое программное обеспечение и программный консорциум, к которому принадлежит производитель.
VIVS	125	Характерная для производителя опция его идентификации (Vendor-Identifying Vendor-Specific Option) С помощью этой опции DHCP-клиенты и серверы могут обмениваться характерной для определенных производителей информацией.

Таблица 63 Дополнительные опции DHCP (продолжение)

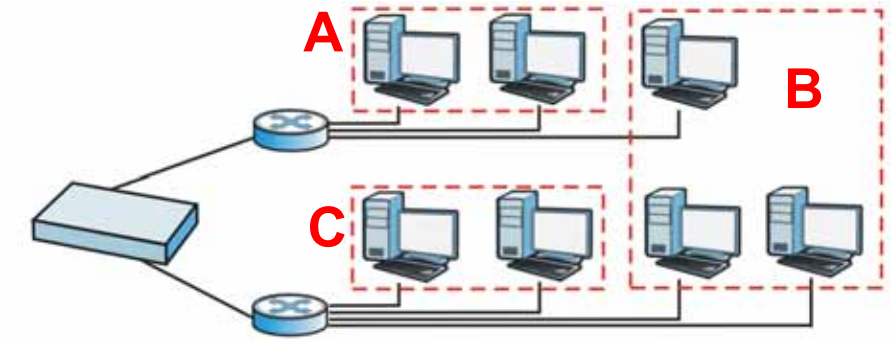
НАЗВАНИЕ ОПЦИИ	КОД	ОПИСАНИЕ
CAPWAP AC	138	Опция адресов контроллера доступа CAPWAP Протокол CAPWAP (Control And Provisioning of Wireless Access Points Protocol, протокол управления и конфигурирования беспроводных точек доступа позволяет точкам WTP (Wireless Termination Point, точка терминирования в беспроводной сети) использовать DHCP для обнаружения контроллеров доступа, к которым можно подключиться. Эта опция переносит список адресов IPv4, указывая на то, что один или более контроллеров доступа CAPWAP доступны данной точке WTP.
TFTP Server	150	Эта опция содержит один или более адресов IPv4, которые доступны клиенту для использования. В настоящее время эта опция используется для загрузки конфигурации с VoIP-сервера по протоколу TFTP; однако ее можно использовать и для иных целей, кроме связи с сервером конфигурации VoIP.

8.3 Интерфейсы VLAN

Виртуальные локальные сети (Virtual Local Area Network, VLAN) разделяют физическую сеть на несколько логических сетей. Этот стандарт описан в документе IEEE 802.1q.

Примечание: По умолчанию устройство NXC выполняет функции моста. Это означает, что все интерфейсы (ge1~g6) объединены в группу с одним идентификатором VID, то есть приписаны к одной локальной сети vlan0. Обратите внимание, что сеть vlan0 нельзя удалить, а ее идентификатор VID нельзя изменить.

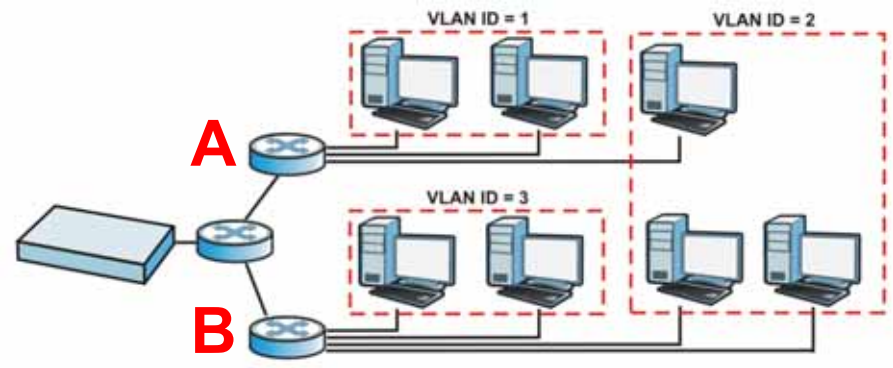
Рисунок 68 Пример: До внедрения VLAN



В данном примере рассматриваются две физических сети и три отдела – **A**, **B** и **C**. Физические сети подключены к концентраторам, а концентраторы – к маршрутизатору.

Можно разделить указанные физические сети на три виртуальных локальных сети – VLAN.

Рисунок 69 Пример: После внедрения VLAN



Каждая VLAN представляет собой отдельную сеть со своими IP-адресами, масками подсетей и шлюзами. Каждая сеть VLAN имеет уникальный идентификационный номер (ID). Этот идентификатор представляет собой 12-разрядное значение, которое хранится в заголовке MAC. Сети VLAN подключены к коммутаторам, а коммутаторы подключены к маршрутизатору. (Если на одном коммутаторе достаточно портов для подключения всех сетевых устройств, то для такой сети не нужны два коммутатора – **A** и **B**).

- Трафик внутри каждой сети VLAN является коммуникацией второго уровня (канальный уровень, MAC-адреса). За его обработку отвечают коммутаторы. Таким образом, для обработки трафика внутри сети VLAN 2 необходим еще один коммутатор. Широковещательная передача трафика осуществляется не внутри каждой физической сети, а внутри каждой сети VLAN.
- Трафик между сетями VLAN (или между сетью VLAN и сетью другого типа) является коммуникацией третьего уровня (сетевой уровень, IP-адреса). Его обрабатывает маршрутизатор.

Такой подход имеет несколько преимуществ.

- Увеличение производительности – дополнительный коммутатор должен маршрутизировать трафик в сети VLAN 2 между компьютерами сотрудников отдела продаж быстрее, чем это делает маршрутизатор. Кроме того, широковещательные передачи ограничены более мелкими и логически обособленными группами пользователей.
- Повышение уровня безопасности – если каждый компьютер имеет отдельное физическое подключение к коммутатору, то широковещательный трафик из одной сети VLAN никогда не попадет на компьютеры, находящиеся в другой сети VLAN.
- Улучшение управляемости – появляется возможность более точного применения сетевых политик к пользователям. Например, можно создать собственные правила на основе политик для каждой сети VLAN (то есть для каждого отдела в примере, описанном выше) и установить различную пропускную способность для каждой сети VLAN. Эти правила не зависят от конфигурации физической сети, поэтому ее можно будет менять, не затрагивая политики.

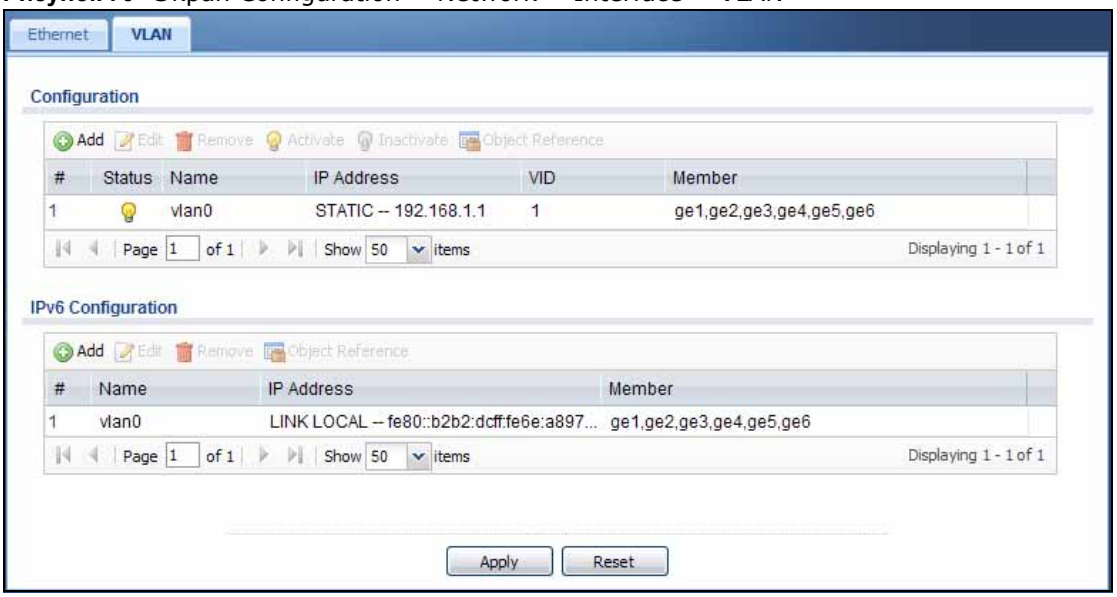
В приведенном примере новый коммутатор обрабатывает следующие типы трафика:

- Внутри VLAN 2.
- Между маршрутизатором и VLAN 1.
- Между маршрутизатором и VLAN 2.
- Между маршрутизатором и VLAN 3.

8.3.1 Сводный экран VLAN

На этом экране присутствует список всех интерфейсов VLAN. Если на экране **Configuration > System > IPv6** включена поддержка протокола IPv6, то на этом экране также можно будет настроить параметры интерфейсов VLAN, используемых сетями IPv6. Чтобы открыть этот экран, выберите в меню **Configuration > Network > Interface** > **VLAN**.

Рисунок 70 Экран Configuration > Network > Interface > VLAN



Описание каждого из полей приведено в таблице ниже.

Таблица 64 Экран Configuration > Network > Interface > VLAN

ПОЛЕ	ОПИСАНИЕ
Configuration/ IPv6 Configuration	С помощью раздела **Configuration** можно настроить параметры протокола IPv4. С помощью раздела **IPv6 Configuration** можно настроить параметры протокола IPv6, если устройство NXC подключается к сети IPv6. В обоих разделах присутствуют схожие поля, которые описаны ниже.
Add	Нажмите эту кнопку, чтобы создать новую сеть VLAN.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо интерфейсом.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Name	В этом поле отображается наименование данного интерфейса.

Таблица 64 Экран Configuration > Network > Interface > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Address	В этом поле отображается текущий IP-адрес интерфейса. если в поле IP-адреса отображается значение 0.0.0.0 (в сети IPv4) или значение :: (в сети IPv6), то это означает, что IP-адрес интерфейсу еще не назначен. Для сети IPv4 на этом экране также присутствуют сведения о том, является ли данный IP-адрес статическим (**STATIC**) или динамическим (**DHCP**). Для сети IPv6 этот экран показывает еще и информацию о том, является ли IP-адрес статическим (STATIC), относящимся к локальному соединению (LINK LOCAL), динамически назначенным (DHCP) или IP-адресом IPv6 SLAAC (StateLess Address AutoConfiguration). Дополнительную информацию об IPv6 можно найти в прил. E на стр. 477.
VID	Это поле отображает идентификатор сети VLAN (VLAN ID).
Member	Это поле отображает интерфейсы Ethernet, которые входят в данную сеть VLAN.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

8.3.2 Экран Add/Edit VLAN

С помощью этого экрана можно настроить параметры назначения IP-адресов, полосы пропускания интерфейсов, параметры DHCP и проверки доступности соединений для каждого интерфейса VLAN. Чтобы открыть этот экран, нажмите на пиктограмму **Add** вверху столбца **Add** или на пиктограмму **Edit** рядом с соответствующим интерфейсом VLAN на экране **VLAN Summary**. Появится следующий экран.

Рисунок 71 Экран Configuration > Network > Interface > VLAN > Add/Edit

Описание каждого из полей приведено в таблице ниже.

Таблица 65 Экран Configuration > Network > Interface > VLAN > Add/Edit

ПОЛЕ	ОПИСАНИЕ
IPv4/IPv6 View / IPv4 View / IPv6 View	С помощью этой кнопки можно вывести на экран поля настроек для протоколов IPv4 и IPv6, только для протокола IPv4 и только для протокола IPv6.
Show / Hide Advanced Settings	С помощью этой кнопки можно показать или скрыть на экране дополнительные поля настроек.
Create New Object	Используйте эту кнопку для создания объекта запроса DHCPv6, который можно использовать для работы с настройками DHCPv6 на этом экране.
General Settings	
Enable	Установить этот переключатель, чтобы включить данный интерфейс. Снимите выделение переключателя, чтобы отключить данный интерфейс.
Interface Properties	
Interface Name	При изменении настроек существующего интерфейса VLAN это поле доступно только для чтения. Введите номер интерфейса VLAN. Номер можно выбрать из диапазона от 0 до 4094. Например, vlan0, vlan8 и т.д.
VID	Введите идентификатор сети VLAN (VLAN ID). Это 12-разрядное число уникальным образом идентифицирует каждую сеть VLAN. Допустимые значения выбираются из диапазона от 1 до 4094. (значения 0 и 4095 зарезервированы)
Zone	Выберите зону, к которой принадлежит данный интерфейс VLAN.
Description	Введите описание для данного интерфейса. Больше это поле нигде не используется. В тексте описания можно использовать алфавитно-цифровые символы, а также символы `()+/:=?!*#@$_%-`, длина описания не может быть больше 60 символов.
Member Configuration	С помощью настроек этой группы можно назначить интерфейсы участниками данной сети VLAN.
Edit	Нажмите эту кнопку, чтобы изменить параметры участия выбранного интерфейса в сети VLAN.
#	Это поле содержит последовательный указатель номера интерфейса.
Port Name	Это поле показывает имя интерфейса.
Member	Это поле указывает на то, является ли выбранный интерфейс участником сети VLAN, параметры которой редактируются в настоящий момент. Щелкните по этому полю, чтобы изменить значение в нем.
Tx Tagging	Это поле указывает на то, помечает ли выбранный интерфейс исходящий трафик тегами, содержащими идентификатор этой сети VLAN. Щелкните по этому полю, чтобы изменить значение в нем.
IP Address Assignment	
Get Automatically	Укажите, является ли данный интерфейс DHCP-клиентом. При выборе этой опции DHCP-сервер автоматически назначает данному интерфейсу IP-адрес, маску подсети и шлюз.
Use Fixed IP Address	Установите этот переключатель, если необходимо вручную указать IP-адрес, маску подсети и шлюз.
IP Address	Это поле становится доступным при выборе опции **Use Fixed IP Address**. Введите IP-адрес для данного интерфейса.

Таблица 65 Экран Configuration > Network > Interface > VLAN > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subnet Mask	Это поле становится доступным при выборе опции **Use Fixed IP Address**. Введите маску подсети для данного интерфейса в точечно-десятичной нотации. Маска подсети указывает на то, какая часть IP-адреса является одинаковой для всех компьютеров в данной сети.
Gateway	Это поле становится доступным при выборе опции **Use Fixed IP Address**. Введите IP-адрес шлюза. Устройство NXC отправляет пакеты на шлюз в том случае, когда не знает, каким образом доставить пакет по адресу назначения. Шлюз должен принадлежать той же сети, что и интерфейс.
Metric	Укажите приоритет шлюза (если таковой имеется) на данном интерфейсе. Устройство NXC решает, какой шлюз использовать исходя из приоритета. Чем меньше число, тем выше приоритет. Если два и более шлюзов имеют одинаковый приоритет, устройство NXC использует тот из них, который был сконфигурирован первым.
IPv6 Address Assignment	Значения в этих полях определяют параметры адреса IPv6 на самом интерфейсе.
Enable Stateless Address Auto-configuration (SLAAC)	Установите этот переключатель, чтобы включить функцию автоматической настройки параметров IPv6 на этом интерфейсе без сохранения состояния. Интерфейс самостоятельно сгенерирует адрес IPv6 на основе префикса, полученного от маршрутизатора IPv6 в сети.
Link-Local Address	Это поле показывает IPv6-адрес link-local и сетевой префикс, который устройство NXC самостоятельно генерирует для данного интерфейса.
IPv6 Address/ Prefix Length	Введите IPv6-адрес и длину префикса для данного интерфейса, если необходимо использовать статический IP-адрес. Данное поле является необязательным. Длина префикса определяет, какая часть IP-адреса (если смотреть слева) совпадает для всех компьютеров в данной сети, то есть является адресом сети.
Gateway	Введите IPv6-адрес исходящего шлюза по умолчанию с использованием шестнадцатеричной нотации и двоеточия (:) в качестве разделителя.
Metric	Укажите приоритет шлюза (если таковой имеется) на данном интерфейсе. Устройство NXC решает, какой шлюз использовать исходя из приоритета. Чем меньше число, тем выше приоритет. Если два и более шлюзов имеют одинаковый приоритет, устройство NXC использует тот из них, который был сконфигурирован первым.
DHCPv6 Setting	
DHCPv6	Выберите опцию **N/A**, если использовать DHCPv6 не требуется. Выберите опцию **Client**, чтобы данный интерфейс выступал в качестве клиента DHCPv6.
DUID	Это поле отображает идентификатор DUID (DHCP Unique IDentifier) данного интерфейса, который является уникальным и используется для идентификации интерфейса в процессе обмена сообщениями DHCPv6 с другими интерфейсами. Дополнительную информацию можно найти в прил. E на стр. 477.
DUID as MAC	Выберите эту опцию, чтобы устройство генерировало идентификатор DUID на основе MAC-адреса интерфейса по умолчанию.
Customized DUID	Если необходимо выбрать идентификатор DUID самостоятельно, введите его в этом поле.
Enable Rapid Commit	Выберите эту опцию, если необходимо сократить процесс обмена сообщениями DHCPv6 с четырех шагов до двух. Эта функция позволяет уменьшить высокую нагрузку, создаваемую сетевым трафиком. Примечание: Для того, чтобы функция быстрого подтверждения транзакций (rapid commit) работала, необходимо включить ее на сервере DHCPv6.

Таблица 65 Экран Configuration > Network > Interface > VLAN > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Request Address	Выберите эту опцию, если необходимо получать адрес IPv6 для этого интерфейса с DHCP-сервера. Снимите выделение с этого переключателя, чтобы отказаться от получения какой-либо информации об IP-адресе через DHCPv6.
DHCPv6 Request Options	Ели данный интерфейс является клиентом DHCPv6, то в этом разделе можно настроить параметры запросов DHCPv6, которые определяют объем дополнительной информации, получаемой с сервера DHCPv6.
Add	Нажмите эту кнопку, чтобы создать запись в таблице. Дополнительную информацию можно найти в разд. 8.2.3 на стр. 132.
Remove	Выберите требуемую запись и нажмите эту кнопку, чтобы удалить ее из таблицы.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись. Пример можно найти в разд. 8.2.2 на стр. 131.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
Name	Это поле отображает имя объекта запроса DHCPv6.
Type	Это поле показывает тип объекта.
Value	Это поле показывает IPv6-адрес, полученный устройством NXC от агрегирующего маршрутизатора.
Interface Parameters	
Egress Bandwidth	Укажите максимальный объем трафика (в килобитах в секунду), который устройство NXC может отправлять в сеть через этот интерфейс. Значения можно выбирать из диапазона от 0 до 1048576.
Ingress Bandwidth	Это поле зарезервировано для использования в будущем. Укажите максимальный объем трафика (в килобитах в секунду), который устройство NXC может принимать из сети через этот интерфейс. Значения можно выбирать из диапазона от 0 до 1048576.
MTU	Maximum Transmission Unit. Укажите максимальный размер каждого пакета данных (в байтах), который может перемещаться через этот интерфейс. Если на интерфейс приходит пакет большего размера, устройство NXC разбивает его на более мелкие фрагменты. Значения можно выбирать из диапазона от 576 до 1500. Обычно выбирают значение 1500.
DHCP Setting	
DHCP	Выберите тип службы DHCP, которую устройство NXC предоставляет сети. Возможные варианты: **None** – устройство NXC не предоставляет никаких служб DHCP. В сети уже есть DHCP-сервер. **DHCP Relay** – устройство NXC направляет DHCP-запросы на один или несколько указанных DHCP-серверов. DHCP-сервер (-ы) может(-гут) находиться в другой сети. **DHCP Server** – устройство NXC назначает IP-адреса, выдает маску подсети, адрес шлюза и информацию о DNS-серверах сетевым устройствам. В этом случае устройство NXC выполняет в сети функции DHCP-сервера.
	Эти поля появляются на экране, если выбрать для устройства NXC роль **DHCP Relay**.
Relay Server 1	Укажите IP-адрес DHCP-сервера в сети.
Relay Server 2	Данное поле является необязательным. Укажите IP-адрес другого DHCP-сервера в сети.
	Эти поля появятся на экране, если выбрать для устройства NXC роль **DHCP Server**.

Таблица 65 Экран Configuration > Network > Interface > VLAN > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Pool Start Address	Укажите IP-адрес, с которого устройство NXC начинает раздачу IP-адресов. Если необходимо назначить определенному компьютеру статический IP-адрес, нажмите кнопку **Add Static DHCP**. При отсутствии значения в этом поле поле **Pool Size** также необходимо оставить пустым. В этом случае устройство NXC может назначить каждый IP-адрес, разрешенный параметрами IP-адреса и маски подсети данного интерфейса, за исключением первого адреса (сетевого адреса), последнего адреса (широковещательного адреса) и IP-адреса самого интерфейса.
Pool Size	Укажите количество выделяемых IP-адресов. Значение в этом поле не может быть меньше единицы; верхний предел указываемого значения ограничен маской **Subnet Mask** подсети данного интерфейса. Например, если в поле **Subnet Mask** указано значение 255.255.255.0, а в поле **IP Pool Start Address** – значение 10.10.10.10, то устройство NXC может выделять адреса из диапазона от 10.10.10.10 до 10.10.10.254, то есть 245 IP-адресов. Если это поле пусто, то поле **IP Pool Start Address** также должно быть пустым. В этом случае устройство NXC может назначить каждый IP-адрес, разрешенный параметрами IP-адреса и маски подсети данного интерфейса, за исключением первого адреса (сетевого адреса), последнего адреса (широковещательного адреса) и IP-адреса самого интерфейса.
First DNS Server Second DNS Server Third DNS Server	Укажите IP-адреса DNS-сервером (не более трех), к которым могут обращаться DHCP-клиенты. Для этого можно воспользоваться следующими опциями. **Custom Defined** – укажите статический IP-адрес. **From ISP** – выберите DNS-сервер, сведения о котором другой интерфейс получил от своего DHCP-сервера. **EnterpriseWLAN** – DHCP-клиенты используют IP-адрес данного интерфейса, а устройство NXC выступает в качестве DNS-ретранслятора.
First WINS Server, Second WINS Server	Укажите IP-адрес сервера WINS (Windows Internet Naming Service), который необходимо рассылать DHCP-клиентам. Сервер WINS хранит таблицу соответствий имен компьютеров в сети и IP-адресов, назначенных им на текущий момент.
Lease time	Укажите, в течение какого времени каждый компьютер может использовать эту информацию (особенно IP-адрес), прежде, чем запросить ее снова. Возможные варианты: **infinite** – срок действия IP-адресов бесконечен **days** (дней), **hours** (часов) и **minutes** (минут) – выберите вариант и укажите, как долго длится аренда IP-адресов.
Enable IP/MAC Binding	Выберите эту опцию, чтобы устройство NXC в обязательном порядке устанавливало связь между определенными IP-адресами и определенными MAC-адресами для данной сети VLAN. Это позволит исключить возможность ручной привязки связанного IP-адреса к другому устройству, подключенному к данному интерфейсу. Воспользуйтесь этой опцией, если необходимо разрешить использование определенных IP-адресов только определенным пользователям.
Enable Logs for IP/MAC Binding Violation	При выборе этой опции устройство NXC будет генерировать сообщение в журнале каждый раз, когда устройство, подключенное к данной сети VLAN, попытается использовать IP-адрес, привязанный к MAC-адресу другого устройства.
Static DHCP Table	Создайте список статических IP-адресов, которые устройство NXC назначит компьютерам, подключенным к данному интерфейсу. В противном случае устройство NXC выберет динамические IP-адреса, используя значения, указанные в полях **IP Pool Start Address** и **Pool Size** для данного интерфейса.
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Выберите нужную запись и нажмите эту кнопку, чтобы изменить ее.
Remove	Выберите нужную запись и нажмите эту кнопку, чтобы удалить ее.

Таблица 65 Экран Configuration > Network > Interface > VLAN > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
IP Address	Введите IP-адрес, который необходимо назначить устройству с MAC-адресом, указанным в этой записи.
MAC Address	Введите MAC-адрес, который необходимо связать с IP-адресом, указанным в этой записи.
Description	Введите описание, которое поможет идентифицировать эту статическую запись DHCP. В тексте описания можно использовать алфавитно-цифровые символы, а также символы `()+/:=?!*#@$_%-`, длина описания не может быть больше 60 символов.
Connectivity Check	Устройство NXC может регулярно проверять доступность соединения с указанным шлюзом. Можно также указать, с какой периодичностью необходимо проверять соединение, как долго следует ожидать ответа, прежде, чем расценить проверку как неудачную, и сколько неудачных попыток подряд должно произойти прежде, чем устройство NXC прекратит направлять трафик на этот шлюз. Устройство NXC возобновляет отправку трафика на указанный шлюз после первой удачной проверки доступности соединения.
Enable Connectivity Check	Выберите эту опцию, чтобы включить проверку доступности соединения.
Check Method	Выберите метод проверки, который можно использовать для данного шлюза. Выберите опцию **icmp**, чтобы устройство NXC регулярно отправляло пакеты типа ping на шлюз, чтобы убедиться в его доступности. Выберите опцию **tcp**, чтобы устройство NXC регулярно выполняло процедуру согласования параметров TCP (TCP handshake) со шлюзом, чтобы убедиться в его доступности.
Check Period	Укажите интервал опроса с целью проверки соединения (в секундах).
Check Timeout	Укажите, сколько должно длиться ожидание в секундах, прежде чем попытка проверки доступности соединения будет расценена как неудачная.
Check Fail Tolerance	Укажите, сколько неудачных попыток подряд должно совершить устройство NXC до того, как оно перестанет направлять трафик на этот шлюз.
Check Default Gateway	Выберите эту опцию, если необходимо проверять доступность шлюза по умолчанию.
Check this address	Выберите эту опцию, если необходимо проверять доступность определенного доменного имени или IP-адреса. В поле рядом введите имя домена или IP-адрес для проверки.
Check Port	Это поле отображается на экране только в том случае, если в поле **Check Method** выбрана опция **tcp**. Укажите номер порта, используемого при проверке соединения TCP.
Related Setting	
Configure Policy Route	Щелкните по ссылке **Policy Route**, чтобы перейти на экран, на котором можно вручную создать маршрут на основе политик для ассоциации трафика с данной сетью VLAN.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

8.4 Справочная техническая информация

В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

Назначение IP-адресов

Большинство интерфейсов имеют IP-адрес и маску подсети. Эту информацию используют при создании записей в таблице маршрутизации.

Для большинства интерфейсов IP-адрес и маску подсети можно ввести вручную.

Для многих интерфейсов можно также назначить IP-адрес и маску подсети автоматически с помощью внешнего DHCP-сервера, подключенного к сети. В таком случае этот интерфейс выступает в качестве DHCP-клиента.

Вообще говоря, IP-адреса и маски подсети интерфейсов не должны накладываться друг на друга, хотя такая ситуация и возможна для DHCP-клиентов.

В описанном выше примере, если устройство NXC получает пакет с адресом назначения 5.5.5.5, то оно может не найти для такого адреса записей в таблице маршрутизации. В этом случае устройство отбрасывает пакет. Однако при наличии маршрутизатора по умолчанию, которому устройство NXC должно направлять такой пакет, можно указать такой маршрутизатор в качестве шлюза на одном из интерфейсов. Например, если имеется маршрутизатор по умолчанию с адресом 200.200.200.100, можно создать шлюз с адресом 200.200.200.100 на интерфейсе ge2. В этом случае устройство NXC создает следующую запись в таблице маршрутизации.

Таблица 66 Пример: Запись в таблице маршрутизации для шлюза

IP-АДРЕС(-А)	АДРЕС НАЗНАЧЕНИЯ
0.0.0.0/0	200.200.200.100

Шлюз является опциональным параметром для каждого интерфейса. Если шлюзов два и больше, устройство NXC использует шлюз с наименьшей метрикой или ценой. Если два и более шлюзов имеют одинаковую метрику, устройство NXC использует тот из них, который был сконфигурирован первым (то есть тот, запись для которого была создана в таблице маршрутизации первой).

Если интерфейс получает IP-адрес и маску подсети от DHCP-сервера, то DHCP-сервер тоже передает сведения о шлюзе, если таковые имеются.

Параметры интерфейсов

Устройство NXC ограничивает объем входящего и исходящего трафика для каждого интерфейса NXC.

- Пропускная способность egress определяет объем трафика, который устройство NXC может отправить в сеть через данный интерфейс.
- Пропускная способность ingress определяет объем трафика, который устройство NXC может пропустить через данный интерфейс из сети.[1]

Установка слишком жестких ограничений на пропускную способность практически эквивалентна снятию ограничений.

Кроме того, устройство NXC ограничивает размер каждого пакета данных. Максимально допустимое число байт в каждом пакете называется максимальным блоком передачи (MTU, maximum transmission unit). Если размер пакета превышает MTU, устройство NXC разбивает такой пакет на несколько более мелких фрагментов. Каждый фрагмент отправляется отдельно, а затем из этих фрагментов собирается исходный пакет. Чем меньше значение MTU, тем большее число фрагментов приходится отправлять и тем больше усилий затрачивается на корректную сборку пакетов в последующем. С другой стороны, некоторые коммуникационные каналы, такие, как Ethernet over ATM, не могут обрабатывать пакеты данных большого размера.

Настройки DHCP

Протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol, DHCP, RFC 2131, RFC 2132) позволяет автоматически конфигурировать и обновлять IP-адреса, маски подсетей, адреса шлюзов и некоторые сведения о сети (например, IP-адреса DNS-серверов) на компьютерах в сети. Использование DHCP позволяет сократить объем ручной работы и обеспечить более эффективное использование пула доступных IP-адресов.

В соответствии с моделью DHCP в каждой сети должен присутствовать хотя бы один DHCP-сервер. Когда компьютер (DHCP-клиент) подключается к сети, он направляет DHCP-запрос. DHCP-серверы принимают запрос; назначают IP-адрес; и предоставляют IP-адрес, маску подсети, адрес шлюза и имеющуюся информацию о сети DHCP-клиенту. После того, как данный DHCP-клиент покинет сети, DHCP-серверы могут назначить его бывший IP-адрес другому DHCP-клиенту.

Некоторые интерфейсы устройства NXC могут предоставлять в сети службы DHCP. В данном случае этот интерфейс может выступать в качестве DHCP-ретранслятора или DHCP-сервера.

В роли DHCP-ретранслятора данный интерфейс направляет DHCP-запросы DHCP-серверам в различных сетях. В сети можно установить два и более DHCP-серверов. В этом случае интерфейс будет отправлять DHCP-запросы всем серверам. Интерфейс может выступать в качестве DHCP-ретранслятора и DHCP-клиента одновременно.

В роли DHCP-сервера данный интерфейс предоставляет следующую информацию DHCP-клиентам.

1. На момент написания настоящего документа устройство NXC не поддерживает управление пропускной способностью ingress (то есть входящей пропускной способностью).

- IP-адрес – Если MAC-адрес DHCP-клиента присутствует в таблице статических адресов DHCP устройства NXC, данный интерфейс назначает соответствующий IP-адрес. Если нет, данный интерфейс выбирает IP-адрес из пула адресов, который определяется начальным адресом и размером пула.

Таблица 67 Пример: Назначение IP-адресов из пула

НАЧАЛЬНЫЙ IP-АДРЕС	РАЗМЕР ПУЛА	ДИАПАЗОН ВЫДЕЛЯЕМЫХ IP-АДРЕСОВ
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

  Устройство NXC не может назначить первый адрес (адрес сети) и последний адрес (широковещательный адрес) из подсети, определяемой IP-адресом и маской подсети данного интерфейса. Например, если для первой записи маска подсети имеет вид 255.255.255.0, устройство NXC не может назначить адреса 50.50.50.0 и 50.50.50.255. Если маска подсети имеет вид 255.255.0.0, устройство NXC не может назначить адреса 50.50.0.0 и 50.50.255.255. В остальных случаях устройство может назначить любой IP-адрес из диапазона за исключением IP-адреса самого интерфейса.

  Если не указать начальный адрес или размер пула, то интерфейс рассматривает в качестве пула максимальный диапазон IP-адресов, разрешенный IP-адресом интерфейса и его маской подсети. Например, если интерфейс имеет IP-адрес 9.9.9.1 и маску подсети 255.255.255.0, то в качестве начального IP-адреса берется адрес 9.9.9.2, а размер пула берется равным 253.

- Маска подсети – Интерфейс предоставляет ту же маску подсети, которая задана для самого интерфейса.
- Шлюз – Интерфейс предоставляет тот же адрес шлюза, который указан для самого интерфейса.
- DNS-серверы – Данный интерфейс предоставляет IP-адреса для не более чем трех DNS-серверов, которые предоставляют службы DNS DHCP-клиентам. Каждый IP-адрес можно указать вручную (например, адрес собственного DNS-сервера компании), либо можно сослаться на DNS-серверы, адреса которых другие интерфейсы получили от DHCP-серверов (например, адрес DNS-сервера провайдера услуг Интернет). Другие интерфейсы, упомянутые выше, должны быть DHCP-клиентами.

Один и тот же интерфейс не может быть одновременно и DHCP-сервером, и DHCP-клиентом.

WINS

WINS (Windows Internet Naming Service) – это реализация NetBIOS Name Server (NBNS) для операционной системы Windows. WINS-сервер отслеживает NetBIOS-имена компьютеров. Он хранит таблицу соответствия между именами компьютеров в сети и IP-адресами. Обновление этой таблицы происходит автоматически при выдаче новых IP-адресов службой DHCP. Это помогает уменьшить объем широковещательного трафика, поскольку компьютеры могут отправлять запросы на определенный сервер вместо отправки широковещательного запроса на получение IP-адреса для компьютера с определенным именем. В этом смысле WINS напоминает DNS, хотя в отличие от DNS WINS не использует иерархию. В сети может присутствовать два и более WINS-серверов. Samba также может выступать в качестве WINS-сервера.

9

Маршруты на основе политик и статические маршруты

9.1 Обзор

Маршруты на основе политик и статические маршруты можно использовать для замены алгоритмов маршрутизации устройства NXC по умолчанию с целью отправки пакетов на нужный интерфейс.

9.1.1 О чем рассказывается в этой главе

- Экраны **Policy Route** (разд. 9.2 на стр. 150) отображают перечень маршрутов на основе политик и позволяют выполнить их настройку.
- Экраны **Static Route** (разд. 9.3 на стр. 155) отображают перечень статических маршрутов и позволяют выполнить их настройку.

9.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Маршрутизация на основе политик

Традиционно маршрутизация осуществляется исключительно исходя из адреса назначения, и устройство NXC выбирает кратчайший путь для доставки пакета. Маршрутизация IP на основе политик (IP Policy Routing, IPPR) позволяет заменить алгоритм маршрутизации по умолчанию и изменить правила пересылки пакетов в зависимости от политики, описанной сетевым администратором. Правила маршрутизации на основе политик применяются ко входящим пакетам для каждого интерфейса в отдельности до применения стандартных правил маршрутизации.

Как использовать маршрутизацию на основе политик

- Маршрутизация по адресу источника – Сетевые администраторы могут использовать маршрутизацию на основе политик для пересылки трафика от различных пользователей по различным соединениям.
- Экономия затрат – Маршрутизация IPPR позволяет организациям распространять интерактивный трафик по дорогим каналам с высокой пропускной способностью, а пакетный трафик – по дешевым каналам.
- Распределение нагрузки – Сетевые администраторы могут использовать маршрутизацию IPPR для распределения трафика по нескольким каналам.

Статические маршруты

Устройство NXC обычно использует шлюз по умолчанию для пересылки исходящего трафика от компьютеров в локальной сети в сеть Интернет. Чтобы устройство NXC могло отправлять данные на устройства, не доступные через шлюз по умолчанию, используйте статические маршруты.

Маршруты на основе политик и статические маршруты

- Маршруты на основе политик обладают большей гибкостью по сравнению со статическими маршрутами. Можно выбрать дополнительные критерии для анализа трафика, использовать расписания и механизм трансляции сетевых адресов (NAT).
- Маршруты на основе политик можно использовать только внутри самого устройства NXC. Статические маршруты можно распространять на другие маршрутизаторы.
- Маршруты на основе политик имеют более высокий приоритет по отношению к статическим маршрутам. Если необходимо использовать политику маршрутизации на устройстве NXC и распространить ее на другие маршрутизаторы, можно создать маршрут на основе политик, а затем создать аналогичный статический маршрут.

Дифференцированное обслуживание

Управление качеством обслуживания (QoS) используют для приоритизации потоков трафика на пути от источника к пункту назначения. Всем пакетам в одном потоке назначается одинаковый приоритет. Класс обслуживания (CoS, class of service) – это способ управления трафиком в сети, который заключается в группировке схожих типов трафика и обработке каждого из типов как отдельного класса. CoS можно использовать для назначения различных приоритетов различным типам пакетов.

Дифференцированное обслуживание (DiffServ) представляет собой модель на базе классов обслуживания (CoS), в которой пакеты маркируются таким образом, чтобы на пути следования маршрута на сетевых устройствах с поддержкой DiffServ они подвергались особой обработке на каждом конкретном переходе в зависимости от типа приложения и плотности трафика. Пакеты маркируются кодовыми маркерами DiffServ (DiffServ Code Points, DSCP), которые указывают на желаемый уровень обслуживания. Это позволяет промежуточным сетевым устройствам с поддержкой DiffServ обрабатывать пакеты различным образом в зависимости от маркера, без необходимости согласования путей или запоминания информации о состоянии для каждого потока. Кроме того, приложениям не требуется запрашивать конкретное обслуживание или выдавать предварительное уведомление о том, куда направляется трафик.

Маркировка DSCP и обработка на конкретных переходах (Per-Hop Behavior)

При использовании DiffServ в заголовок IP-пакетов добавляется новое поле DS (Differentiated Services), которое заменяет поле типа обслуживания ToS (Type of Service). Поле DS состоит из двухбитного неиспользуемого поля и 6-битного поля маркера DSCP, которое позволяет определить до 64 уровней обслуживания. Поле DS изображено на следующем рисунке.

DSCP (6 бит)	Не используется (2 бита)

Маркер DSCP обратно совместим с тремя битами приоритета в октете ToS, благодаря чему сетевое устройство с поддержкой ToS, но без поддержки DiffServ не будет конфликтовать с отображением маркера DSCP.

Значение DSCP определяет обработку при пересылке, так называемую обработку на каждом конкретном переходе (PHB, Per-Hop Behavior), которая осуществляется над каждым пакетом при прохождении по сети с поддержкой DiffServ. В зависимости от правила маркирования различные типы трафика могут подвергаться различным способам пересылки. Ресурсы могут быть распределены соответственно значениям DSCP и настроенным политикам.

9.2 Экран Policy Route

Чтобы перейти к этому экрану, выберите в меню **Configuration > Network > Routing**. На этом экране можно увидеть список созданных маршрутов на основе политик и включить или отключить управление пропускной способностью с применением маршрутизации на основе политик.

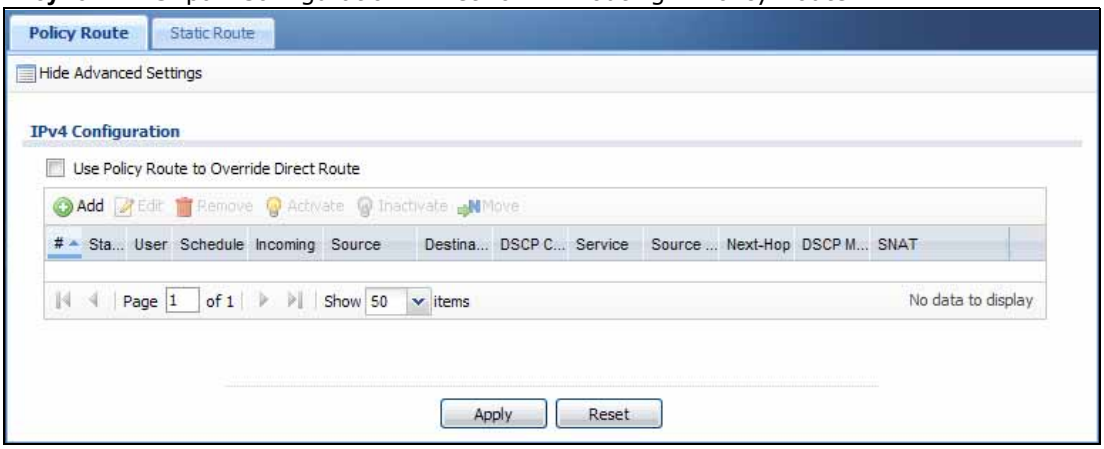
Маршрут на основе политик описывает критерии соответствия и действия, которые необходимо предпринять в отношении пакетов, соответствующих этим критериям. Действия применяются только к пакетам, соответствующим всем критериям. Критерии могут включать в себя имя пользователя, адрес источника и входящий интерфейс, адрес назначения, расписание, IP-протокол (ICMP, UDP, TCP и т.д.) и порт.

В отношении трафика могут быть предприняты следующие действия:

- Пересылка пакета на другой шлюз или на исходящий интерфейс.
- Ограничение доступной пропускной способности и установка приоритета для трафика.

По стилю и реализации средства фильтрации пакетов IPPR весьма напоминают средства фильтрации пакетов, применяемые службой RAS.

Рисунок 72 Экран Configuration > Network > Routing > Policy Route



Поля экрана описаны в следующей таблице.

Таблица 68 Экран Configuration > Network > Routing > Policy Route

ПОЛЕ	ОПИСАНИЕ
Show / Hide Advanced Settings	С помощью этой кнопки можно показать или скрыть на экране дополнительные поля настроек.
Use Policy Route to Override Direct Route	Установите этот переключатель, чтобы устройство NXC пересылало пакеты, соответствующие критериям маршрута на основе политик, в соответствии с этим маршрутом вместо непосредственной пересылки таких пакетов в подключенную к устройству сеть.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Move	Чтобы изменить позицию правила в нумерованном списке, выберите это правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести это правило. Чтобы перенести правило на указанную позицию, введите нужное значение и нажмите клавишу [ENTER]. Порядок расположения правил имеет большое значение, поскольку правила применяются в порядке нумерации.
#	Это поле показывает номер данного маршрута на основе политик.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
User	Здесь отображается имя пользовательского (группового) объекта, с которого осуществляется отправка пакетов. Значение **any** означает «все пользователи».
Schedule	Это название объекта расписания. **none** означает, что маршрут – если он включен – активен постоянно.
Incoming	Это интерфейс, который принимает пакеты.
Source	Это название (группового) объекта IP-адреса источника. Значение **any** означает «все IP-адреса».
Destination	Это название (группового) объекта IP-адреса назначения. Значение **any** означает «все IP-адреса».
DSCP Code	Это значение кода DSCP входящих пакетов, к которому применяется данный маршрут на основе политик. Значение **any** означает любые значения кода DSCP или отсутствие маркера DSCP. Значение **default** означает трафик со значением кода DSCP, равным 0. Как правило, это трафик, доставляемый по принципу «без гарантий» («наилучших усилий»). Записи с пометкой «**af**» означают гарантированную передачу (Assured Forwarding). Число, идущее сразу за префиксом «**af**», идентифицирует один из четырех классов и один из трех приоритетов отбрасывания. Записи с пометкой «**wmm**» соответствуют правилам QoS. Более подробную информацию о категориях QoS и WMM можно найти настр. 158.
Service	Это название объекта службы. Значение **any** означает «все службы».
Source Port	Это имя объекта службы. Устройство NXC применяет маршрут на основе политик к пакетам, отправляемым с порта соответствующей службы. Значение **any** означает «порты всех служб».

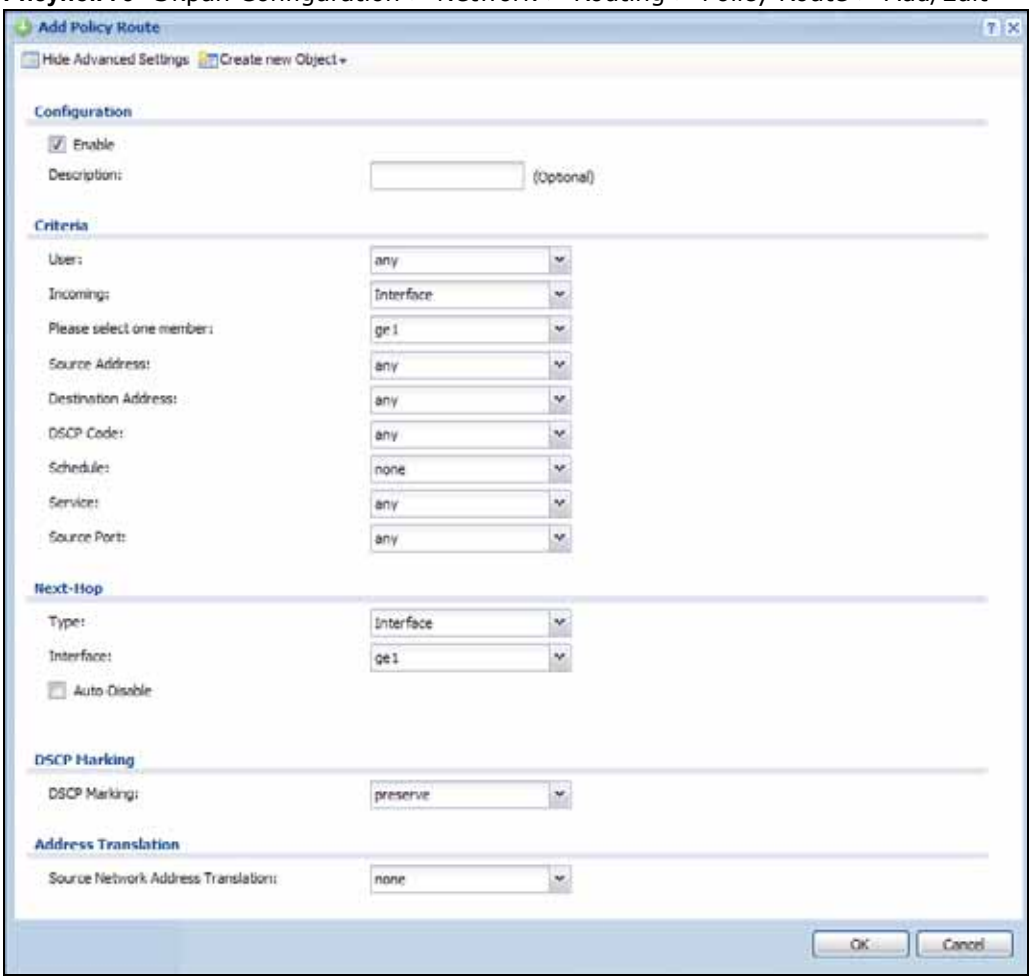
Таблица 68 Экран Configuration > Network > Routing > Policy Route (продолжение)

ПОЛЕ	ОПИСАНИЕ
Next-Hop	Это следующий переход, на который отправляются пакеты. Это поле помогает доставлять пакеты по адресам назначения, в этом поле можно указать адрес маршрутизатора или исходящего интерфейса.
DSCP Marking	Это поле указывает на то, каким образом устройство NXC обрабатывает значение кодового маркера DSCP, содержащееся в исходящих пакетах, удовлетворяющих критериям данного маршрута. Если данное поле содержит значение DSCP, устройство NXC применяет данное значение DSCP к исходящим пакетам, к которым применяется данный маршрут. Значение **preserve** означает, что устройство NXC не изменяет значение кодового маркера DSCP в исходящих пакетах, к которым применяется данный маршрут. Значение **default** означает, что устройство NXC устанавливает значение кодового маркера DSCP в исходящих пакетах, к которым применяется данный маршрут, равным 0. Опции с пометкой «**af**» означают гарантированную передачу (Assured Forwarding). Число, идущее сразу за префиксом «**af**», идентифицирует один из четырех классов и один из трех приоритетов отбрасывания. Записи с пометкой «**wmm**» соответствуют правилам QoS. Более подробную информацию о категориях QoS и WMM можно найти настр. 158.
SNAT	В этом поле содержится IP-адрес источника, который использует данный маршрут. Если в поле отображается значение **none**, то это означает, устройство NXC не выполняет трансляцию сетевых адресов (NAT) для данного маршрута.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

9.2.1 Экран Add/Edit Policy Route

Чтобы перейти к экрану Policy Route, выберите в меню **Configuration > Network > Routing**. Затем нажмите на пиктограмму **Add** или **Edit**, чтобы открыть экран **Policy Route Edit**. С помощью этого экрана можно создать или изменить маршрут на основе политик.

Рисунок 73 Экран Configuration > Network > Routing > Policy Route > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 69 Экран Configuration > Network > Routing > Policy Route > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Show / Hide Advanced Settings	С помощью этой кнопки можно показать или скрыть на экране дополнительные поля настроек.
Create new Object	С помощью этой кнопки можно создать любые новые объекты настроек, которые понадобятся на этом экране.
Configuration	
Enable	Установите этот переключатель, чтобы активировать данную политику.
Description	Введите имя-описание политики (не более 60 печатных ASCII-символов).
Criteria	
User	Выберите имя пользователя или пользовательской группы, от имени которой осуществляется отправка пакетов.
Incoming	Выберите источник пакетов; любой (any), интерфейс (interface) или само устройство NXC (**EnterpriseWLAN**). В случае выбора опции interface необходимо будет указать конкретный интерфейс.
Please select one member	Это поле появляется на экране только в том случае, если выбрать значение **Incoming** в поле **Interface**. Выберите интерфейс, с которого осуществляется отправка пакетов.

Таблица 69 Экран Configuration > Network > Routing > Policy Route > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Source Address	Выберите объект IP-адреса источника, с которого будет осуществляться отправка пакетов.
Destination Address	Выберите объект IP-адреса назначения, на который будет отправляться трафик.
DSCP Code	Выберите значение кодового маркера DSCP входящих пакетов, к которым будет применяться данная политика на основе маршрутов, или выберите опцию **User Defined**, чтобы указать другую кодовую точку DSCP. Чем меньше указанное число – тем выше приоритет, за исключением значения 0. Пакеты, содержащие это значение, обрабатываются обычно по принципу максимальных усилий. Значение **any** означает любое значение кода DSCP или отсутствие маркера DSCP. Значение **default** означает трафик со значением кода DSCP, равным 0. Как правило, это трафик, доставляемый по принципу «без гарантий» («наилучших усилий»). Опции с пометкой «**af**» означают гарантированную передачу (Assured Forwarding). Число, идущее сразу за префиксом «**af**», идентифицирует один из четырех классов и один из трех приоритетов отбрасывания. Записи с пометкой «**wmm**» соответствуют правилам QoS. Более подробную информацию о категориях QoS и WMM можно найти настр. 158.
User-Defined DSCP Code	Укажите в этом поле собственное значение кодового маркера DSCP.
Schedule	Выберите расписание для управления периодами активности политик. Значение **none** означает, что маршрут – если он включен – активен постоянно.
Service	Выберите службу или группу служб для идентификации типа трафика, к которому будет применяться маршрут на основе политик.
Source Port	Выберите службу или группу служб для идентификации порта-источника пакетов, к которым будет применяться маршрут на основе политик.
Next-Hop	
Type	При выборе опции **Auto** устройство NXC будет использовать таблицу маршрутизации для поиска следующего перехода и автоматической пересылки пакетов, удовлетворяющих критериям. При выборе опции **Gateway** устройство будет пересылать пакеты, удовлетворяющие критериям, на маршрутизатор или коммутатор следующего перехода, который указан в поле **Gateway**. Предварительно необходимо создать маршрутизатор или коммутатор следующего перехода как объект адреса HOST. При выборе опции **Interface** устройство будет пересылать пакеты, удовлетворяющие критериям, через указанный исходящий интерфейс на шлюз (который подключен к данному интерфейсу).
Gateway	Это поле появляется на экране, если выбрать опцию **Gateway** в поле **Type**. Выберите адресный объект HOST. Шлюз – это ближайший сосед устройства NXC, который направляет пакет к пункту его назначения. В качестве шлюза может выступать маршрутизатор или коммутатор, которые находятся в том же сегменте сети, что и данный интерфейс устройства NXC.
Interface	Это поле появляется на экране, если выбрать опцию **Interface** в поле **Type**. Выберите интерфейс, через который устройство NXC будет отправлять трафик, удовлетворяющий маршруту на основе политик.
Auto-Disable	Это поле появляется на экране, если выбрать опцию **Interface** в поле **Type**. Установите этот флаг, чтобы устройство NXC автоматически отключало этот маршрут на основе политик в случае недоступности соединения со следующим переходом.
DSCP Marking	

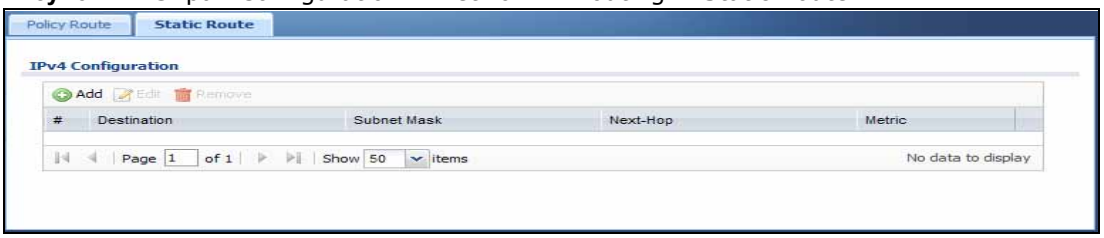
Таблица 69 Экран Configuration > Network > Routing > Policy Route > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
DSCP Marking	Значение в этом поле указывает на то, каким образом устройство NXC должно обрабатывать значение DSCP в исходящих пакетах, которые удовлетворяют данному маршруту. Выберите одно из заранее определенных значений DSCP или опцию **User Defined**, чтобы указать другое значение DSCP. Опции с пометкой «**af**» означают гарантированную передачу (Assured Forwarding). Число, идущее сразу за префиксом «**af**», идентифицирует один из четырех классов и один из трех приоритетов отбрасывания. При выборе опции **preserve** устройство NXC будет сохранять исходное значение DSCP в пакетах. При выборе опции **default** устройство NXC будет устанавливать значение DSCP в пакетах равным 0. Записи с пометкой «**wmm**» соответствуют правилам QoS. Более подробную информацию о категориях QoS и WMM можно найти настр. 158.
User-Defined DSCP Code	В этом поле можно указать собственное значение DSCP.
Address Translation	В этом разделе можно настроить механизм трансляции сетевых адресов (NAT) для маршрута на основе политик.
Source Network Address Translation	Выберите опцию **none**, если использовать трансляцию сетевых адресов (NAT) для данного маршрута не требуется. Выберите опцию **outgoing-interface**, если необходимо использовать IP-адрес исходящего интерфейса в качестве IP-адреса источника для пакетов, удовлетворяющих критериям данного маршрута. В случае выбора опции **outgoing-interface** также можно будет настроить параметры триггера портов для данного интерфейса. Выберите заранее заданный адрес (группу), чтобы использовать IP-адреса источников пакетов, удовлетворяющих критериям данного маршрута. Выберите опцию **Create new Object**, если необходимо создать новый адрес (группу) и использовать ее в качестве IP-адреса источника пакетов, удовлетворяющих критериям данного маршрута.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

9.3 Экран Static Route

Выберите в меню **Configuration > Network > Routing > Static Route**, чтобы перейти к экрану **Static Route**. Этот экран показывает список созданных статических маршрутов.

Рисунок 74 Экран Configuration > Network > Routing > Static Route



Поля экрана описаны в следующей таблице.

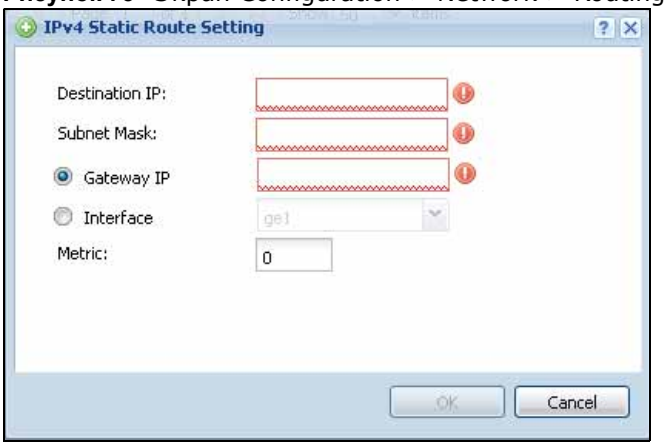
Таблица 70 Экран Configuration > Network > Routing > Static Route

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новый статический маршрут.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
#	Это номер данного статического маршрута.
Destination	Это IP-адрес назначения.
Subnet Mask	Это маска подсети для IP-адреса.
Next-Hop	Это IP-адрес шлюза следующего перехода или интерфейса, через который направляется трафик. В качестве шлюза может выступать маршрутизатор или коммутатор, которые находятся в том же сегменте сети, что и данный интерфейс устройства NXC. Шлюз помогает доставлять пакеты по адресам назначения.
Metric	Это приоритет маршрута среди других маршрутов устройства NXC. Чем меньше число, указанное в этом поле, тем более высокий приоритет имеет данный маршрут.

9.3.1 Настройка статических маршрутов

Выберите последовательный номер статического маршрута и нажмите кнопку **Add** или **Edit**. Откроется экран, изображенный на рисунке ниже. С помощью этого экрана можно ввести информацию, необходимую для создания статического маршрута.

Рисунок 75 Экран Configuration > Network > Routing > Static Route > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 71 Экран Configuration > Network > Routing > Static Route > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Destination IP	Сетевой IP-адрес конечного пункта назначения. Маршрутизация всегда основывается на номере сети. Если нужно указать маршрут к конкретному хосту, в поле ввода маски подсети необходимо ввести маску 255.255.255.255, и тогда в качестве номера сети можно использовать идентификатор требуемого хоста.
Subnet Mask	Введите в этом поле маску подсети для IP-адреса.

Таблица 71 Экран Configuration > Network > Routing > Static Route > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Gateway IP	Выберите нужный переключатель и введите IP-адрес шлюза следующего перехода. В качестве шлюза может выступать маршрутизатор или коммутатор, которые находятся в том же сегменте сети, что и данный интерфейс устройства NXC. Шлюз помогает доставлять пакеты по адресам назначения.
Interface	Выберите нужный переключатель и заранее заданный интерфейс, через который будет направляться трафик.
Metric	Поле Metric хранит «стоимость» передачи для целей маршрутизации. В IP-маршрутизации в качестве меры стоимости используется счетчик пройденных узлов, с минимальным значением 1 для сетей, соединенных напрямую. Введите число, примерно отражающее стоимость данного канала. Это число необязательно должно быть точным, но оно должно лежать в диапазоне от 0 до 127. На практике обычно подходит 2 или 3.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

9.4 Справочная техническая информация

В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

NAT и SNAT

NAT (Network Address Translation – NAT, RFC 1631) – это трансляция IP-адреса, содержащегося в пакете в одной сети, в другой IP-адрес в другой сети. Механизм SNAT (Source NAT, трансляция сетевого адреса источника) позволяет подменять IP-адрес источника в одной сети на другой IP-адрес в другой сети.

Гарантированная передача на следующем переходе для дифференцированного обслуживания

Алгоритм гарантированной передачи (Assured Forwarding, AF) описан в документе RFC 2597. Группа алгоритмов AF описывает четыре класса AF. Внутри каждого класса пакетам назначается высокий, средний или низкий приоритет отбрасывания. Приоритет отбрасывания определяет вероятность того, что маршрутизаторы в сети отбросят эти пакеты при возникновении перегрузки. Если перегрузка затрагивает трафик разных классов, то трафик с более высоким классом (и меньшим номером), как правило, имеет приоритет. Сочетание классов и приоритета отбрасывания дает следующие двенадцать кодов DSCP с AF11 по AF43. Десятичный эквивалент каждого кода указан в скобках.

Таблица 72 Группа алгоритмов гарантированной передачи (Assured Forwarding, AF)

	Класс 1	Класс 2	Класс 3	Класс 4
Низкий приоритет отбрасывания	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Средний приоритет отбрасывания	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
Высокий приоритет отбрасывания	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

WMM

Wi-Fi Multimedia (WMM) реализует базовые функции управления качеством обслуживания (Quality of Service, QoS) для беспроводных сетей. WMM описывает четыре категории QoS: голос (VO), видео (VI), негарантированный трафик (BE) и фоновый трафик (BK). Эти категории, известные также под названием «категории доступа» (access categories, AC), поставлены в соответствие со значениями приоритетов 802.1D, которые в свою очередь можно привязать к соответствующим шестнадцатеричным значениям кода DSCP.

Таблица 73 Преобразование WMM -> DiffServ на устройстве NXC

Priority	Категория доступа WMM	Приоритет 802.1D	Шестнадцатеричное значение DSCP
Самое низкое	BK	1	0x08
	BK	2	0x10
	BE	0	0x00
	BE	3	0x18
	VI	4	0x20
	VI	5	0x28
	VO	6	0x30
Самое высокое	VO	7	0x38

Категории доступа WMM, реализованные на устройстве NXC, имеют следующие функции:

VOICE: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как голосовые данные. Эту категорию рекомендуется использовать в случае, если сеть с идентификатором SSID служит для совершения и приема голосовых VoIP-вызовов.

VIDEO: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как данные видео. Эту категорию рекомендуется использовать в случае, если сеть с идентификатором SSID служит для организации видеоконференций.

BEST EFFORT: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как «best effort» («без гарантий»); это означает, что данные пойдут по наиболее оптимальному маршруту, но так, чтобы не препятствовать трафику с более высоким приоритетом. Эта категория доступа хорошо подходит для тех случаев, когда необходимости в обеспечении наивысшей пропускной способности нет, например, при серфинге в сети Интернет.

BACKGROUND: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как низкоприоритетный или «background traffic» («фоновый трафик»); это означает, что все трафик всех остальных категорий имеет приоритет над трафиком этой категории. Если трафик из сети с данным идентификатором SSID не предъявляет жестких требований к пропускной способности, то рекомендуется использовать эту категорию доступа. Например, это может быть сеть, к которой подключены исключительно сетевые принтеры.

10

Зоны

10.1 Обзор

Зоны создаются с целью настройки параметров безопасности сети и сетевых политик на устройстве NXC. Зона – это группа интерфейсов. При настройке многих параметров безопасности и политик, например, правил для межсетевых экранов, устройство NXC использует зоны вместо интерфейсов. Зоны не могут пересекаться. Каждый интерфейс может быть приписан только к одной зоне.

10.1.1 О чем рассказывается в этой главе

Экраны **Zone** (см. разд. 10.2 на стр. 160) позволяют управлять зонами устройства NXC.

10.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Эффект от использования для различных типов трафика

Зоны эффективно разделяют трафик на три типа -- внутризональный трафик, межзональный трафик и внезональный трафик -- на которые по-разному влияют настройки безопасности и политик на основе зон.

Внутризональный трафик

- Внутризональным называется трафик между интерфейсами, относящимися к одной зоне.
- В любой зоне можно либо разрешить, либо запретить весь внутризональный трафик.
- Для управления внутризональным трафиком можно создать правила межсетевых экранов, но многие другие типы параметров безопасности и политик на основе зон не влияют на внутризональный трафик.

Межзональный трафик

Межзональным называется трафик между интерфейсами, относящимися к разным зонам.

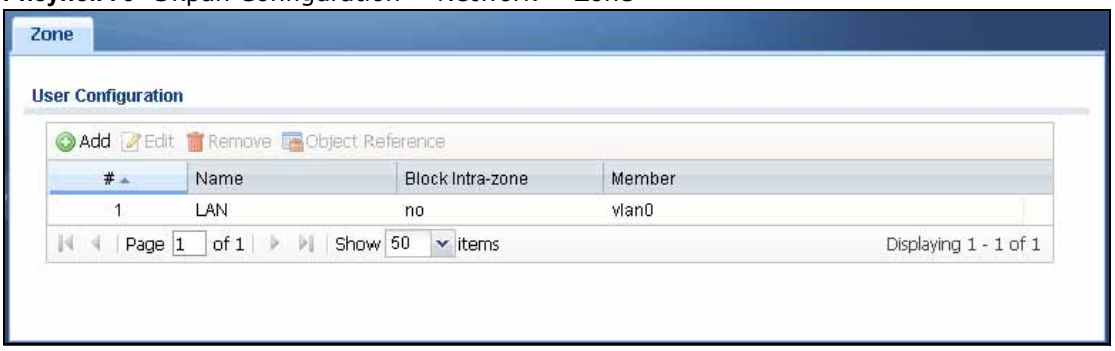
Внезональный трафик

- Внезональным называется трафик, который поступает от или к любому интерфейсу, не относящемуся к какой-либо зоне.
- Некоторые параметры безопасности и настройки политик на основе зон могут быть применимы к внезональному трафику, в особенности если имеется возможность установить для них значение атрибута зоны равным **Any** или **All**. Более подробную информацию можно найти в описании конкретной функции.

10.2 Экран Zone

Экран **Zone** содержит сводную информацию обо всех зонах. Кроме того, этот экран позволяет добавлять, изменять и удалять зоны. Чтобы открыть этот экран, выберите в меню **Configuration > Network > Zone**.

Рисунок 76 Экран Configuration > Network > Zone



Поля экрана описаны в следующей таблице.

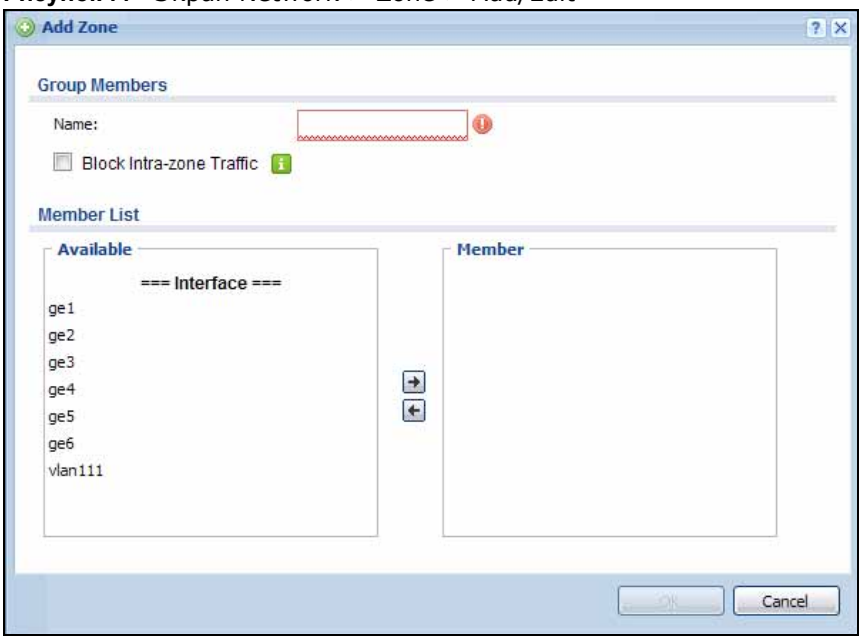
Таблица 74 Экран Configuration > Network > Zone

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новую зону, доступную для пользовательских настроек.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Чтобы удалить зону, созданную пользователем, выберите ее и нажмите кнопку **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо интерфейсом.
Name	Это поле показывает имя зоны.
Block Intra-zone	Это поле указывает на то, должно ли устройство NXC блокировать сетевой трафик между участниками одной зоны.
Member	Это поле отображает имена интерфейсов, которые принадлежат каждой из зон.

10.2.1 Экран Add/Edit Zone

С помощью этого экрана можно добавлять зоны и изменять их параметры. Чтобы открыть этот экран, перейдите на экран **Zone** и нажмите на пиктограмму **Add** или пиктограмму **Edit**.

Рисунок 77 Экран Network > Zone > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 75 Экран Network > Zone > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя, которое будет использоваться для ссылки на эту зону. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
Block Intra-zone Traffic	Установите этот переключатель для блокировки сетевого трафика между участниками одной зоны.
Member List	В поле **Available** перечислены все интерфейсы, которые не принадлежат ни одной из зон. Выберите интерфейсы, которые необходимо добавить к определенной редактируемой зоне, и нажмите кнопку с правой стрелкой, чтобы их добавить. В поле **Member** перечислены интерфейсы, которые принадлежат определенной зоне. Выберите все интерфейсы, которые необходимо удалить из данной зоны, и нажмите кнопку с левой стрелкой, чтобы их удалить.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

11

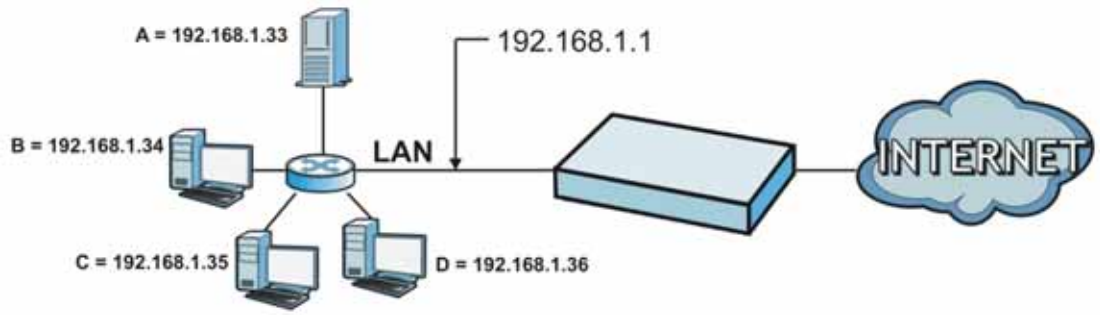
Трансляция сетевых адресов (NAT)

11.1 Обзор

NAT (Network Address Translation – NAT, RFC 1631) – это трансляция IP-адреса хоста в пакете. К примеру, адрес источника исходящего пакета, используемый в одной сети, меняется на другой IP-адрес, известный в другой сети. Трансляция сетевых адресов позволяет сделать компьютеры, находящиеся в частной сети за устройством NXC, доступными за ее пределами. Если устройство NXC имеет только один внешний IP-адрес, компьютеры из частной сети можно сделать доступными, используя порты для пересылки пакетов на соответствующие внутренние IP-адреса.

Предположим, необходимо назначить порты 21-25 одному серверу FTP, Telnet и SMTP (**сервер A** из примера), порт 80 – другому серверу (**сервер B** из примера), а IP-адрес сервера по умолчанию 192.168.1.35 – третьему серверу (**сервер C** из примера). Можно назначить указанным серверам IP-адреса в локальной сети, а провайдер услуг Интернета назначит IP-адрес в сети WAN. Сеть NAT предстает для Интернета как один хост.

Рисунок 78 Пример: несколько серверов за устройством NAT



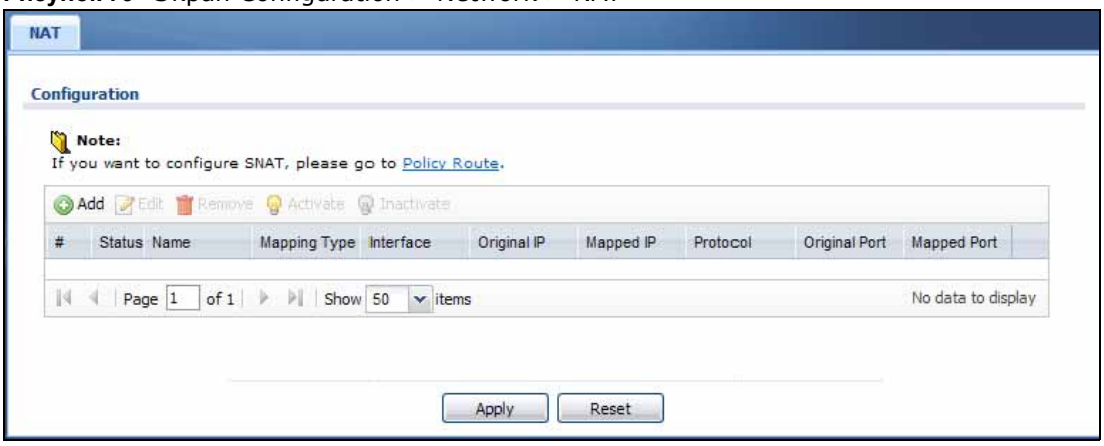
11.1.1 О чем рассказывается в этой главе

Экраны **NAT** (см. разд. 11.2 на стр. 162) показывают список правил NAT и подробные сведения об их конфигурации, а также позволяют управлять ими. Можно создавать новые правила NAT, изменять и удалять существующие правила.

11.2 Сводный экран NAT

Сводный экран **NAT** содержит информацию обо всех правилах NAT и их конфигурации. Кроме того, этот экран позволяет создавать новые правила NAT, а также менять и удалять существующие правила NAT. Чтобы попасть на этот экран, выполните вход в Web-конфигуратор и выберите в меню **Configuration > Network > NAT**. Откроется следующий экран, содержащий сводную информацию о существующих правилах NAT.

Рисунок 79 Экран Configuration > Network > NAT



Поля экрана описаны в следующей таблице.

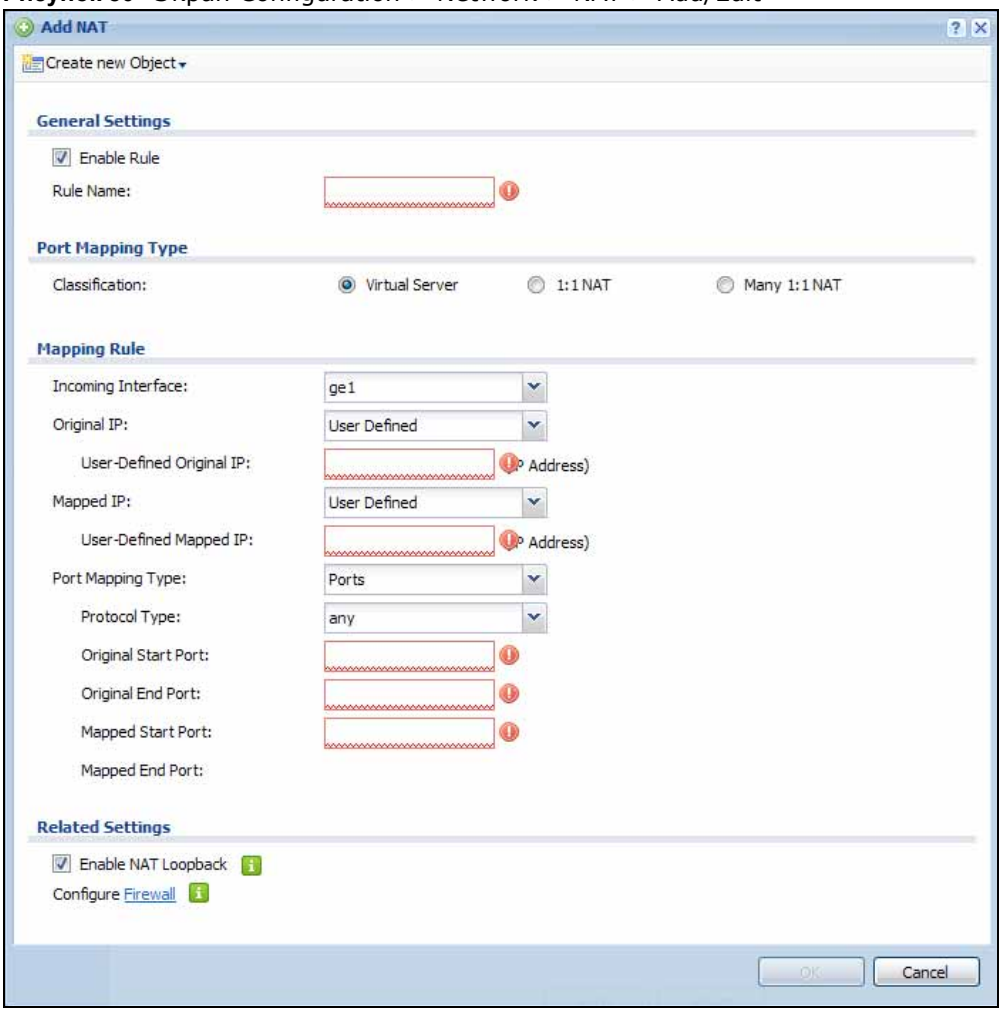
Таблица 76 Экран Configuration > Network > NAT

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Name	Это поле показывает имя записи.
Mapping Type	Это поле указывает на то, какой тип трансляции NAT выполняет эта запись: **Virtual Server**, **1:1 NAT** или **Many 1:1 NAT**.
Interface	Это поле показывает имя интерфейса, который принимает пакеты для данной записи NAT.
Original IP	Это поле показывает исходный IP-адрес назначения (или адресный объект) трафика, который соответствует критериям этой записи NAT. Если ограничения на исходный IP-адрес назначения отсутствуют, в этом поле отображается значение **any**.
Mapped IP	Это поле показывает новый IP-адрес назначения для пакетов.
Protocol	Это поле показывает название службы, используемой пакетами для данной записи NAT. Если ограничения на службы отсутствуют, в этом поле отображается значение **any**.
Original Port	Это поле показывает исходный порт(-ы) назначения для пакетов, соответствующих критериям данной записи NAT. Если ограничения на исходный порт назначения отсутствуют, это поле остается пустым.
Mapped Port	Это поле показывает новый порты(-ы) назначения для пакетов. Если ограничения на исходный порт назначения отсутствуют, это поле остается пустым.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в конфигурации NXC.
Reset	Нажмите эту кнопку, чтобы вернуть на экран настройки, сохраненные ранее.

11.2.1 Экран Add/Edit NAT

Этот экран позволяет создавать новые и изменять существующие правила NAT. Чтобы перейти к этому окну, откройте сводный экран **NAT**. Затем нажмите на пиктограмму **Add** или пиктограмму **Edit**, чтобы открыть следующий экран.

Рисунок 80 Экран Configuration > Network > NAT > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 77 Экран Configuration > Network > NAT > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Create new Object	С помощью этой кнопки можно создать любые новые объекты настроек, которые понадобятся на этом экране.
Enable Rule	С помощью этого переключателя можно включить или отключить данное правило NAT.
Rule Name	Введите имя правила NAT. Это имя будет использоваться для ссылки на данное правило NAT. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.

Таблица 77 Экран Configuration > Network > NAT > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Classification	Выберите тип трансляции NAT, который должно выполнять это правило. **Virtual Server** – Эта опция делает компьютеры в частной сети, находящейся за устройством NXC, доступными в публичной сети перед устройством NXC (например, в сети Интернет). **1:1 NAT** – Если сервер в частной сети инициирует сессии с внешними клиентами, можно выбрать эту опцию, чтобы устройство NXC транслировало IP-адрес источника в исходящем от сервера трафике в тот же внешний IP-адрес, который внешние клиенты используют для доступа к серверу. **Many 1:1 NAT** – Если в частной сети имеется группа серверов, которые инициируют сессии с внешними клиентами, и в наличии имеется ряд внешних IP-адресов, можно выбрать эту опцию, и тогда устройство NXC будет транслировать IP-адреса источника в исходящем от этих серверов трафике в те же внешние IP-адреса, которые внешние клиенты используют для доступа к эти серверам. Количество частных и соответствующих им внешних IP-адресов должно быть одинаковым. Одно правило NAT типа «many 1:1» фактически действует как несколько правил NAT типа «1:1». Таким образом, наличие типа «many 1:1» упрощает процесс настройки, поскольку необходимо создать всего одно правило вместо нескольких.
Incoming Interface	Выберите интерфейс, который будет принимать пакеты в соответствии с данным правилом NAT. Это может быть интерфейс Ethernet или интерфейс VLAN.
Original IP	Укажите IP-адрес назначения пакетов, принимаемых входящим интерфейсом, указанным для данного правила NAT. **any** – При выборе этой опции учитываются все IP-адреса для входящего интерфейса, включая динамические. **User Defined** – При выборе этой опции можно вручную ввести нужный IP-адрес в поле **User Defined**. Например, можно указать статический внешний IP-адрес, выданный провайдером. **Host address** – выберите объект адреса хоста с тем, чтобы использовать IP-адрес, на который он ссылается. Этот список также содержит адресные объекты на основе IP-адресов интерфейсов. Поэтому можно, к примеру, выбрать адресный объект на основе интерфейса WAN, даже если ему назначен динамический IP-адрес.
User Defined Original IP	Это поле становится доступным, если в поле **Original IP** выбрана опция **User Defined**. Введите IP-адрес назначения, который поддерживает это правило NAT.
Original IP Subnet/Range	Это поле появляется на экране при выборе опции Many 1:1 NAT. Выберите подсеть или диапазон IP-адресов назначения, которые поддерживает данное правило NAT. Количество IP-адресов в исходных/транслированных подсетях/диапазонах IP-адресов должно быть одинаковым.
Mapped IP	Укажите транслированный IP-адрес назначения, на который данное правило NAT будет пересылать пакеты. **User Defined** – это правило NAT поддерживает конкретный IP-адрес, указанный в поле **User Defined**. **HOST address** – этот выпадающий список содержит все адресные объекты HOST устройства NXC. Если выбрать один из них, то правило NAT будет поддерживать IP-адрес, на который указывает этот адресный объект.
User Defined Original IP	Это поле становится доступным, если в поле **Mapped IP** выбрана опция **User Defined**. Введите транслированный IP-адрес назначения, который поддерживает это правило NAT.
Mapped IP Subnet/Range	Это поле появляется на экране при выборе опции **Many 1:1 NAT**. Выберите подсеть или диапазон транслированных IP-адресов назначения, на которые данное правило NAT будет пересылать пакеты. Количество IP-адресов в исходных/транслированных подсетях/диапазонах IP-адресов должно быть одинаковым.

Таблица 77 Экран Configuration > Network > NAT > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Port Mapping Type	Выберите в этом выпадающем списке перечень исходных портов назначения, которые поддерживает данное правило NAT для выбранного IP-адреса назначения (**Original IP**). Возможные варианты: **Any** – данное правило NAT поддерживает все порты назначения. **Service** – данное правило NAT поддерживает порты назначения, используемые указанной службой (или службами). **Port** – данное правило NAT поддерживает один порт назначения. **Ports** – данное правило NAT поддерживает диапазон портов назначения. Диапазон портов назначения можно использовать в случае неизвестных служб или в ситуации, когда один сервер поддерживает две и более служб. Это поле доступно только для чтения и отображает значение **any** при выбранной опции **Many 1:1 NAT**.
Original Service	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Service**. Выберите исходную службу, чьи порты назначения поддерживает данное правило NAT.
Mapped Service	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Service**. Выберите транслированную службу, на порты назначения которой будет пересылать пакеты данное правило NAT.
Protocol Type	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Port** или опция **Ports**. Выберите протокол (**TCP**, **UDP** или **Any**), который использует служба, запрашивающая соединение.
Original Port	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Port**. Введите исходный порт назначения, который поддерживает данное правило NAT.
Mapped Port	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Port**. Введите транслированный порт назначения, на который данное правило NAT пересылает пакеты.
Original Start Port	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Ports**. Укажите начало диапазона исходных портов назначения, которые поддерживает данное правило NAT.
Original End Port	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Ports**. Укажите конец диапазона исходных портов назначения, которые поддерживает данное правило NAT.
Mapped Start Port	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Ports**. Укажите начало диапазона транслированных портов назначения, которые поддерживает данное правило NAT.
Mapped End Port	Это поле становится доступным, если в поле **Port Mapping Type** выбрана опция **Ports**. Укажите конец диапазона транслированных портов назначения, которые поддерживает данное правило NAT. Количество портов в диапазонах исходных и транслированных портов должно быть одинаковым.

Таблица 77 Экран Configuration > Network > NAT > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enable NAT Loopback	Опция обратной петли NAT позволяет пользователям, подключенным к любому интерфейсу (а не только к интерфейсу, указанному в поле **Incoming Interface**) использовать адрес, указанный в поле **Original IP** для данного правила NAT, для доступа к устройству по адресу, указанному в поле **Mapped IP**. Для пользователей, подключенных к тому же интерфейсу, что и устройство с адресом, указанным в поле **Mapped IP**, устройство NXC использует IP-адрес этого интерфейса как адрес источника для трафика, который оно пересылает от пользователей на устройство по адресу, указанному в поле **Mapped IP**. Например, если создано правило NAT для пересылки трафика из сети WAN на сервер в локальной сети, включение обратной петли NAT позволит пользователям, подключенным к другим интерфейсам, также получить доступ к данному серверу. Для пользователей локальной сети устройство NXC использует IP-адрес интерфейса локальной сети в качестве адреса источника для трафика, пересылаемого на сервер локальной сети. Если не включать опцию обратной петли NAT, то данное правило NAT будет применяться только к пакетам, полученным на конкретном входящем интерфейсе, указанном для данного правила.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы вернуться на общий экран **NAT**, отказавшись от создания правила NAT (в случае создания нового правила) или от сохранения изменений (в случае изменения существующего правила).

11.3 Справочная техническая информация

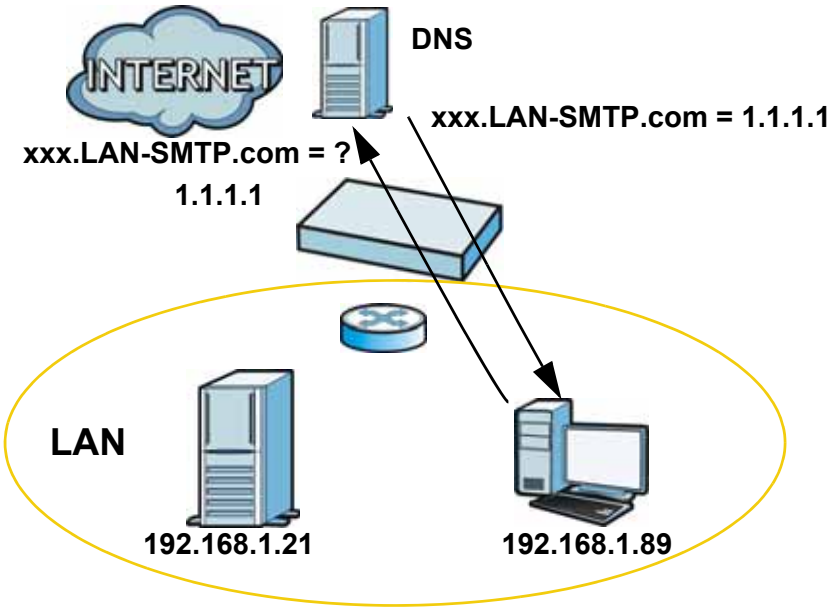
В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

Обратная петля NAT

Предположим, правило типа NAT 1:1 транслирует внешний IP-адрес в частный IP-адрес почтового SMTP-сервера, расположенного в локальной сети, с целью предоставления доступа к нему пользователям сети WAN. Обратная петля NAT дает возможность другим пользователям также использовать исходный IP-адрес, указанный в правиле, для доступа к данному почтовому серверу.

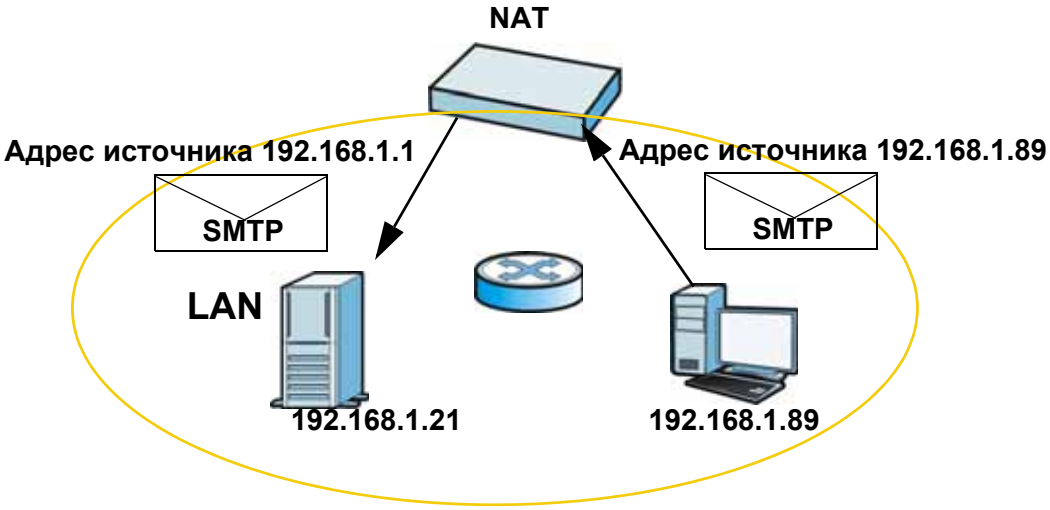
Например, компьютер пользователя в локальной сети с IP-адресом 192.168.1.89 запрашивает у публичного DNS-сервера разрешение доменного имени SMTP-сервера (в нашем примере – xxx.LAN-SMTP.com) и получает транслированный внешний IP-адрес SMTP-сервера 1.1.1.1.

Рисунок 81 Компьютер, находящийся в локальной сети, направляет запрос на публичный DNS-сервер



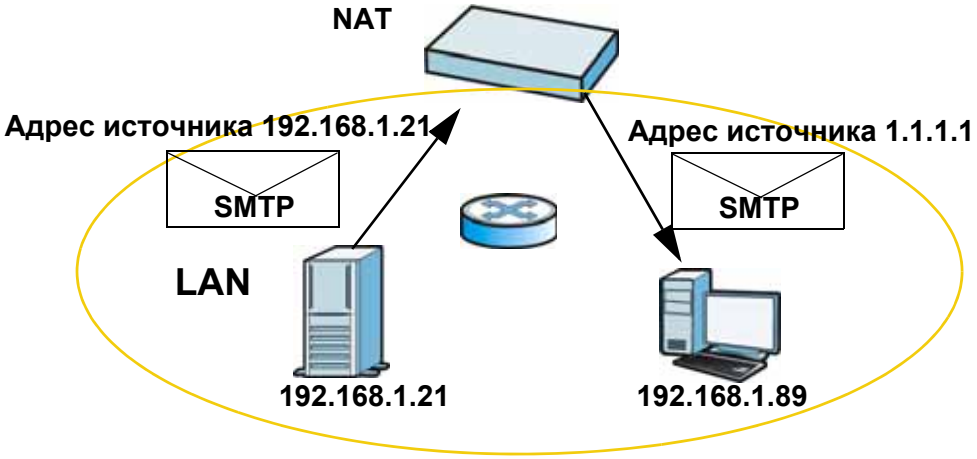
После этого компьютер пользователя в локальной сети направляет трафик по IP-адресу 1.1.1.1. Обратная петля NAT использует IP-адрес интерфейса локальной сети устройства NXC (192.168.1.1) в качестве адреса источника для трафика, идущего от пользователей локальной сети на SMTP-сервер, расположенный в локальной сети.

Рисунок 82 Трафик из локальной сети в локальную сеть



SMTP-сервер, находящийся в локальной сети, отправляет ответ на IP-адрес интерфейса локальной сети устройства NXC, и устройство NXC подменяет адрес источника на 1.1.1.1 перед отправкой пакетов пользователям локальной сети. IP-адрес источника в ответных пакетах совпадает с исходным IP-адресом назначения (1.1.1.1). Если бы SMTP-сервер отвечал непосредственно пользователю в локальной сети, минуя NAT, то адрес источника в ответном трафике не совпадал бы с исходным адресом назначения, и компьютер пользователя в локальной сети завершил бы сессию.

Рисунок 83 Ответный трафик из локальной сети в локальную сеть



12

Шлюз прикладного уровня (ALG)

12.1 Обзор

Шлюз прикладного уровня (Application Layer Gateway, ALG) позволяет следующему приложению нормально функционировать при использовании трансляции сетевых адресов (NAT) на устройстве NXC.

- FTP – File Transfer Protocol – служба передачи файлов в сети Интернет.

Функция ALG нужна только для трафика, который подвергается трансляции сетевых адресов (NAT) на устройстве NXC.

12.1.1 О чем рассказывается в этой главе

Параметры функции ALG для FTP можно настроить на экране **ALG** (разд. 12.2 на стр. 171).

12.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Application Layer Gateway (ALG) и NAT

Устройство NXC может выступать в качестве шлюза прикладного уровня (Application Layer Gateway, ALG), позволяющего некоторым приложениям, плохо совместимым с трансляцией сетевых адресов (NAT), нормально функционировать в сочетании с функцией NAT, включенной на устройстве NXC. Устройство NXC динамически создает неявную сессию NAT для трафика данного приложения, передаваемого из сети WAN в локальную сеть. Функция ALG устройства NXC поддерживает все типы трансляции сетевых адресов, выполняемые устройством NXC.

FTP ALG

Функция FTP ALG позволяет организовать сквозную передачу пакетов TCP с указанным портом назначения. Если FTP-сервер находится в локальной сети, необходимо создать правила NAT (правила перенаправления портов), чтобы разрешить доступ к этому серверу из сети WAN.

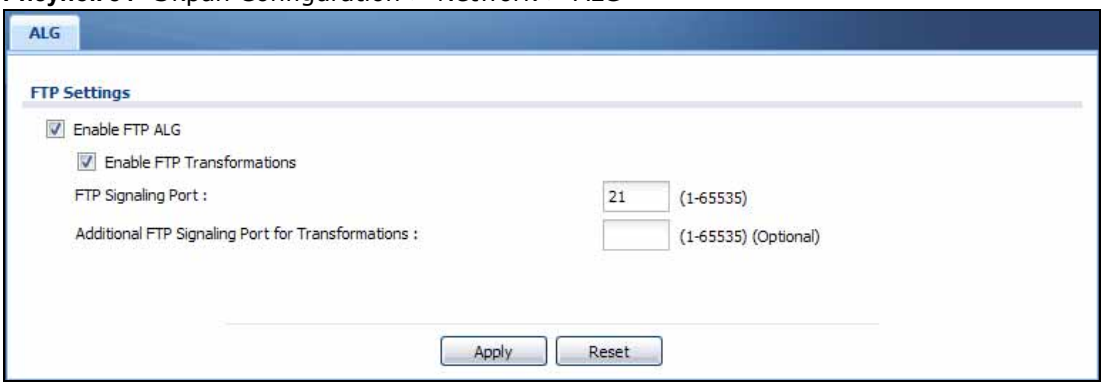
12.1.3 Подготовительные действия

Чтобы разрешить сессии, инициируемые в сети WAN, необходимо включить поддержку NAT на устройстве NXC.

12.2 Экран ALG

Чтобы открыть этот экран, выберите в меню **Configuration > Network > ALG**. С помощью этого экрана можно включить или выключить функцию ALG, а также указать номера портов, к которым она применяется.

Рисунок 84 Экран Configuration > Network > ALG



Поля экрана описаны в следующей таблице.

Таблица 78 Экран Configuration > Network > ALG

ПОЛЕ	ОПИСАНИЕ
Enable FTP ALG	Включите функцию FTP ALG для обнаружения трафика FTP (File Transfer Program) и поддержки сессий FTP при использовании трансляции сетевых адресов на устройстве NXC.
Enable FTP Transformations	Установите этот переключатель, чтобы устройство NXC модифицировало IP-адреса и номера портов, встроенные в полезные данные FTP, с целью нормального прохождения трафика при включенной функции NAT на устройстве NXC. Не включайте эту опцию, если имеется другое устройство или сервер FTP, который будет модифицировать IP-адреса и номера портов, встроенные в полезные данные FTP, с целью нормального прохождения трафика при включенной функции NAT на устройстве NXC.
FTP Signaling Port	Если для FTP-трафика используется TCP-порт, отличный от стандартного (21), укажите его здесь.
Additional FTP Signaling Port for Transformations	Если протокол FTP используется еще на одном порту TCP, укажите его номер в этом поле.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

12.3 Справочная техническая информация

В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

FTP

File Transfer Protocol (FTP) – это Интернет-протокол для передачи файлов, который работает в сети Интернет и в сетях на основе протоколов TCP/IP. Система, на которой работает сервер FTP, принимает запросы от системы, на которой запущен клиент FTP. Эта служба позволяет пользователям отправлять серверу команды на выгрузку и загрузку файлов.

13

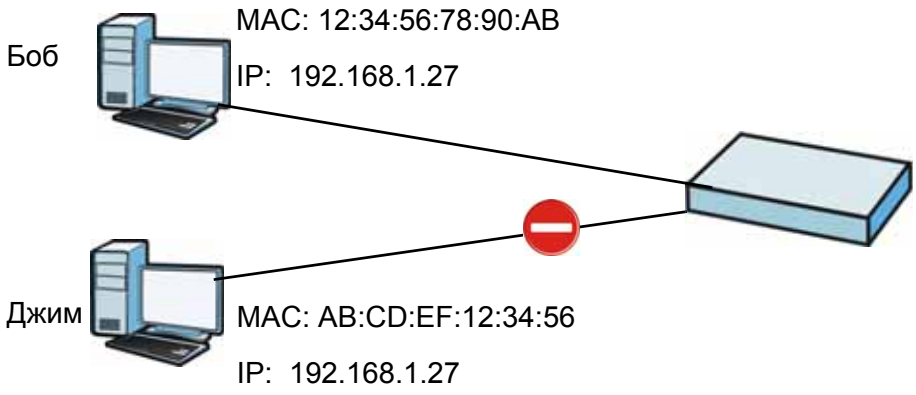
Привязка IP/MAC

13.1 Обзор

Привязка IP-адресов к MAC-адресам позволяет гарантировать получение привилегированных IP-адресов только нужными устройствами. Устройство NXC использует протокол DHCP для назначения IP-адресов и создания записей для MAC-адресов, которым были назначены все выделенные IP-адреса. Затем устройство NXC проверяет полученный список при поступлении запросов на входящие соединения. Пользователь не может вручную назначить своему компьютеру другой IP-адрес и использовать его для подключения к устройству NXC.

Допустим, были созданы привилегии доступа для IP-адреса 192.168.1.27 и для его назначения компьютеру Тима, имеющему MAC-адрес 12:34:56:78:90:AB, используется статическая запись DHCP. Механизм привязки IP/MAC отбрасывает трафик, исходящий от любого компьютера, пытающегося использовать IP-адрес 192.168.1.27 в сочетании с другим MAC-адресом.

Рисунок 85 Пример привязки IP/MAC



13.1.1 О чем рассказывается в этой главе

- Экраны **Summary** и **Edit** (разд. 13.2 на стр. 174) содержат информацию о привязке IP-адресов к MAC-адресам.
- Экран **Exempt List** (разд. 13.3 на стр. 177) содержит перечень диапазонов IP-адресов, к которым устройство NXC не применяет привязку IP/MAC.

13.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

DHCP

В основе привязки IP/MAC лежат динамические и статические записи DHCP устройства NXC.

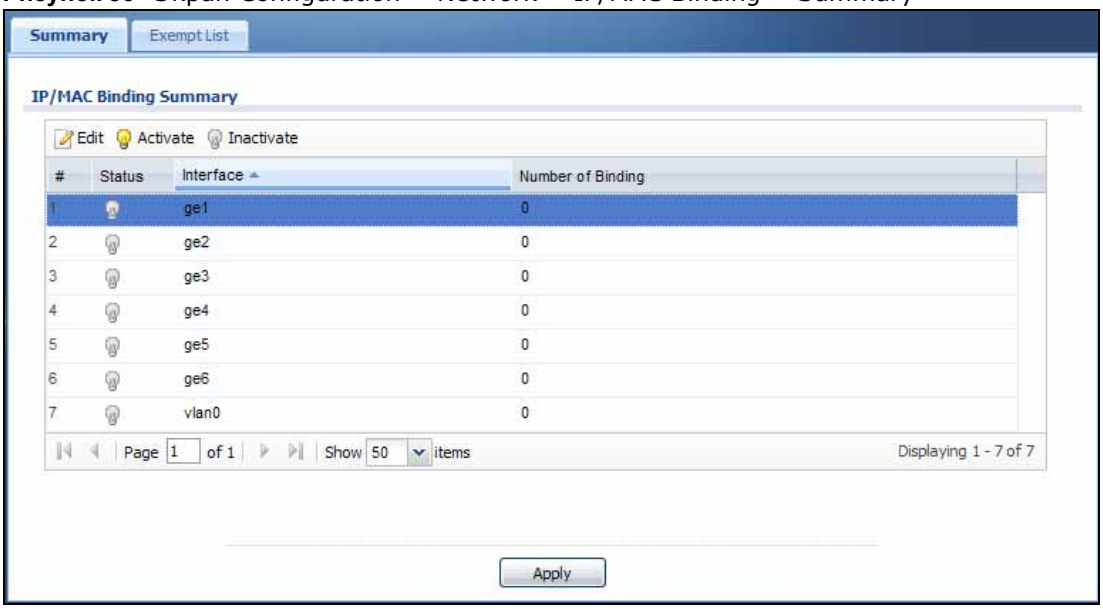
Интерфейсы, используемые с привязкой IP/MAC

Привязки адресов IP/MAC сгруппированы по интерфейсам. Привязки IP/MAC можно использовать на интерфейсах Ethernet и VLAN. На экране настроек интерфейса можно включить или отключить привязку и журналирование IP/MAC.

13.2 Экран IP/MAC Binding Summary

Чтобы открыть экран **IP/MAC Binding Summary**, выберите в меню **Configuration > Network > IP/MAC Binding**. На этом экране показано общее количество привязок IP/MAC для устройств, подключенных к каждому из поддерживаемых интерфейсов.

Рисунок 86 Экран Configuration > Network > IP/MAC Binding > Summary



Поля экрана описаны в следующей таблице.

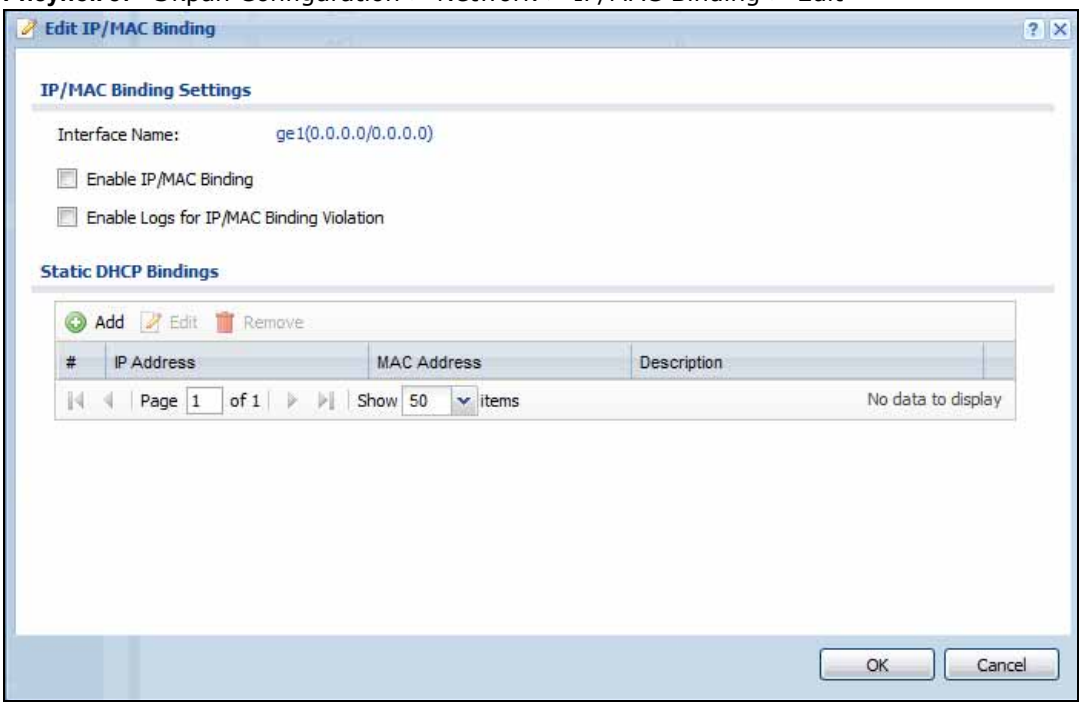
Таблица 79 Экран Configuration > Network > IP/MAC Binding > Summary

ПОЛЕ	ОПИСАНИЕ
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Interface	Это имя интерфейса, который поддерживает привязку IP/MAC.
Number of Binding	Это поле показывает общее число привязок IP/MAC и IP-адресов, которые данный интерфейс назначил по протоколу DHCP.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.

13.2.1 Экран Edit IP/MAC Binding

Чтобы открыть этот экран, выберите в меню **Configuration > Network > IP/MAC Binding > Edit**. С помощью этого экрана можно настроить параметры привязок IP/MAC-адресов для соответствующих интерфейсов.

Рисунок 87 Экран Configuration > Network > IP/MAC Binding > Edit



Поля экрана описаны в следующей таблице.

Таблица 80 Экран Configuration > Network > IP/MAC Binding > Edit

ПОЛЕ	ОПИСАНИЕ
IP/MAC Binding Settings	
Interface Name	Это поле показывает имя данного интерфейса на устройстве NXC, а также его IP-адрес и маску подсети.
Enable IP/MAC Binding	Выберите эту опцию, чтобы данный интерфейс в обязательном порядке устанавливал связь между определенными IP-адресами и определенными MAC-адресами. Это позволит исключить возможность ручной привязки связанного IP-адреса к другому устройству, подключенному к данному интерфейсу. Воспользуйтесь этой опцией, если необходимо разрешить использование определенных IP-адресов только определенным пользователям.
Enable Logs for IP/MAC Binding Violation	Выберите эту опцию, чтобы устройство NXC генерировало запись в журнале каждый раз, когда устройство, подключенное к данному интерфейсу, пытается использовать IP-адрес, который не был назначен ему устройством NXC.
Static DHCP Bindings	Эта таблица содержит список связанных IP- и MAC-адресов. Устройство NXC обращается к этой таблице в процессе назначения IP-адресов. Если MAC-адрес данного компьютера присутствует в этой таблице, устройство NXC назначит этому компьютеру соответствующий IP-адрес. Изменить содержимое этой таблицы можно также на экране редактирования настроек интерфейса.
Add	Нажатие на этот значок позволяет создать новую запись.

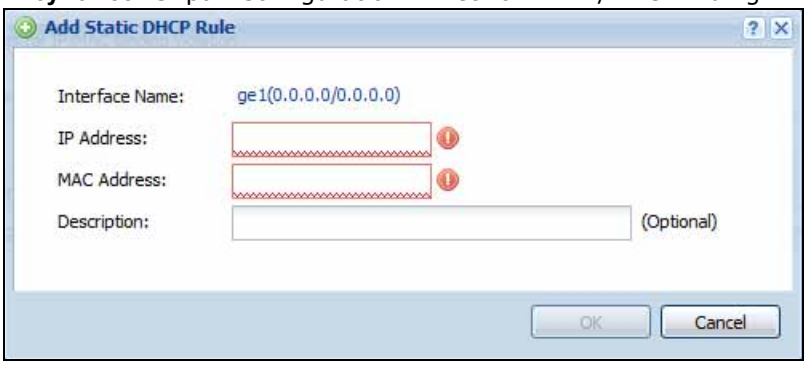
Таблица 80 Экран Configuration > Network > IP/MAC Binding > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
#	Это порядковый номер статической записи DHCP.
IP Address	Это IP-адрес, который устройство NXC назначает устройству, чей MAC-адрес указан в данной записи.
MAC Address	Это MAC-адрес устройства, которому устройство NXC назначает IP-адрес, указанный в данной записи.
Description	Описание, содержащееся в этом поле, помогает идентифицировать запись.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

13.2.2 Экран Add/Edit Static DHCP Rule

Чтобы перейти к этому экрану, выберите в меню **Configuration > Network > IP/MAC Binding > Edit**. Нажмите на пиктограмму **Add** или **Edit**, чтобы открыть следующий экран. С помощью этого экрана можно настроить параметры привязок IP/MAC-адресов для соответствующих интерфейсов.

Рисунок 88 Экран Configuration > Network > IP/MAC Binding > Edit > Add/Edit



Поля экрана описаны в следующей таблице.

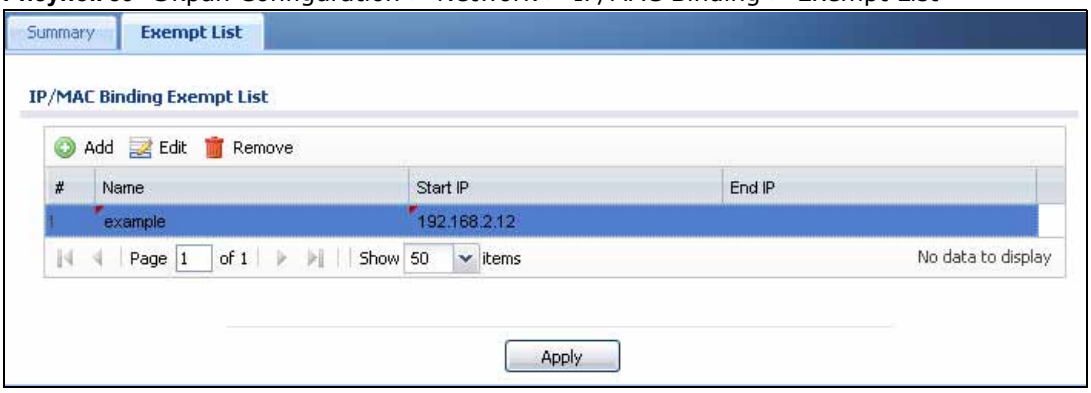
Таблица 81 Экран Configuration > Network > IP/MAC Binding > Edit > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Interface Name	Это поле показывает имя данного интерфейса на устройстве NXC, а также его IP-адрес и маску подсети.
IP Address	Укажите IP-адрес, который устройство NXC должно назначать устройству, чей MAC-адрес указан в данной записи.
MAC Address	Введите MAC-адрес устройства, которому устройство NXC должно назначить IP-адрес, указанный в этой записи.
Description	Введите описание (не более 64 печатных ASCII-символов), помогающее идентифицировать данную запись. Например, в этом поле можно указать владельца компьютера.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

13.3 Экран IP/MAC Binding Exempt List

Выберите в меню **Configuration > Network > IP/MAC Binding > Exempt List**, чтобы открыть экран **IP/MAC Binding Exempt List**. На этом экране можно указать диапазоны IP-адресов, для которых устройство NXC не будет использовать привязку IP/MAC.

Рисунок 89 Экран Configuration > Network > IP/MAC Binding > Exempt List



Поля экрана описаны в следующей таблице.

Таблица 82 Экран Configuration > Network > IP/MAC Binding > Exempt List

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
#	Это порядковый номер записи в списке привязок IP/MAC.
Name	Введите имя, помогающее идентифицировать запись.
Start IP	Введите начальный адрес из диапазона IP-адресов, для которых устройство NXC не будет использовать привязку IP/MAC.
End IP	Введите конечный адрес из диапазона IP-адресов, для которых устройство NXC не будет использовать привязку IP/MAC.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.

14

Непокидаемый портал

14.1 Обзор

Непокидаемый портал может перехватывать сетевой трафик в соответствии с политиками аутентификации до тех пор, пока пользователь, пытающийся установить соединение, не пройдет аутентификацию, как правило – на специальной веб-странице для ввода имени и пароля.

Устройство NXC включает в себя функциональность непокидаемого портала как дополнительную меру безопасности. Это означает, что все запросы на открытие веб-страниц можно изначально перенаправлять на специальную веб-страницу с требованием аутентифицировать сессию. В случае успешной аутентификации открывается доступ к остальным ресурсам сети или к Интернету.

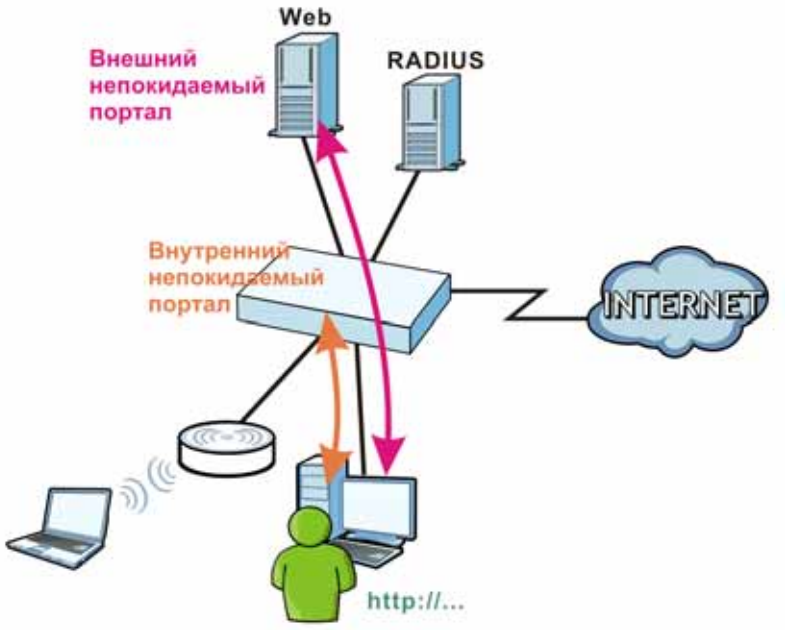
С непокидаемыми порталами часто можно встретиться в точках публичного доступа к Интернету, например, в книжных магазинах, кофейнях и отелях; при попытке открыть веб-страницу точка доступа, обслуживающая данную зону, перенаправит браузер на страницу непокидаемого портала, где будет предложено ввести свои учетные данные.

Рисунок 90 Пример непокидаемого портала

Страница непокидаемого портала появляется только один раз за время сессии аутентификации. Обычно пользователь больше не видит этого окна в пределах одной сессии, за исключением случаев, когда сессия разрывается по тайм-ауту или пользователь закрывает соединение.

14.1.1 Тип непокидаемого портала

Устройство NXC позволяет использовать либо внутренний непокидаемый веб-портал (встроенный в устройство NXC), либо внешний непокидаемый портал (размещенный на внешнем веб-сервере). Можно также настроить страницы портала по своему усмотрению. Более подробную информацию о страницах портала можно найти в разд. 14.3.1 на стр. 188 и разд. 14.3.2 на стр. 190.



Следующая таблица описывает различия между возможными вариантами веб-портала.

Таблица 83 Варианты непокидаемого портала

ВАРИАНТ	ТИП ПОРТАЛА	СТРАНИЦЫ ПОРТАЛА, СОЗДАННЫЕ ПОЛЬЗОВАТЕЛЕМ	ГДЕ ВЫПОЛНЯЕТСЯ НАСТРОЙКА
External Web Portal	Внешний	Вход в систему (Login), выход из системы (Logout), приветственная страница (Welcome), сессия (Session), страница с сообщением об ошибке (Error)	Captive Portal > Captive Portal
Default Login Page	Внутренний	н/п	Captive Portal > Login Page
Customized Login Page	Внутренний	Вход в систему (Login), доступ (Access)	
Uploaded Web Portal File	Внутренний	Вход в систему (Login), выход из системы (Logout), приветственная страница (Welcome), сессия (Session), страница с сообщением об ошибке (Error)	

14.1.2 О чем рассказывается в этой главе

- На экране **Captive Portal** (разд. 14.2 на стр. 180) указывается набор сетевых служб на основе HTTP, для которых по умолчанию будет выводиться страница непокидаемого портала при первой попытке пользователя подключиться к сети.
- На экране **Login Page** (разд. 14.3 на стр. 186) можно назначить страницу для входа в систему по умолчанию или создать адаптированную страницу.

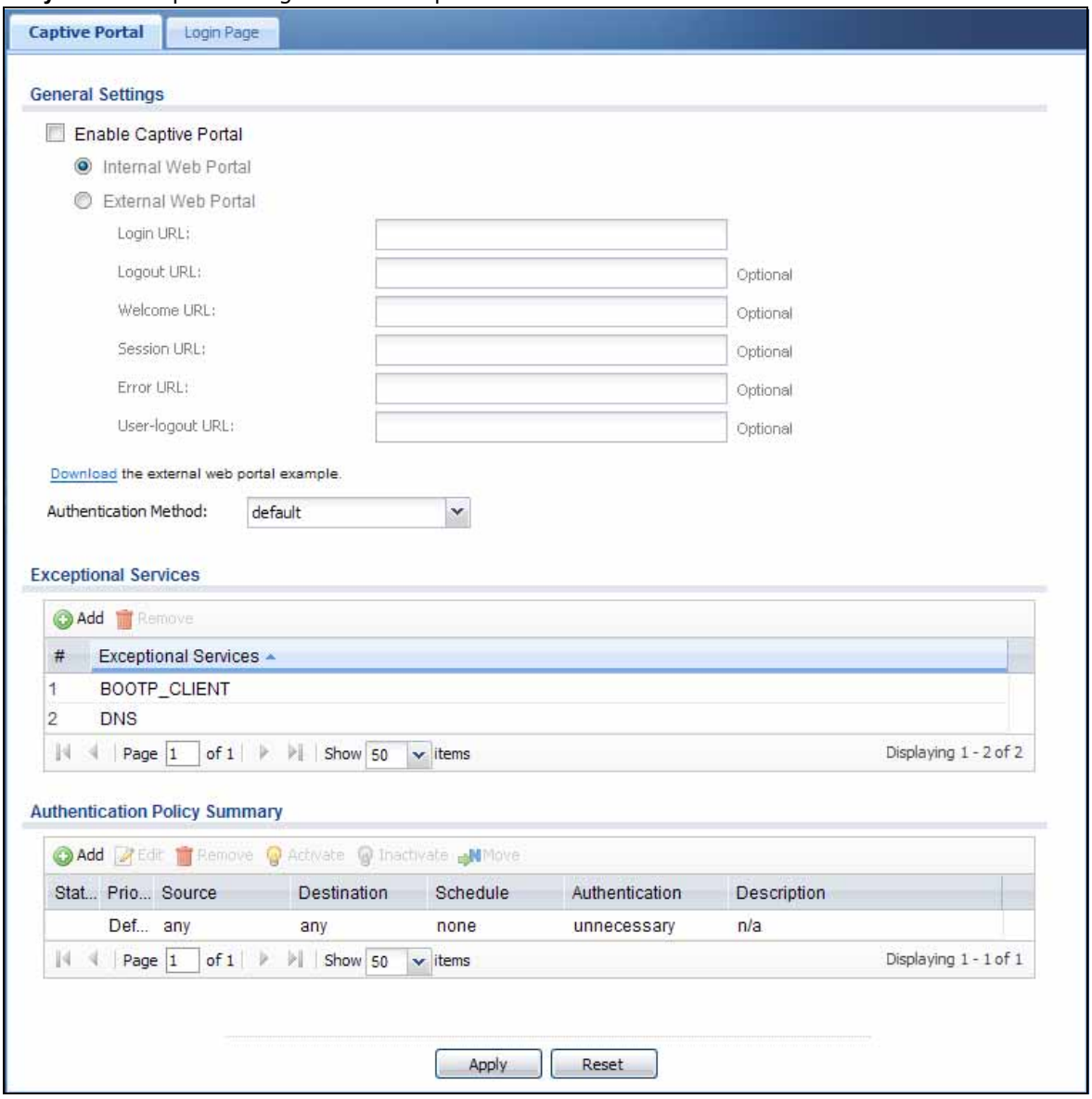
14.2 Экран Captive Portal

С помощью этого экрана можно указать перечень сетевых служб на основе HTTP, для которых по умолчанию будет выводиться страница непокидаемого портала при первой попытке клиента подключиться к сети.

Чтобы перейти к этому экрану, выберите в меню **Configuration > Captive Portal**.

Примечание: Внешний вид страницы непокидаемого портала можно изменить на экране **Login Page**; более подробную информацию см. в разд. 14.3 на стр. 186.

Рисунок 91 Экран Configuration > Captive Portal



Поля экрана описаны в следующей таблице.

Таблица 84 Экран Configuration > Captive Portal

ПОЛЕ	ОПИСАНИЕ
Enable Captive Portal	Выберите эту опцию, чтобы включить функцию непокидаемого портала. В этом случае весь сетевой трафик будет блокироваться до тех пор, пока клиент не пройдет процедуру аутентификации на специальной странице непокидаемого портала устройства NXC.
Internal Web Portal	Выберите эту опцию, если необходимо использовать страницу для входа, встроенную в устройство NXC. Страница для входа в систему появляется на экране в тот момент, когда веб-портал перехватывает сетевой трафик, предотвращая доступ неавторизованных пользователей к сети.

Таблица 84 Экран Configuration > Captive Portal (продолжение)

ПОЛЕ	ОПИСАНИЕ
External Web Portal	Выберите эту опцию, если необходимо использовать собственную страницу для входа в систему, размещенную на внешнем веб-портале, вместо страницы, встроенной в устройство NXC. Можно поменять внешний вид страницы веб-портала. Примечание: Внешний веб-сервер рекомендуется размещать в той же подсети, в которой находятся пользователи, попадающие на страницу входа в систему.
Login URL	Укажите адрес страницы для входа в систему; например, http://IP-адрес сервера IIS/login.asp. Это поле является обязательным для заполнения, если выбрана опция **External Web Portal**. Internet Information Server (IIS) – это веб-сервер, на котором размещают файлы веб-портала.
Logout URL	Укажите адрес страницы для выхода из системы; например, http://IP-адрес сервера IIS/logout.asp. Internet Information Server (IIS) – это веб-сервер, на котором размещают файлы веб-портала.
Welcome URL	Укажите адрес приветственной страницы; например, http://IP-адрес сервера IIS/welcome.asp. Internet Information Server (IIS) – это веб-сервер, на котором размещают файлы веб-портала.
Session URL	Укажите адрес страницы сессии; например, http://IP-адрес сервера IIS/session.asp. Эта страница записывает интервалы тайм-аута аренды, повторной аутентификации и сессии для данного пользователя. Для выхода из системы пользователь также может нажать кнопку logout. Internet Information Server (IIS) – это веб-сервер, на котором размещают файлы веб-портала.
Error URL	Укажите адрес страницы ошибок; например, http://IP-адрес сервера IIS/error.asp. Internet Information Server (IIS) – это веб-сервер, на котором размещают файлы веб-портала.
User-logout URL	Укажите адрес страницы, на которой пользователи могут завершить свои сессии; например, http://IP-адрес сервера IIS/userlogout.asp. Internet Information Server (IIS) – это веб-сервер, на котором размещают файлы веб-портала.
Download	Щелкните по этой ссылке, чтобы загрузить пример файла портала для информации.
Authentication Method	Выберите метод аутентификации для страницы непокидаемого портала. Метод аутентификации можно настроить на экране **Configuration > Object > Auth. Method** (гл. 25 на стр. 287). Эта опция задает метод по умолчанию для всех беспроводных клиентов, взаимодействующих с сетью через страницу непокидаемого портала. Ее можно подменить на экране **Auth. Policy Edit** (разд. 14.2.2 на стр. 184).
Exceptional Services	Эта таблица позволяет настроить исключения для сетевого трафика, перехватываемого непокидаемым порталом.
Add	Нажмите эту кнопку, чтобы добавить службу в число исключений, чей трафик пойдет в обход непокидаемого портала. Это позволяет разрешить беспрепятственное прохождение трафика при выполнении некоторых сетевых функций (например, при подключении к серверу DNS, это одно из заранее добавленных исключений по умолчанию).
Remove	Выберите ненужное исключение в таблице и нажмите эту кнопку, чтобы удалить его. После удаления исключения непокидаемый портал снова будет перехватывать весь трафик для соответствующего протокола.
#	Это порядковый номер записи в списке **Exceptional Services**.

Таблица 84 Экран Configuration > Captive Portal (продолжение)

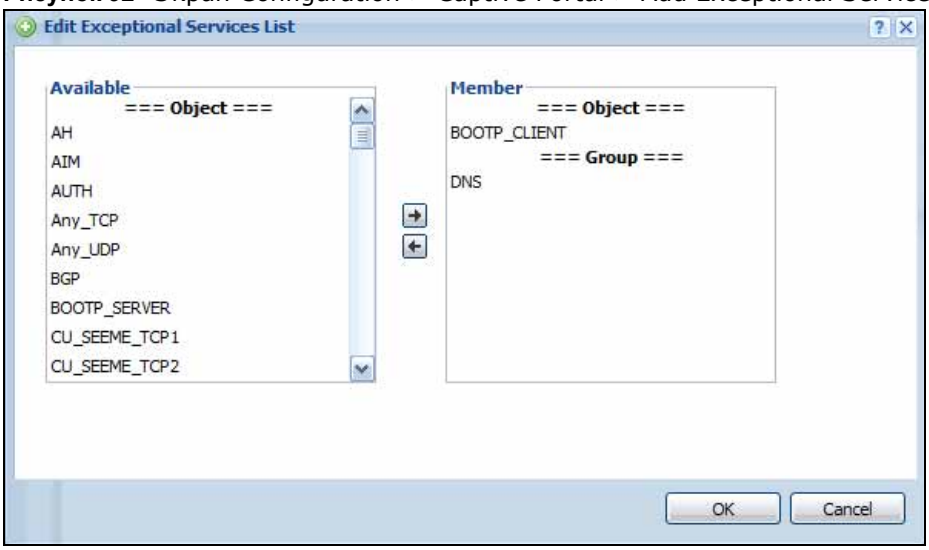
ПОЛЕ	ОПИСАНИЕ
Exceptional Services	В этом столбце перечислены службы, которые отмечены как исключения, то есть службы, чей трафик не будет перехватывать непокидаемый портал.
Authentication Policy Summary	Эта таблица описывает алгоритм реализации перехвата трафика непокидаемым порталом с использованием указанных IP-адресов источника и назначения.
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Move	Нажмите эту кнопку, чтобы назначить выбранной политике новый приоритет (**Priority**). При нажатии этой кнопки рядом с ней открывается окно с текстовым полем. Введите значение приоритета, затем нажмите клавишу [Enter].
Status	Это поле указывает на состояние политики – активна или не активна.
Priority	Это поле указывает на приоритет политики. Значения приоритета являются уникальными для каждой политики. Если необходимо изменить приоритет, воспользуйтесь кнопкой **Move**.
Source	Это поле показывает IP-адрес источника, который должна отслеживать данная политика. Политика будет применяться ко всему трафику с указанным IP-адресом источника.
Destination	Это поле показывает IP-адрес назначения, который должна отслеживать данная политика. Политика будет применяться ко всему трафику, идущему по указанному IP-адресу назначения.
Schedule	Это поле указывает на то, какие объекты расписания (если таковые существуют) применяются к данной политике. Объект расписания позволяет указать периоды времени, в которые правило является активным.
Authentication	Это поле указывает на то, требуется ли для данной политики аутентификация.
Description	Это поле содержит описание данной политики. В системе ему не соответствует никакое внутреннее значение.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

14.2.1 Добавление служб в список исключений

Этот экран позволяет управлять исключениями при перехвате трафика непокидаемым порталом. Чтобы открыть этот экран, нажмите кнопку **Add** в таблице **Exceptional Services** на экране **Captive Portal**.

Примечание: Если необходимо обеспечить нормальную работу протокола 802.1x, потребуется добавить в исключения службы BOOTP_Client и DNS.

Рисунок 92 Экран Configuration > Captive Portal > Add Exceptional Services



Поля экрана описаны в следующей таблице.

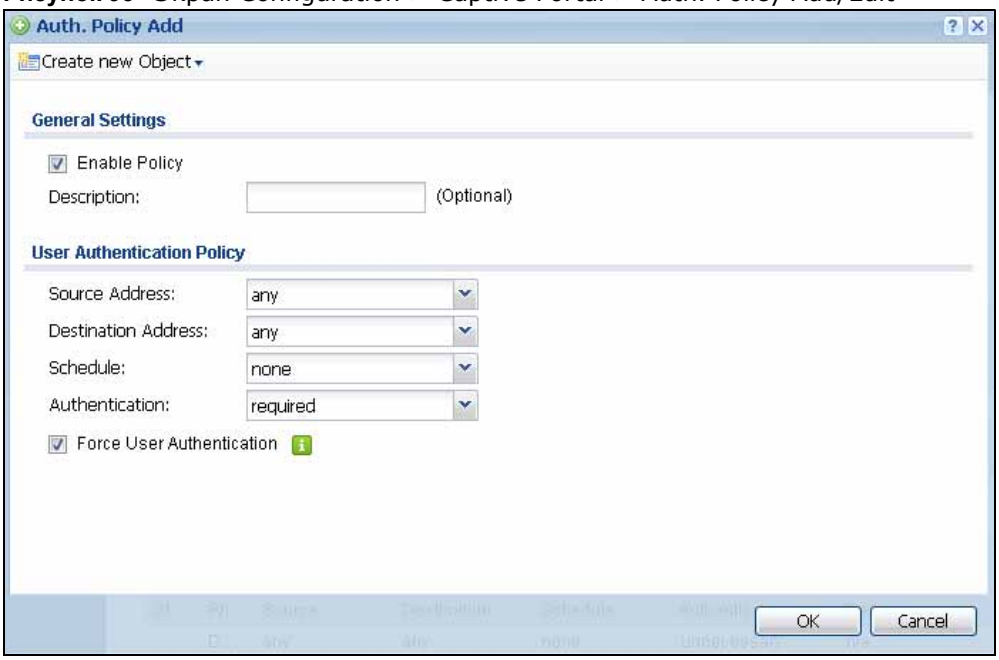
Таблица 85 Экран Configuration > Captive Portal > Add Exceptional Services

ПОЛЕ	ОПИСАНИЕ
Available	В этом поле перечислены все сетевые службы, которые могут быть отнесены к исключениям в части перехвата трафика непокидаемым порталом.
Member	В этом поле перечислены все сетевые службы, которые на текущий момент добавлены в таблицу исключений – **Exceptional Services**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

14.2.2 Экран Auth. Policy Add/Edit

Этот экран позволяет добавить политики аутентификации для перехвата трафика непокидаемым порталом. Чтобы перейти к этому экрану, нажмите на кнопку **Add** или **Edit** (для существующей политики) в таблице **Authentication Policy Summary** на экране **Captive Portal**.

Рисунок 93 Экран Configuration > Captive Portal > Auth. Policy Add/Edit



Поля экрана описаны в следующей таблице.

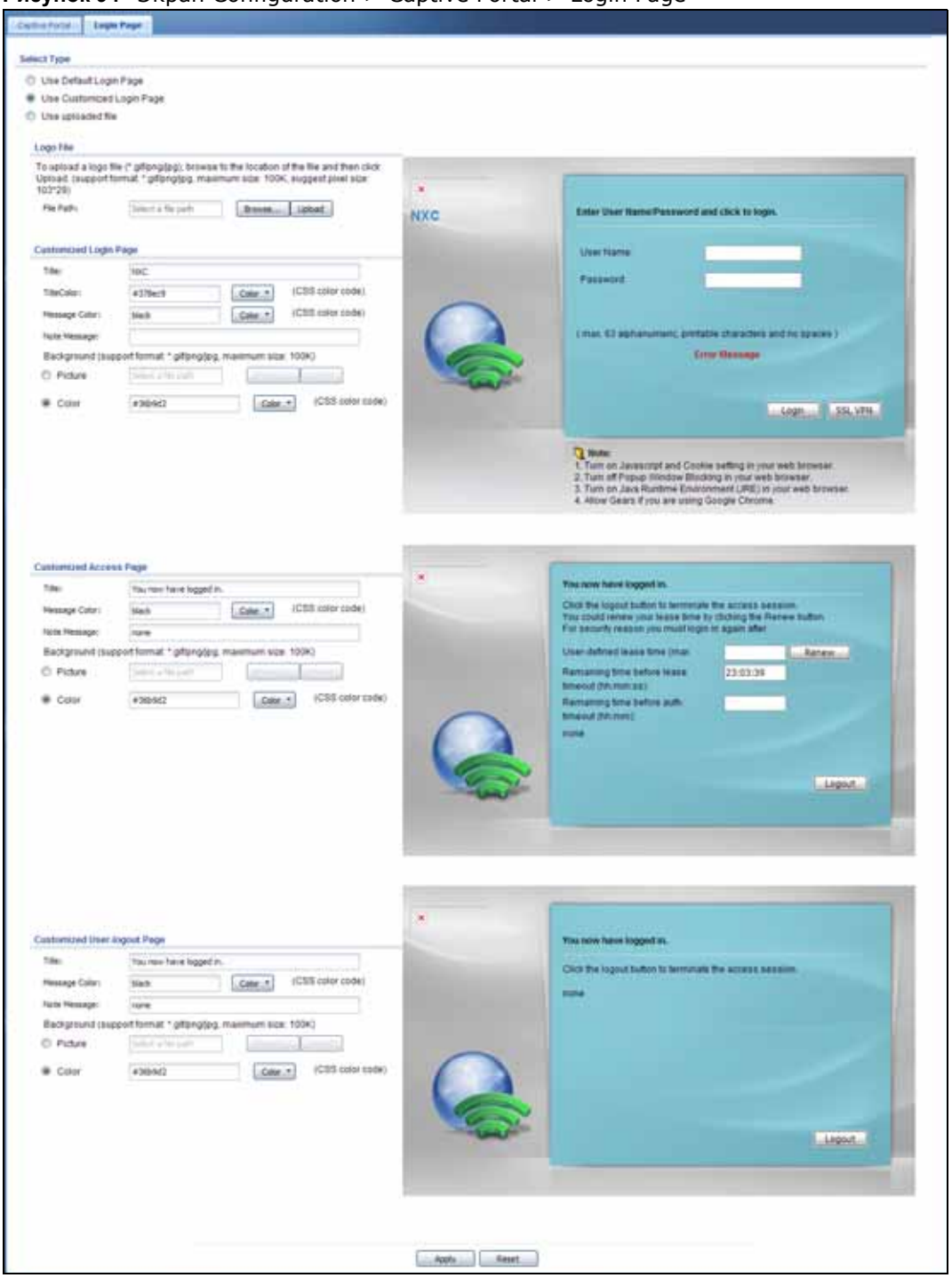
Таблица 86 Экран Configuration > Captive Portal > Auth. Policy Add/Edit

ПОЛЕ	ОПИСАНИЕ
Create New Object	Выберите тип объекта (SSID Profile, Address или Service), чтобы создать новый объект. Затем этот объект можно будет использовать при настройке правил политики аутентификации. Например, можно создать новый объект типа SSID Profile с названием «CoffeeBar», а затем тут же выбрать его из списка **SSID** на этом экране.
Enable Policy	Установите этот переключатель, чтобы включить новую политику аутентификации. Позднее можно изменить ее параметры или вообще при необходимости отключить.
Description	Введите опциональное описание политики аутентификации. Длина описания не может превышать 60 символов.
Source Address	Выберите адресный объект из списка. Если нужных объектов в списке нет, можно создать новый объект с помощью кнопки **Create New Object**. Непокидаемый портал будет перехватывать весь сетевой трафик, у которого в качестве IP-адреса источника присутствует данный адрес.
Destination Address	Выберите адресный объект из списка. Если нужных объектов в списке нет, можно создать новый объект с помощью кнопки **Create New Object**. Непокидаемый портал будет перехватывать весь сетевой трафик, у которого в качестве IP-адреса назначения присутствует данный адрес.
Schedule	Выберите расписание из списка. Если нужного объекта в списке нет, можно создать новый объект, выбрав в меню **Configuration > Object > Schedule**.
Authentication	Укажите, требуется ли для данного правила аутентификация.
Force User Authentication	Выберите эту опцию, если необходимо перенаправлять HTTP-трафик на экран входа в систему, если пользователь еще не выполнил вход.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения настроек NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

14.3 Экран Login Page

Страница для входа в систему появляется на экране в тот момент, когда непокидаемый портал перехватывает сетевой трафик, предотвращая доступ неавторизованных пользователей к сети. На этой странице можно выбрать страницу для входа в систему по умолчанию или адаптировать ее. Чтобы перейти на эту страницу, выберите в меню **Configuration > Captive Portal > Login Page**.

Рисунок 94 Экран Configuration > Captive Portal > Login Page



Поля экрана описаны в следующей таблице.

Таблица 87 Экран Configuration > Captive Portal > Login Page

ПОЛЕ	ОПИСАНИЕ
Select Type	
Use Default Login Page	Выберите эту опцию, если необходимо использовать страницу для входа, встроенную в устройство. Даже если в будущем будет создана собственная страница для входа, в любой момент можно вернуться к странице по умолчанию устройства NXC, поскольку она хранится независимо от других страниц.
Use Customized Login Page	Выберите эту опцию, если необходимо использовать собственную страницу для входа в систему вместо страницы, встроенной в устройство NXC. После выбора этой опции становятся активными дополнительные элементы управления для страницы входа, описанные ниже.
Use uploaded file	Выберите эту опцию, чтобы выгрузить файл веб-портала с собственными html-страницами на устройство NXC и использовать его. При выборе этой опции экран изменит свой вид.
Logo File	В этом разделе можно выбрать и выгрузить собственный логотип для адаптированной страницы входа в систему. Этот логотип займет место логотипа «ZyXEL» на странице по умолчанию.
File Path / Browse / Upload	Найдите файл образа или введите путь к нему в текстовом поле, а затем нажмите кнопку **Upload**, чтобы выгрузить этот файл на устройство NXC. После выгрузки этот файл образа заменяет логотип по умолчанию «ZyXEL» на странице входа в систему. Допускается использование следующих графических форматов: GIF, PNG и JPG.
Customized Login Page	В этом разделе можно поменять остальные элементы, находящиеся на странице входа в систему непокидаемого портала.
Title	Введите заголовок страницы длиной от 1 до 64 символов. В этом поле можно использовать пробелы. Этот заголовок заменит заголовок «NXC» на странице по умолчанию.
Title Color	Выберите цвет шрифта заголовка страницы. Можно воспользоваться компонентом палитры для выбора цвета или самостоятельно ввести значение цвета.
Message Color	Выберите цвет текста на экране.
Note Message	Введите примечание, которое будет отображаться под заголовком. Примечание может состоять из печатных ASCII-символов (не более 1024). В этом поле можно использовать пробелы.
Background	Укажите, как должен выглядеть фон окна. Чтобы использовать графическое изображение, выберите опцию **Picture** и выгрузите графическое изображение. Укажите путь к файлу и имя графического изображения для логотипа или воспользуйтесь кнопкой **Browse**, чтобы найти его. Допускается использование следующих графических форматов: GIF, PNG и JPG. Чтобы использовать определенный цвет, выберите опцию **Color** и укажите нужный цвет.
Customized Access Page	В этом разделе можно поменять элементы, находящиеся на странице доступа, которую пользователь видит после успешного входа в систему.
Title	Введите заголовок страницы длиной от 1 до 64 символов. В этом поле можно использовать пробелы.
Message Color	Выберите цвет текста на экране.
Note Message	Введите примечание, которое будет отображаться под заголовком. Примечание может состоять из печатных ASCII-символов (не более 1024). В этом поле можно использовать пробелы.

Таблица 87 Экран Configuration > Captive Portal > Login Page

ПОЛЕ	ОПИСАНИЕ
Background	Укажите, как должен выглядеть фон окна. Чтобы использовать графическое изображение, выберите опцию **Picture** и выгрузите графическое изображение. Укажите путь к файлу и имя графического изображения для логотипа или воспользуйтесь кнопкой **Browse**, чтобы найти его. Допускается использование следующих графических форматов: GIF, PNG и JPG. Чтобы использовать определенный цвет, выберите опцию **Color** и укажите нужный цвет.
Customized User-logout Page	В этом разделе можно поменять элементы, находящиеся на странице выхода пользователя из системы, которая появляется на экране после успешного входа в систему.
Title	Введите заголовок страницы длиной от 1 до 64 символов. В этом поле можно использовать пробелы.
Message Color	Выберите цвет текста на экране.
Note Message	Введите примечание, которое будет отображаться под заголовком. Примечание может состоять из печатных ASCII-символов (не более 1024). В этом поле можно использовать пробелы.
Background	Укажите, как должен выглядеть фон окна. Чтобы использовать графическое изображение, выберите опцию **Picture** и выгрузите графическое изображение. Укажите путь к файлу и имя графического изображения для логотипа или воспользуйтесь кнопкой **Browse**, чтобы найти его. Допускается использование следующих графических форматов: GIF, PNG и JPG. Чтобы использовать определенный цвет, выберите опцию **Color** и укажите нужный цвет.
Upload File	Этот раздел появляется на экране при выборе опции **Use uploaded file**. Он позволяет выбрать и выгрузить на устройство NXC заархивированный в формате zip файл веб-портала.
Download	Щелкните по этой ссылке, чтобы загрузить пример файла портала для информации.
File Path / Browse / Upload	Найдите файл портала или введите путь к нему в текстовом поле, а затем нажмите кнопку **Upload**, чтобы выгрузить этот файл на устройство NXC.
Download customized zip	Нажмите кнопку **Download**, чтобы загрузить файл веб-портала с устройства NXC на компьютер. Эта кнопка становится доступной для нажатия только после выгрузки заархивированного в формате zip файла веб-портала на устройство NXC.
Preview	Нажмите эту кнопку, чтобы вывести на экран соответствующую страницу портала, который был выгружен на устройство NXC. Эти кнопки становятся доступными для нажатия только после выгрузки соответствующих страниц портала на устройство NXC.
Restore customization file to default	Нажмите кнопку **Restore**, чтобы снова сделать на устройстве NXC активной встроенную страницу для входа в систему по умолчанию.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

14.3.1 Собственные страницы для входа в систему и доступа

Ниже приведен перечень элементов, которые можно менять на страницах входа в систему и доступа.

Рисунок 95 Изменение страницы входа в систему

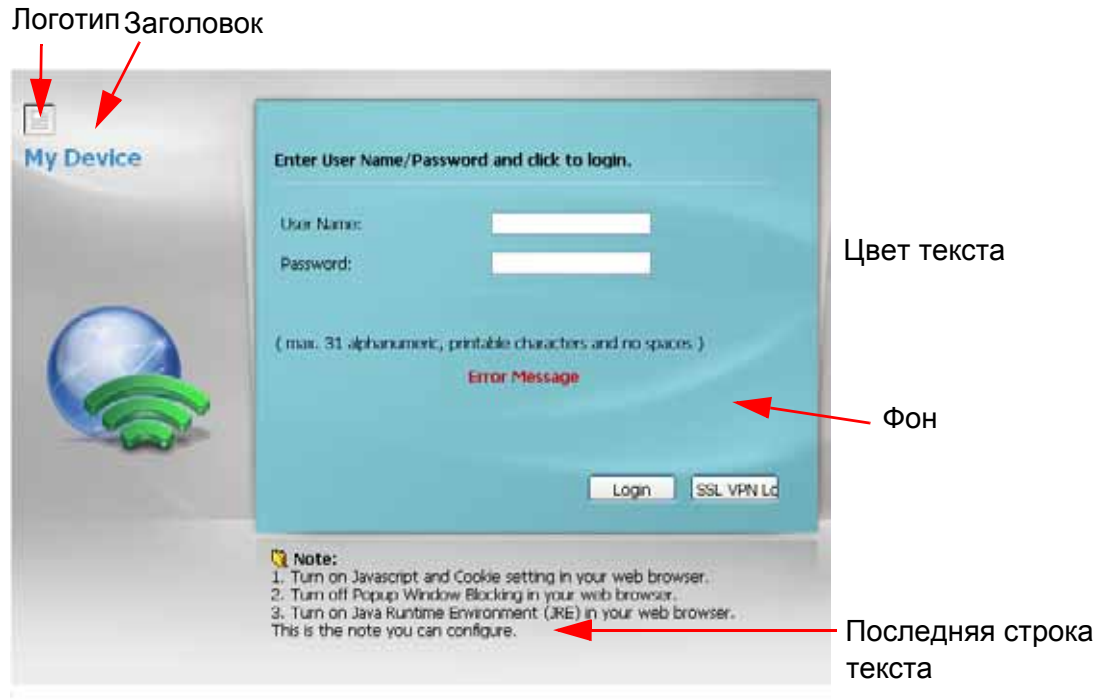
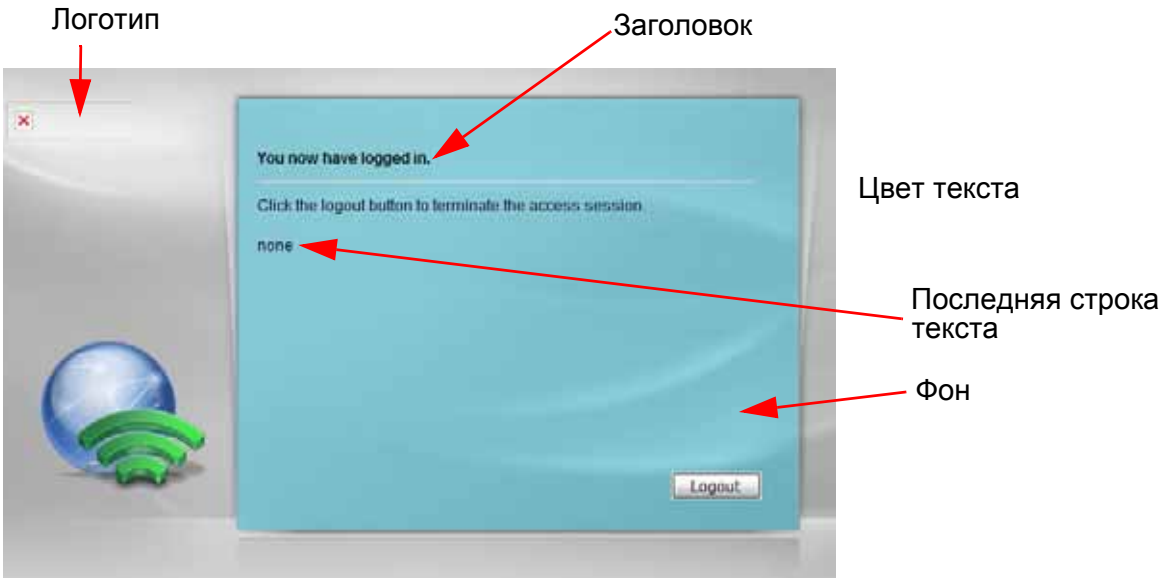


Рисунок 96 Изменение страницы доступа

Рисунок 97 Изменение страницы выхода из системы



Указать нужные цвета можно одним из перечисленных ниже способов:

- Нажмите кнопку **Color**, чтобы открыть экран с цветами, нормально отображающимися в Интернете, и выберите нужный цвет.
- Введите название нужного цвета.
- Введите шестизначное шестнадцатеричное число с символом «решетка» (#) в качестве префикса, которое представляет желаемый цвет. Например, число «#000000» соответствует черному цвету.
- Введите префикс «rgb», а следом за ним – значения для красного, зеленого и синего цветов в скобках, разделенные запятыми. Например, строка «rgb(0,0,0)» соответствует черному цвету.

Выбранный цвет должен отобразиться на экране предварительного просмотра, который находится справа, после щелчка по другому полю и нажатия на кнопку **Apply** или клавишу [ENTER]. Если желаемый цвет не отобразится, то, возможно, браузер его не поддерживает. Попробуйте выбрать другой цвет.

14.3.2 Сведения о внешнем или выгруженном на устройство веб-портале

Если используется внешний веб-портал или на устройство NXC был выгружен файл веб-портала, можно поменять внешний вид страниц веб-портала. Ниже приведены несколько примеров.

Рисунок 98 Пример страницы для входа в систему внешнего веб-портала

Рисунок 99 Пример приветственной страницы для входа в систему внешнего веб-портала

Рисунок 100 Пример страницы сессии внешнего веб-портала

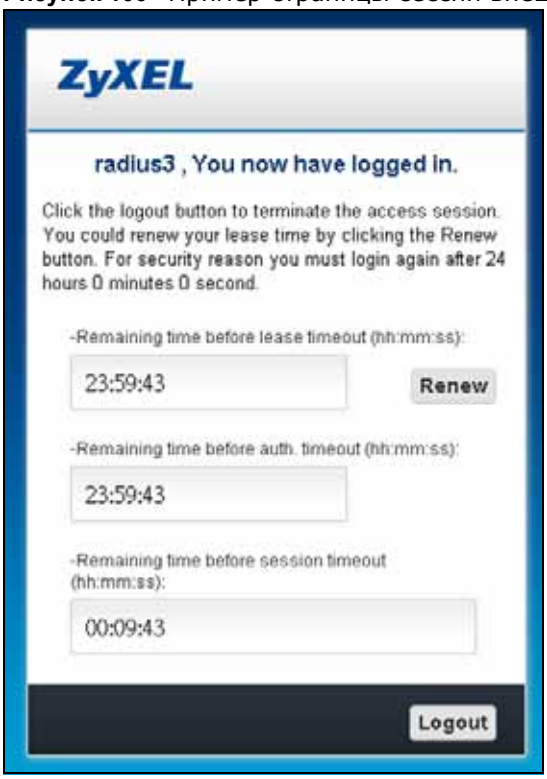


Рисунок 101 Пример страницы выхода из системы внешнего веб-портала

Рисунок 102 Пример страницы выхода пользователя из системы внешнего веб-портала

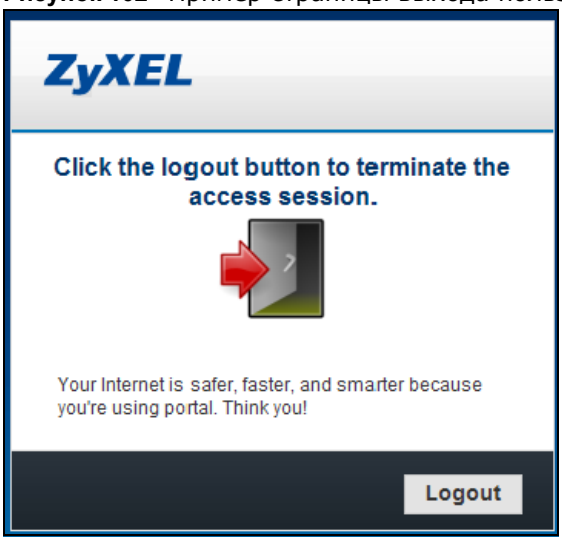


Рисунок 103 Пример страницы ошибки внешнего веб-портала

Ниже приведены коды ошибок, которые устройство NXC отправляет странице ошибок внешнего веб-портала.

Таблица 88 Коды ошибок для страницы ошибок внешнего веб-портала

КОД ОШИБКИ	ЗАГОЛОВОК	СООБЩЕНИЕ
-1	Login denied (Отказано в доступе)	Validation failed (Не удалось пройти проверку)
-2	Login denied (Отказано в доступе)	Login attempt from a locked out address (Попытка входа в систему с заблокированного адреса)
-3	Login denied (Отказано в доступе)	Simultaneous admin/access logons or users have reached the maximum number (Попытка одновременного входа в систему под учетной записью администратора, или достигнуто максимальное число одновременных подключений)

Ниже приведено описание параметров HTTP, которые устройство NXC использует для обращения по внешним ссылкам.

Таблица 89 Параметры HTTP для внешних ссылок

ПАРАМЕТР	ОПИСАНИЕ	СТРАНИЦА ВХОДА	ПРИВЕТ-СТВЕННАЯ СТРАНИЦА	СТРАНИЦА СЕССИИ	СТРАНИЦА ВЫХОДА	СТРАНИЦА ОШИБКИ
gw_addr	IP-адрес устройства NXC	V	V	V	V	
error_num	Код ошибки входа в систему					V
auth_hour	Количество часов, оставшихся до повторной аутентификации по тайм-ауту			V		
auth_min	Количество минут, оставшихся до повторной аутентификации по тайм-ауту			V		
auth_sec	Количество секунд, оставшихся до повторной аутентификации по тайм-ауту			V		
lease_time	Общее количество секунд, оставшихся до окончания срока аренды по тайм-ауту			V		
username	Имя пользователя для входа в систему			V		
cgi_str	CGI для имени пользователя. Тип для администратора – «admin.cgi», тип для пользователя – «login.cgi».	V				
Ses_time	Тайм-аут для сессии учета			V		

15

Служба обнаружения местоположения в реальном времени (RTLS)

15.1 Обзор

Служба обнаружения местоположения в реальном времени Ekahau RTLS (Real Time Location Service) отслеживает запитываемые от батарей теги Wi-Fi, присоединенные к точкам доступа, которыми управляет устройство NXC, для создания карт, оповещений и отчетов.

Центральным звеном системы RTLS является RTLS-контроллер Ekahau (Ekahau RTLS Controller). Это серверное программное обеспечение, работающее на компьютерах под управлением Windows, отслеживает и обнаруживает теги Ekahau на основе измерений силы сигнала Wi-Fi. Используйте устройство NXC в сочетании с RTLS-системой Ekahau для измерения силы сигнала на точках доступа (Integrated Approach / Blink Mode, интегрированный подход / «маячковый» режим).

Приведенный ниже пример иллюстрирует интегрированный подход RTLS-системы Ekahau («маячковый» режим).

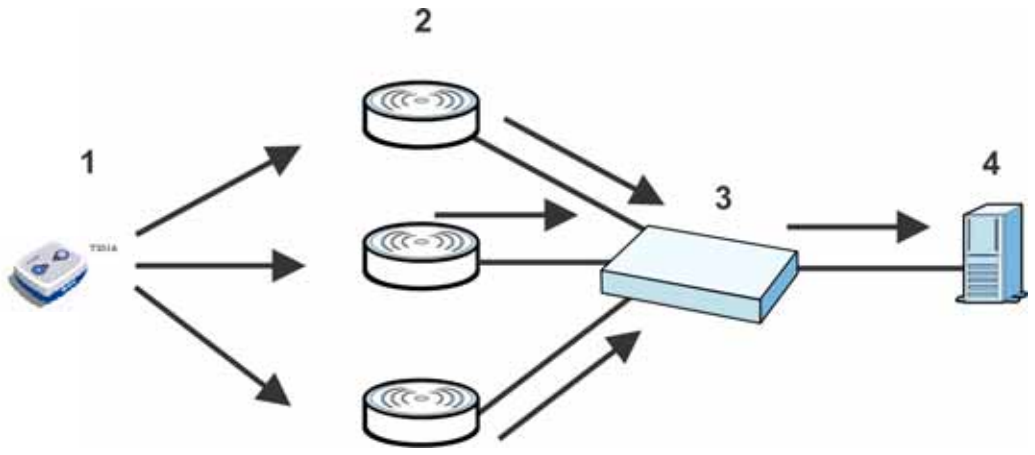
1 Тег Wi-Fi отправляет «маячковые» пакеты через указанные интервалы (или при наступлении определенных событий, таких, как движение или нажатие кнопки).

2 Точки доступа принимают «маячковые» пакеты, измеряют силу сигнала и пересылают сведения о ней устройству NXC.

3 Устройство NXC пересылает данные измерений силы сигнала на RTLS-контроллер Ekahau.

4 RTLS-контроллер Ekahau рассчитывает положение тегов.

Рисунок 104 Пример работы RTLS



15.1.1 О чем рассказывается в этой главе

Экран **RTLS** (разд. 15.3 на стр. 196) позволяет сконфигурировать управляемые точки доступа для работы в качестве элементов RTLS-системы Ekahau для отслеживания Wi-Fi-тегов Ekahau.

15.2 Подготовительные действия

Потребуется:

- Не менее трех точек доступа, управляемых устройством NXC (чем больше количество точек доступа – тем лучше, поскольку от этого напрямую зависит объем информации, который RTLS-контроллер Ekahau получает для расчета местоположения тегов)
- IP-адреса для Wi-Fi-тегов Ekahau
- Рекомендуется использовать выделенную сеть RTLS
- RTLS-контроллер Ekahau в «маячковом» режиме со включенной функцией TZSP Updater
- Правила межсетевого экрана, разрешающие прохождение RTLS-трафика – в случае, если межсетевой экран NXC включен или RTLS-контроллер Ekahau находится за межсетевым экраном.

Например, если RTLS-контроллер Ekahau находится за межсетевым экраном, необходимо открыть на межсетевом экране порты 8550, 8553 и 8569, чтобы разрешить прохождение трафика от точек доступа к RTLS-контроллеру Ekahau.

В приведенной ниже таблице перечислены номера портов по умолчанию и типы пакетов, которые использует служба RTLS.

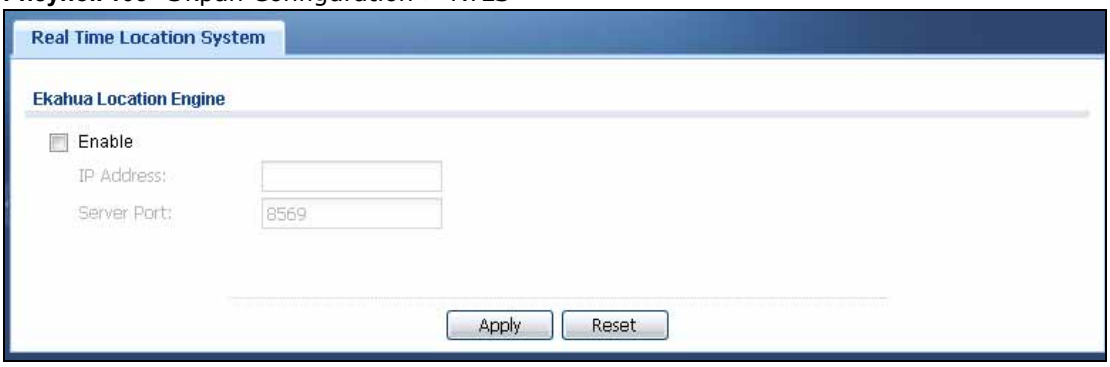
Таблица 90 Номера портов для трафика RTLS

НОМЕР ПОРТА	ТИП	ОПИСАНИЕ
8548	TCP	Обновление сведений о местоположении Ekahau T201.
8549	UDP	Обновление сведений о местоположении Ekahau T201.
8550	TCP	Протокол обслуживания тегов Ekahau T201 и пользовательский интерфейс RTLS-контроллера Ekahau.
8552	UDP	Протокол определения местонахождения Ekahau
8553	UDP	Протокол обслуживания Ekahau
8554	UDP	Обновление встроенного программного обеспечения Ekahau T301
8560	TCP	Веб-интерфейс Ekahau Vision
8562	UDP	Обновление встроенного программного обеспечения Ekahau T301W
8569	UDP	Порт обработчика Ekahau TZSP

15.3 Настройка службы RTLS

Выберите в меню **Configuration > RTLS**, чтобы открыть этот экран. На этом экране можно включить или отключить службу RTLS (Real Time Location System), а также указать IP-адрес и порт сервера RTLS-контроллера Ekahau.

Рисунок 105 Экран Configuration > RTLS



Поля экрана описаны в следующей таблице.

Таблица 91 Экран Configuration > RTLS

ПОЛЕ	ОПИСАНИЕ
Enable	Выберите эту опцию, чтобы использовать Wi-Fi для отслеживания местоположения Wi-Fi-тегов Ekahau.
IP Address	Укажите IP-адрес RTLS-контроллера Ekahau.
Server Port	Укажите номер порта сервера RTLS-контроллера Ekahau.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

16

Межсетевой экран

16.1 Обзор

Межсетевой экран используют для блокировки или разрешения служб, которые используют статические номера портов. Кроме того, межсетевой экран может ограничивать количество пользовательских сессий.

16.1.1 О чем рассказывается в этой главе

- Экраны **Firewall** (разд. 16.2 на стр. 200) позволяют включать и отключать межсетевой экран и асимметричные маршруты, а также создавать и настраивать правила межсетевого экрана.
- Экраны **Session Control** (разд. 16.3 на стр. 205) позволяют ограничить количество одновременных сессий трансляции сетевых адресов (NAT)/сессий на межсетевом экране, которые может использовать клиент.

16.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Контроль состояния соединений

Устройство NXC оснащено межсетевым экраном с контролем состояния соединений (Stateful Inspection). Устройство NXC ограничивает доступ посредством фильтрации пакетов данных в соответствии с заданными правилами доступа. Кроме того, межсетевой экран анализирует сессии. Например, трафик из одной зоны может быть запрещен, если он не инициирован компьютером, находящимся в другой зоне.

Зоны

Зона – это группа интерфейсов. Интерфейсы устройства NXC объединяются в различные зоны, исходя из потребностей. Можно создавать правила межсетевого экрана, которые будут применяться к данным, передаваемым между зонами и даже между разными интерфейсами в пределах одной зоны.

Алгоритм работы межсетевого экрана по умолчанию

Правила межсетевого экрана объединены в группы по направлениям движения пакетов, к которым они применяются. Ниже описан алгоритм работы межсетевого экрана по умолчанию для трафика, проходящего через устройство NXC в различных направлениях.

Таблица 92 Алгоритм работы межсетевого экрана по умолчанию

ИЗ ЗОНЫ В ЗОНУ	АЛГОРИТМ РАБОТЫ
Из ANY в ANY	Разрешается трафик, не соответствующий ни одному из правил межсетевого экрана. Например, разрешается трафик из локальной сети в сеть WAN, из локальной сети в DMZ и из локальной сети в сеть WLAN. Сюда относится также трафик, идущий от или к интерфейсам, не приписанным ни к одной из зон (внезональный трафик).

Правила для трафика, идущего к устройству NXC

Правила для корпоративной сети (**EnterpriseWLAN**), обозначенные как **To Zone** («в зону»), применяются к трафику, который поступает на само устройство NXC. По умолчанию:

- Межсетевой экран разрешает всем компьютерам обращаться к устройству NXC и управлять им.

При создании правила межсетевого экрана для пакетов, идущих непосредственно на устройство NXC, удостоверьтесь, что оно не вступает в конфликт с правилом управления службами. Устройство NXC проверяет правила межсетевого экрана до того, как применяются правила управления службами для трафика, идущего на устройство NXC.

Можно создать правило To-NXC на межсетевом экране (с направлением **From Any To EnterpriseWLAN**) для трафика, идущего с какого-либо интерфейса, не приписанного ни к одной зоне.

Глобальные правила межсетевого экрана

Правила межсетевого экрана, у которых в качестве направления пакетов указано «**from any**» и/или «**to any**», называются глобальными правилами межсетевого экрана. Глобальные правила межсетевого экрана – это единственный тип правил, которые применяются к интерфейсам, не приписанным ни к одной зоне. Правила типа «**from any**» применяются к трафику, идущему с определенного интерфейса, а правила типа «**to any**» – к трафику, идущему на определенный интерфейс.

Критерии правил межсетевого экрана

Устройство NXC проверяет следующие параметры трафика на соответствие критериям правил межсетевого экрана: расписание, имя пользователя (имя для входа на устройство NXC), IP-адрес источника, IP-адрес назначения и тип протокола IP для сетевого трафика (в порядке, перечисленном выше). Если трафик соответствует критериям, описанным в правиле, устройство NXC применяет к нему действие, указанное в правиле.

Правила межсетевого экрана, привязанные к имени пользователя

В правилах межсетевого экрана можно указывать пользователей и пользовательские группы. Например, если необходимо разрешить определенному пользователю доступ к некоторой зоне с любого компьютера в случае успешного входа на устройство NXC, можно создать правило,

единственным критерием которого будет имя пользователя. Если потребуется, можно включить в это правило дополнительный критерий – расписание, тогда указанный пользователь сможет получать доступ к сети только в определенные часы или дни. Активация правила межсетевого экрана, привязанного к имени пользователя, происходит в момент входа пользователя на устройство NXC. Соответственно, такое правило перестает действовать при выходе пользователя с устройства NXC.

Ограничения на сессии

Доступ к устройству NXC или сетевым ресурсам через устройство NXC требует установления сессии NAT и соответствующей сессии на межсетевом экране. Одноранговые приложения, такие, как приложения для обмена файлами, могут использовать большое количество NAT-сессий. Один клиент может захватить все доступные NAT-сессии и помешать остальным клиентам установить соединение с устройством NXC. Устройство NXC позволяет ограничить количество одновременных NAT-сессий/сессий на межсетевом экране, которые может использовать один клиент.

Асимметричные маршруты

Если IP-адрес альтернативного шлюза в локальной сети находится в той же подсети, что и IP-адрес устройства NXC в локальной сети, то возвратный трафик может идти в обход устройства NXC. Эта ситуация называется асимметричным или «треугольным» маршрутом. Это вынуждает устройство NXC сбрасывать соединение, поскольку оно не получает подтверждения.

Возможно, придется разрешить использование топологии с асимметричными маршрутами в сети на устройстве NXC (то есть сделать так, чтобы соединение не сбрасывалось). Разрешение асимметричных маршрутов может, однако, привести к тому, что трафик из сети WAN пойдет непосредственно в локальную сеть, минуя устройство NXC.

16.2 Экран Firewall

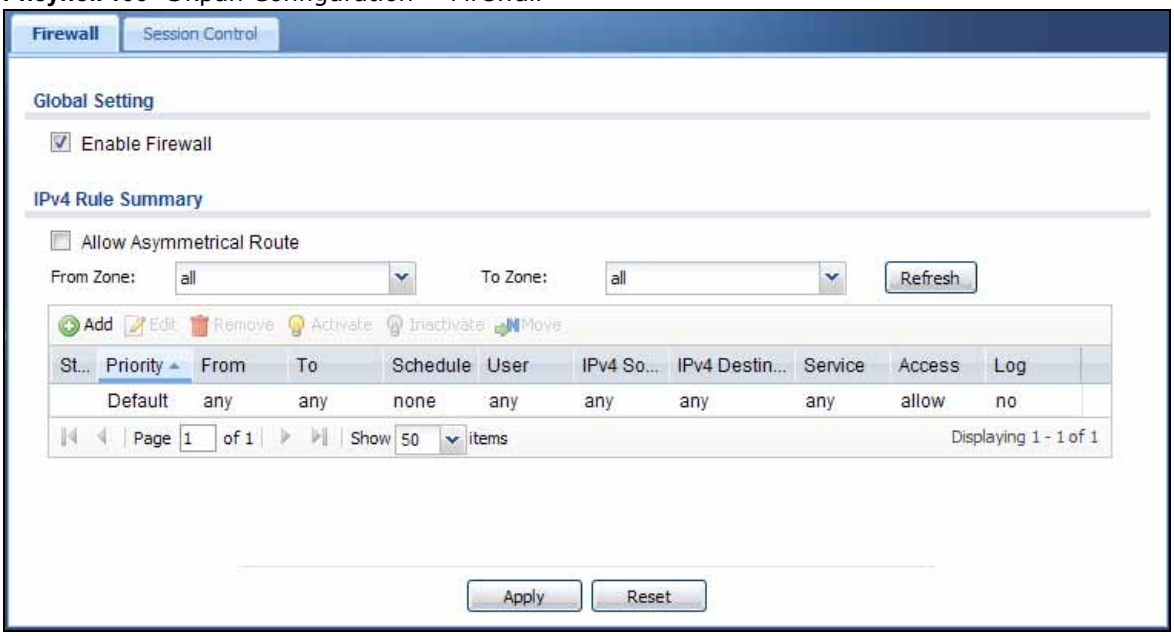
Ниже приводится описание возможностей, доступных пользователю на экране Firewall.

Выберите в меню **Configuration > Firewall**, чтобы открыть экран **Firewall**. С помощью этого экрана можно включать и отключать сам межсетевой экран и асимметричные маршруты, а также создавать, менять и просматривать уже имеющиеся правила межсетевого экрана. Укажите, из какой зоны приходят пакеты, и в какую зону они направляются, чтобы вывести на экран только правила, соответствующие выбранному направлению. Обратите внимание на следующее.

- При включении внутризональной блокировки трафика (см. главу, посвященную зонам) межсетевой экран автоматически создает (неявные) правила, запрещающие прохождение пакетов между интерфейсами указанной зоны.
- Помимо настройки межсетевого экрана необходимо будет создать правила NAT, разрешающие компьютерам в сети WAN доступ к устройствам в локальной сети.
- Устройство NXC применяет параметры NAT (трансляции сетевых адресов назначения) до того, как применить правила межсетевого экрана. К примеру, если в таблице NAT создана запись, которая перенаправляет трафик WAN на IP-адрес в локальной сети, после создания соответствующего правила на межсетевом экране, разрешающего прохождение такого трафика, необходимо будет указать IP-адрес в локальной сети в качестве адреса назначения.

- Порядок расположения правил имеет очень большое значение, поскольку применение правил происходит последовательно.

Рисунок 106 Экран Configuration > Firewall



Поля экрана описаны в следующей таблице.

Таблица 93 Экран Configuration > Firewall

ПОЛЕ	ОПИСАНИЕ
General Settings	
Enable Firewall	Установите этот переключатель, чтобы активировать межсетевой экран. После активации межсетевого экрана устройство NXC начинает осуществлять управление доступом.
Allow Asymmetrical Route	Если IP-адрес альтернативного шлюза в локальной сети находится в той же подсети, что и IP-адрес устройства NXC в локальной сети, то возвратный трафик может идти в обход устройства NXC. Эта ситуация называется асимметричным или «треугольным» маршрутом. Это вынуждает устройство NXC сбрасывать соединение, поскольку оно не получает подтверждения. Установите этот переключатель, чтобы разрешить на устройстве NXC использование топологии с асимметричными маршрутами в сети (то есть сделать так, чтобы соединение не сбрасывалось). Примечание: Разрешение асимметричных маршрутов может, однако, привести к тому, что трафик из сети WAN пойдет непосредственно в локальную сеть, минуя устройство NXC.

Таблица 93 Экран Configuration > Firewall (продолжение)

ПОЛЕ	ОПИСАНИЕ
From Zone / To Zone	Этот параметр определяет направление прохождения пакетов. Выберите зону, из которой приходят пакеты, и зону, в которую они идут. Правила межсетевого экрана объединены в группы по направлениям движения пакетов, к которым они применяются. Например, направление «From **LAN** to **LAN**» означает, что пакеты идут от компьютера или подсети, находящихся в локальной сети, к другому компьютеру или подсети, находящимся в локальной сети. Опция «From **any**» показывает все правила межсетевого экрана для трафика, идущего к зоне, указанной в поле **To Zone**. Опция «To **any**» показывает все правила межсетевого экрана для трафика, идущего от зоны, указанной в поле **From Zone**. Опция «From **any** to **any**» показывает все правила межсетевого экрана. Правила типа «To **EnterpriseWLAN**» предназначены для трафика, адресом назначения которого является устройство NXC. Они определяют, какие компьютеры могут управлять устройством NXC.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Move	Чтобы изменить позицию правила в нумерованном списке, выберите это правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести это правило. Чтобы перенести правило на указанную позицию, введите нужное значение и нажмите клавишу [ENTER]. Порядок расположения правил имеет большое значение, поскольку правила применяются в порядке нумерации.
Перечисленные ниже поля доступны только для чтения. Они содержат общую информацию о созданных правилах, которые применяются к трафику, идущему в выбранном направлении.	
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Priority	Это позиция данного правила межсетевого экрана в глобальном списке правил (включая все правила типа through-NXC и to-NXC). Порядок расположения правил имеет очень большое значение, поскольку применение правил происходит последовательно. Опция **Default** позволяет увидеть алгоритм работы межсетевого экрана по умолчанию, который устройство NXC выполняет для трафика, который не соответствует ни одному из правил межсетевого экрана.
From To	Эти поля определяют направление движения пакетов, к которому применяется данное правило межсетевого экрана.
Schedule	Это поле показывает объект расписания, который использует данное правило. Опция **none** означает, что правило – если оно включено – действует постоянно.
User	В этом поле содержится имя пользователя или группы пользователей, к которым применяется данное правило межсетевого экрана.
IPv4 Source	Это поле показывает объект адреса источника, к которому применяется данное правило межсетевого экрана.
IPv4 Destination	Это поле показывает объект адреса назначения, к которому применяется данное правило межсетевого экрана.

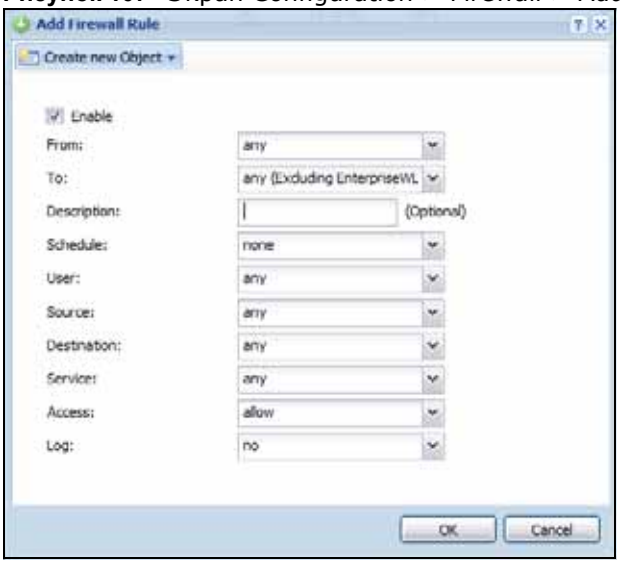
Таблица 93 Экран Configuration > Firewall (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service	Это поле показывает объект службы, к которому применяется данное правило межсетевого экрана.
Access	Это поле указывает на то, как ведет себя межсетевой экран: тихо отбрасывает пакеты (**deny**), отбрасывает пакеты и отправляет пакет сброса TCP отправителю (**reject**) или разрешает прохождение пакетов (**allow**).
Log	Это поле указывает на то, создается ли сообщение в журнале (и оповещение), если пакеты соответствуют данному правилу, или нет.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

16.2.1 Экран Add/Edit Firewall

Чтобы перейти к этому экрану, нажмите на пиктограмме **Edit** или **Add** на экране Firewall.

Рисунок 107 Экран Configuration > Firewall > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 94 Экран Configuration > Firewall > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Create new Object	С помощью этой кнопки можно создать любые новые объекты настроек, которые понадобятся на этом экране.
Enable	Установите этот переключатель, чтобы активировать данное правило межсетевого экрана.
From To	Для правил типа through-NXC выберите направление движения пакетов, к которому применяется данное правило. Значение **any** означает все интерфейсы. **EnterpriseWLAN** означает пакеты, для которых адресом назначения является само устройство NXC.
Description	Введите имя-описание правила межсетевого экрана (не более 60 печатных ASCII-символов). В этом поле можно использовать пробелы.

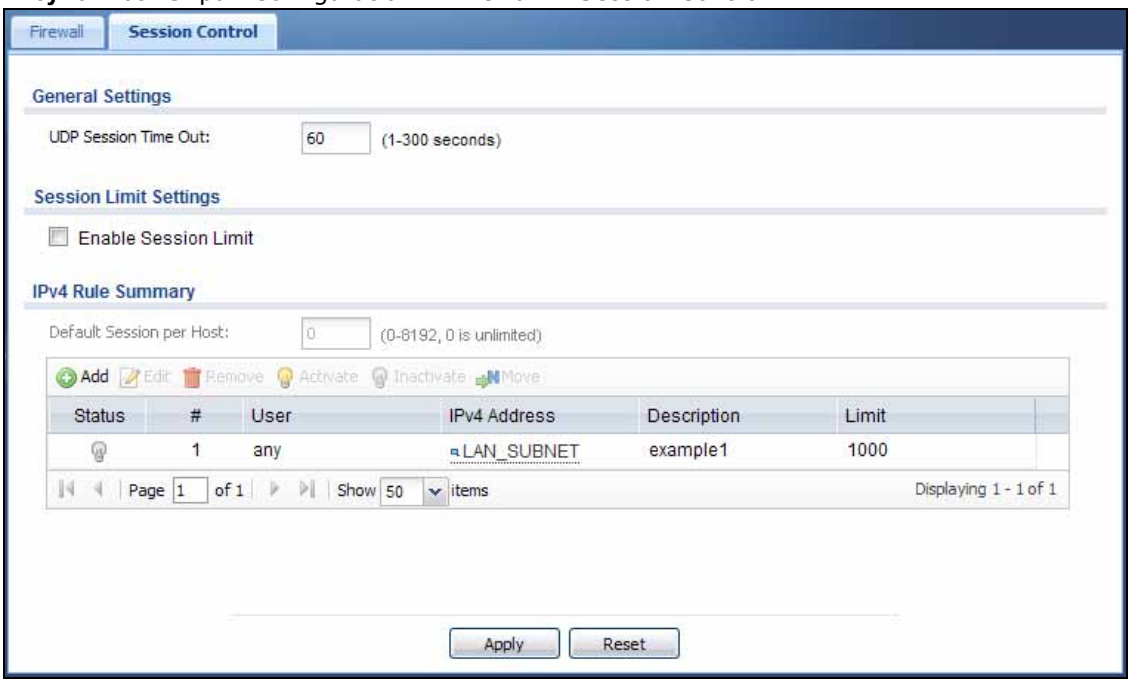
Таблица 94 Экран Configuration > Firewall > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Schedule	Выберите расписание, которое определяет интервалы применения данного правила. Если расписание не требуется, выберите опцию **none** – в этом случае правило будет действовать всегда.
User	Это поле недоступно при настройке правила типа to-NXC. Выберите имя пользователя или группы пользователей, к которым применяется данное правило. Активация этого правила межсетевого экрана происходит только тогда, когда указанный пользователь входит в систему. При выходе пользователя из системы правило действовать перестает. Если не требуется привязывать правило к определенному пользователю, выберите опцию **any**. Примечание: Если вместо опции **any** в поле ниже указан IP-адрес источника (или группа адресов), то IP-адрес нужного пользователя должен входить в заданный диапазон IP-адресов.
Source	Выберите адрес или группу адресов источника, к которым применяется данное правило. Если политика должна действовать для любого источника, выберите опцию **any**.
Destination	Выберите адрес или группу адресов назначения, к которым применяется данное правило. Если политика должна действовать для любого адреса назначения, выберите опцию **any**.
Service	Выберите службу или группу служб из выпадающего списка.
Access	Выберите из выпадающего списка опцию, указывающую на то, что должен делать межсетевой экран с пакетами, которые соответствуют данному правилу. Выберите опцию **deny**, чтобы межсетевой экран тихо отбрасывал пакеты без отправки пакета сброса TCP или сообщения ICMP «хост недоступен» (destination-unreachable) отправителю. Выберите опцию **reject**, чтобы межсетевой экран отбрасывал пакеты и посылал пакет сброса TCP отправителю. Все пакеты UDP отбрасываются без отправки ответного пакета. Выберите опцию **allow**, чтобы межсетевой экран разрешил прохождение пакетов.
Log	Укажите, должно ли устройство NXC генерировать сообщение в журнале (**log**), сообщение в журнале и оповещение (**log alert**) или не генерировать ничего (**no**) при поступлении пакета, соответствующего данному правилу.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

16.3 Экран Session Control

Выберите в меню **Configuration > Firewall > Session Control**, чтобы открыть экран **Firewall Session Control**. С помощью этого экрана можно ограничить количество одновременных сессий NAT/сессий на межсетевом экране, которые может использовать один клиент. Можно применить ограничение по умолчанию для всех пользователей и индивидуальные ограничения для конкретных пользователей, адресов или и пользователей, и адресов. Индивидуальное ограничение имеет приоритет над ограничением по умолчанию в случае применения обоих ограничений.

Рисунок 108 Экран Configuration > Firewall > Session Control



Поля экрана описаны в следующей таблице.

Таблица 95 Экран Configuration > Firewall > Session Control

ПОЛЕ	ОПИСАНИЕ
General Settings	
UDP Session Time Out	Укажите, сколько секунд (в диапазоне от 1 до 300) устройство NXC разрешает сессии UDP находиться в неактивном состоянии (то есть без трафика UDP) перед тем, как ее закрыть.
Session Limit Settings	
Enable Session limit	Установите этот переключатель, если необходимо контролировать количество одновременных сессий, которые могут установить хосты.
IPv4 Rule Summary	В этой таблице перечислены все правила ограничения количества одновременных сессий, которые могут иметь хосты.

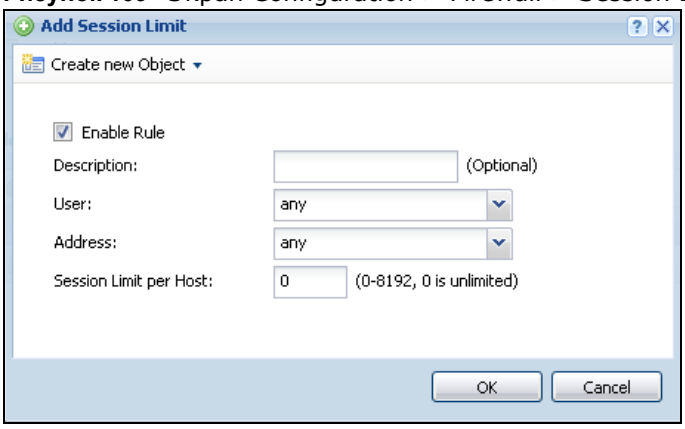
Таблица 95 Экран Configuration > Firewall > Session Control (продолжение)

ПОЛЕ	ОПИСАНИЕ
Default Session per Host	Это поле доступно для редактирования только в случае, если была включена опция ограничения количества сессий. С помощью этого поля можно задать общее ограничение на количество одновременных сессий NAT/сессий межсетевого экрана, которые могут быть установлены с одного компьютера. Если число клиентов, использующих одноранговые (peer to peer) приложения, невелико, можно задать в этом поле большее значение, чтобы улучшить производительность. Напротив, если многие клиенты активно пользуются одноранговыми приложениями, уменьшите значение в этом поле, чтобы ограничить количество доступных каждому отдельному клиенту сессий NAT. Создайте правила, описанные ниже, чтобы применить другие ограничения для конкретных пользователей или адресов.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Move	Чтобы изменить позицию правила в нумерованном списке, выберите это правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести это правило. Чтобы перенести правило на указанную позицию, введите нужное значение и нажмите клавишу [ENTER]. Порядок расположения правил имеет большое значение, поскольку правила применяются в порядке нумерации.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
#	Это порядковый номер правила ограничения количества сессий. Он не связан с конкретным правилом.
User	Это имя пользователя или группы пользователей, к которой применяется данное правило ограничения количества сессий.
IPv4 Address	Это адресный объект, к которому применяется данное правило ограничения количества сессий.
Description	Это описание правила.
Limit	В этом поле указывается максимальное число одновременных сессий, которое может быть установлено от имени данного пользователя или с данного адреса.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

16.3.1 Экран Add/Edit Session Limit

Выберите в меню **Configuration > Firewall > Session Limit**, а затем нажмите на пиктограмму **Add** или **Edit**, чтобы открыть экран **Firewall Session Limit Edit**. С помощью этого экрана можно настроить правила, которые описывают ограничения на количества сессий для определенных пользователей или адресов.

Рисунок 109 Экран Configuration > Firewall > Session Limit > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 96 Экран Configuration > Firewall > Session Limit > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Create new Object	С помощью этой кнопки можно создать любые новые объекты настроек, которые понадобятся на этом экране.
Enable Rule	Установите этот переключатель, чтобы включить это правило ограничения количества сессий.
Description	Введите информацию, которая поможет идентифицировать данное правило. В описании можно использовать печатные ASCII-символы, длина описания – не более 60 символов. В этом поле можно использовать пробелы.
User	Выберите имя пользователя или группы пользователей, к которым применяется данное правило. Активация этого правила межсетевого экрана происходит только тогда, когда указанный пользователь входит в систему. При выходе пользователя из системы правило действовать перестает. Если не требуется привязывать правило к определенному пользователю, выберите опцию **any**. Примечание: Если вместо опции **any** в поле ниже указан IP-адрес (или группа адресов), то IP-адрес нужного пользователя должен входить в заданный диапазон IP-адресов.
Address	Выберите адрес или группу адресов источника, к которым применяется данное правило. Если политика должна действовать для любого адреса источника, выберите опцию **any**.
Session Limit per Host	С помощью этого поля можно задать общее ограничение на количество одновременных сессий NAT/сессий межсетевого экрана, которые могут быть установлены от имени пользователей или с адресов, указанных в этом правиле. Для пользователей и адресов, указанных здесь, данный параметр имеет больший приоритет по сравнению с параметром **Default Session per Host** на общем экране **Firewall Session Limit**.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

17

Пользователи/группы

17.1 Обзор

В этой главе описан процесс создания учетных записей пользователей, групп пользователей и пользовательских настроек на устройстве NXC. Можно также создать правила, которые определяют, когда пользователи должны выполнить вход на устройство NXC, прежде чем NXC начнет направлять им трафик.

17.1.1 О чем рассказывается в этой главе

- Экран **User** (см. разд. 17.2 на стр. 211) служит для просмотра, создания и редактирования учетных записей пользователей.
- Экран **Group** (см. разд. 17.3 на стр. 215) содержит информацию обо всех группах пользователей. Кроме того, этот экран позволяет создавать, редактировать и удалять группы пользователей. Группы пользователей могут включать в себя обычных пользователей (access users) и другие группы пользователей. Добавлять администраторов в группы пользователей нельзя
- Экран **Setting** (см. разд. 17.4 на стр. 217) служит для управления настройками по умолчанию, настройками входа в систему, настройками блокировки и другими пользовательскими настройками устройства NXC. Кроме того, на этом экране можно указать, какие пользователи должны выполнить вход на устройство NXC, прежде чем оно будет направлять им трафик.
- Экран **MAC Address** (см. разд. 17.5 на стр. 227) содержит сведения обо всех привязках MAC-адресов к учетным записям пользователей MAC-адресов (MAC-ролям).

17.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Учетная запись пользователя

Учетная запись определяет права пользователя, выполнившего вход на устройство NXC. Учетные записи пользователей используют для управления доступам к настройкам и службам устройства NXC.

Типы пользователей

Это типы учетных записей пользователей, которые использует устройство NXC.

Таблица 97 Типы учетных записей пользователей

ТИП	ВОЗМОЖНОСТИ	МЕТОД(Ы) ВХОДА В СИСТЕМУ
Администраторы (Admin Users)		
admin	Изменение конфигурации устройства NXC (веб-интерфейс, интерфейс командной строки)	WWW, TELNET, SSH, FTP, консоль
limited-admin	Просмотр конфигурации устройства NXC (веб-интерфейс, интерфейс командной строки) Выполнение базовой диагностики (интерфейс командной строки)	WWW, TELNET, SSH, консоль
Обычные пользователи (Access Users)		
user	Доступ к службам сети Просмотр команд пользовательского режима (интерфейс командной строки)	Непокидаемый портал, TELNET, SSH
guest	Доступ к службам сети	Captive Portal
ext-user	Учетная запись внешнего пользователя	Captive Portal
ext-group-user	Учетная запись пользователя внешней группы	Captive Portal
guest-manager	Создание динамических гостевых учетных записей	WWW
динамическая гостевая	Доступ к службам сети	Captive Portal
mac-address	В зависимости от настроек функций, привязанных к имени пользователя.	Аутентификация по MAC-адресу

Примечание: Аутентификация учетной записи **admin** по умолчанию всегда происходит локально, независимо от настроек метода аутентификации.

Учетные записи типа Ext-User

Учетная запись типа **ext-user** создается в том случае, если аутентификация пользователя осуществляется с участием внешнего сервера, и необходимо создать для этого пользователя особые политики на устройстве NXC. Если не требуется создавать отдельные политики для данного пользователя, то необходимости создавать учетную запись типа **ext-user** нет.

Аутентификация всех пользователей типа **ext-user** должна осуществляться на внешнем сервере, таком, как сервер AD, LDAP или RADIUS. Если устройство NXC попробует аутентифицировать пользователя типа **ext-user** с помощью локальной базы данных, то аутентификацию выполнить не удастся.

Примечание: Если устройство NXC попробует аутентифицировать пользователя типа **ext-user** с использованием локальной базы данных, то аутентификацию выполнить не удастся.

После прохождения пользователем типа **ext-user** аутентификации устройство NXC попытается получить сведения о типе пользователя с внешнего сервера. При отсутствии такой

информации на внешнем сервере устройство NXC устанавливает для данной сессии тип пользователя **User**.

Учетные записи типа Ext-Group-User

Учетные записи типа **Ext-Group-User** похожи на учетные записи типа ext-user с той разницей, что они позволяют объединять пользователей в группы с помощью специального атрибута участия в группе, настраиваемого на сервере AD или LDAP.

Учетные записи типа Ext-Server

Учетные записи типа **Ext-Server** – это учетные записи администраторов, которые могут выполнять вход на устройство NXC из сети WAN. Их аутентификация осуществляется с помощью ассоциированного сервера RADIUS.

Динамические гостевые учетные записи

Динамические гостевые учетные записи – это гостевые учетные записи, которые создает в динамическом режиме владелец учетной записи администратора гостей. Они хранятся в локальной базе данной пользователей устройства NXC. Для динамической гостевой записи в динамическом режиме создаются имя пользователя и пароль. Пользователь, использующий динамическую гостевую запись, может работать со службами устройства NXC только в течение заданного временного интервала, по окончании которого динамическая учетная запись перестает быть активной. Изменить динамическую гостевую учетную запись невозможно.

Учетные записи типа mac-address

Для аутентификации беспроводных клиентов по MAC-адресу можно использовать внешний сервер. После аутентификации устройство NXC сопоставляет беспроводному клиенту учетную запись пользователя типа **mac-address** (роль MAC). Можно настроить функции, привязанные к имени пользователя, для управления доступом пользователей с учетными записями типа mac-address к службам сети.

Например, чтобы предоставить ноутбуку доступ к сетевому принтеру, проделайте следующее.

1. Настройте внешний сервер для аутентификации беспроводного клиента ноутбука по MAC-адресу.
2. Выберите в меню **Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile** и настройте параметры аутентификации по MAC-адресу профиля безопасности SSID таким образом, чтобы точка доступа использовала внешний сервер для аутентификации беспроводных клиентов по MAC-адресу (см. разд. 18.3.2.1 на стр. 242).
3. Выберите в меню **Configuration > Object > User/Group > User > Add** и создайте учетную запись пользователя типа mac-address (см. разд. 17.2.1 на стр. 213).
4. Выберите в меню **Configuration > Object > User/Group > MAC Address > Add** и привяжите MAC-адрес ноутбука к MAC-адресу учетной записи пользователя (именуемой также ролью MAC). См. разд. 17.5 на стр. 227.

Группы

Группы пользователей могут включать в себя учетные записи пользователей или другие группы пользователей. Группы пользователей уместно использовать в тех случаях, когда необходимо создать одно правило для нескольких пользовательских учетных записей вместо того, чтобы создавать отдельные правила для каждой учетной записи.

Примечание: Пользователей с правами «admin» невозможно добавить в одну группу с пользователями, имеющими права «access».

Примечание: Учетную запись по умолчанию **admin** невозможно включить в какую-либо группу пользователей.

Осведомленность о пользователе

По умолчанию пользователям не нужно выполнять вход на устройство NXC для того, чтобы пользоваться предоставляемыми им службами. Устройство NXC автоматически выполняет маршрутизацию пакетов для всех пользователей. Если необходимо ограничить круг служб, доступных определенным пользователям на устройстве NXC, можно потребовать для них обязательного входа на устройство NXC. Устройство NXC, соответственно, «знает» о пользователе, который выполнил вход в систему, поэтому можно создавать политики, привязанные к определенным пользователям и описывающие службы, доступные этим пользователям.

Приоритеты ролей пользователей

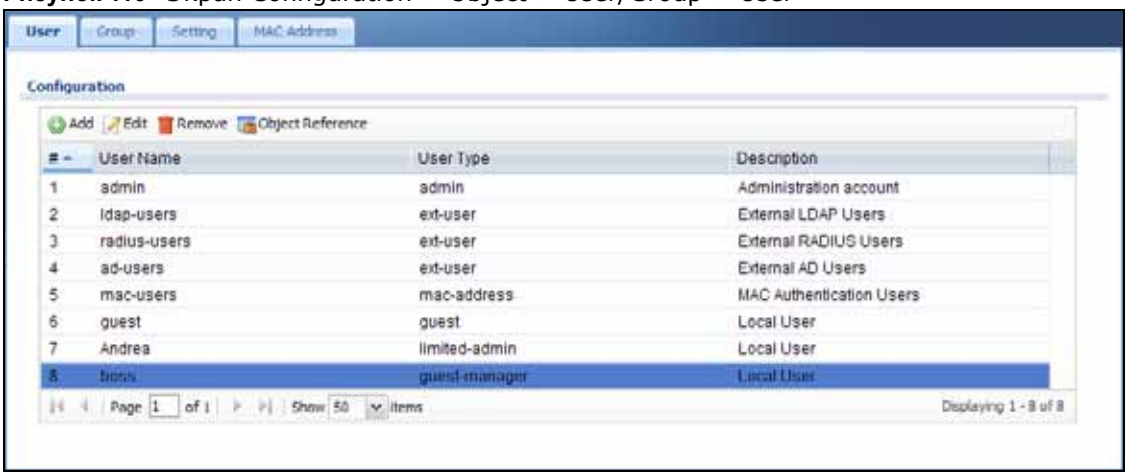
Устройство NXC проверяет следующие роли пользователей в порядке приоритета.

1. Роль пользователя для типа ext-user.
2. Роль пользователя для типа ext-group-user.
3. Роль пользователя для типов по умолчанию (ldap-users, ad-users, radius-users).

17.2 Сводный экран User

Экран **User** содержит сводную информацию обо всех учетных записях пользователей. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > User/Group**.

Рисунок 110 Экран Configuration > Object > User/Group > User



Поля экрана описаны в следующей таблице.

Таблица 98 Экран Configuration > Object > User/Group > User

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с каким-либо пользователем.
User Name	Это поле показывает имя каждого пользователя.
User Type	Это поле указывает на тип учетной записи каждого пользователя. Существует несколько типов учетных записей пользователей, которые поддерживает устройство NXC. • **admin** – этот пользователь может просматривать и менять конфигурацию устройства NXC • **limited-admin** – этот пользователь может просматривать конфигурацию устройства NXC, но не может менять ее • **user** – этот пользователь имеет доступ к службам NXC, но не может просматривать конфигурацию. • **guest** – этот пользователь имеет доступ к службам NXC, но не может просматривать конфигурацию. • **ext-user** – учетная запись пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **ext-group-user** – учетная запись пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **guest-manager** – этот пользователь может выполнить вход на устройство на экране Web-конфигуратора и создать динамические гостевые учетные записи с помощью всплывающего экрана **Master Manager**. • **mac-address** – внешний сервер осуществляет аутентификацию беспроводных клиентов по их MAC-адресам. После аутентификации устройство NXC сопоставляет беспроводному клиенту учетную запись пользователя типа mac-address (роль MAC). Функции, привязанные к имени пользователя, управляют доступом пользователя учетной записи типа mac-address к определенным ресурсам.
Description	Это поле содержит описание для каждого пользователя.

17.2.1 Экран Add/Edit User

С помощью экрана **User Add/Edit** можно создавать новые или редактировать существующие учетные записи пользователей.

17.2.1.1 Правила именования пользователей

Введите имя пользователя длиной от 1 до 31 символа.

Имя пользователя может содержать только:

- алфавитно-цифровые символы A-z 0-9 (unicode не поддерживается)
- _ [подчеркивания]
- - [дефисы]

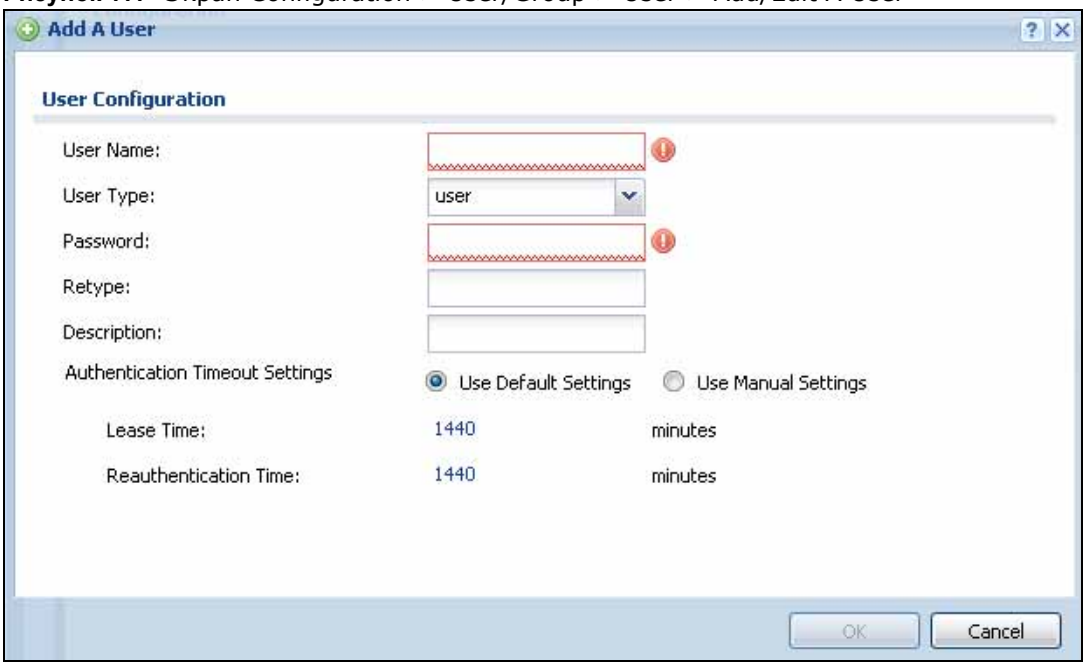
Имя должно начинаться с алфавитного символа (A-Z a-z), подчеркивания (_) или дефиса (-). Кроме того, для имен пользователей действуют следующие ограничения:

- Имена пользователей чувствительны к регистру. Если введено имя пользователя «bob», но при этом при подключении по протоколу CIFS или FTP используется строка «BOB», то система будет использовать настройки учетной записи для пользователя «BOB», а не пользователя ‘bob’.
- Имена пользователей не могут совпадать с именами групп пользователей.
- Следующие имена пользователей относятся к числу зарезервированных:

• adm	• admin	• any	• bin	• daemon
• debug	• devicehaecived	• ftp	• games	• halt
• ldap-users	• lp	• mail	• news	• nobody
• operator	• radius-users	• root	• завершение работы	• sshd
• sync	• uucp	• zyxel		

Чтобы перейти к этому экрану, перейдите на экран **User**, а затем нажмите кнопку **Add** или **Edit**.

Рисунок 111 Экран Configuration > User/Group > User > Add/Edit A User



Поля экрана описаны в следующей таблице.

Таблица 99 Экран Configuration > User/Group > User > Add/Edit A User

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя для этой учетной записи пользователя. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру. Имена пользователей не могут совпадать с именами групп пользователей, кроме того, некоторые слова нельзя использовать в качестве имен пользователей, поскольку они являются зарезервированными.
User Type	Выберите, к какому типу должен принадлежать этот пользователь. Возможные варианты: • **admin** – этот пользователь может просматривать и менять конфигурацию устройства NXC • **limited-admin** – этот пользователь может просматривать конфигурацию устройства NXC, но не может менять ее • **user** – этот пользователь имеет доступ к службам NXC, но не может просматривать его конфигурацию • **guest** – этот пользователь имеет доступ к службам NXC, но не может просматривать его конфигурацию • **ext-user** – учетная запись этого пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **ext-group-user** – учетная запись пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **guest-manager** – этот пользователь может выполнить вход на устройство на экране Web-конфигуратора и создать динамические гостевые учетные записи с помощью всплывающего экрана **Master Manager** • **mac-address** – внешний сервер осуществляет аутентификацию беспроводных клиентов по их MAC-адресам. После аутентификации устройство NXC сопоставляет беспроводному клиенту учетную запись пользователя типа mac-address (роль MAC). Функции, привязанные к имени пользователя, управляют доступом пользователя учетной записи типа mac-address к определенным ресурсам.
Password	Это поле недоступно для пользовательских типов **ext-user** и **ext-group-user**. Введите пароль для этой учетной записи пользователя. Пароль может состоять из алфавитно-цифровых символов, его длина составляет от 4 до 31 символа.

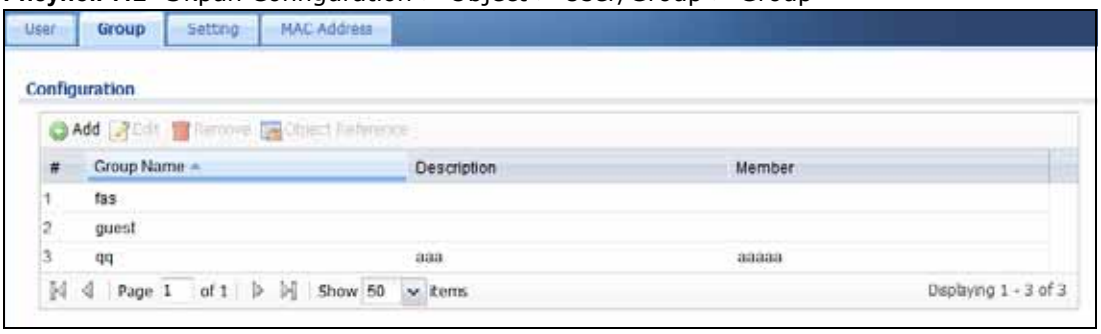
Таблица 99 Экран Configuration > User/Group > User > Add/Edit A User (продолжение)

ПОЛЕ	ОПИСАНИЕ
Retype	Это поле недоступно для пользовательских типов **ext-user** и **ext-group-user**.
Group Identifier	Это поле доступно только для пользовательского типа **ext-group-user**. Укажите значение атрибута участия в группе (**Group Membership Attribute**) сервера AD или LDAP, который идентифицирует принадлежность пользователя к определенной группе.
Associated AAA Server Object	Это поле доступно только для пользовательского типа **ext-group-user**. Выберите сервер AAA, на котором будет происходить аутентификация данной учетной записи.
Description	Введите описание для каждого пользователя (если требуется). В поле можно ввести до 60 печатных символов ASCII. Система предлагает шаблоны описаний по умолчанию.
Authentication Timeout Settings	Если необходимо изменить значение тайм-аута аутентификации, заданное по умолчанию, выберите опцию **Use Manual Settings**, а затем введите желаемые значения в полях ниже.
Lease Time	Укажите интервал в минутах, в течение которого пользователь должен обновить текущую сессию, чтобы она не прервалась. Длительность интервала может составлять от 1 до 1440 минут. 0 будет означать неограниченную продолжительность сессии. Сессия администраторов обновляется каждый раз при обновлении основного экрана Web-конфигуратора. Обычные пользователи могут обновить сессию, нажав кнопку **Renew** на экране. Если обычным пользователям разрешено обновлять сессию автоматически, то у них появляется возможность установить соответствующий переключатель на экране. В этом случае сессия будет автоматически обновляться до истечения срока аренды.
Reauthentication Time	Укажите интервал в минутах, на протяжении которого пользователь может быть подключен к устройству NXC в пределах одной сессии и по истечении которого пользователь должен снова выполнить вход на устройство. Длительность интервала может составлять от 1 до 1440 минут. 0 будет означать неограниченную продолжительность сессии. В отличие от параметра **Lease Time** у пользователя нет возможности обновить сессию, не выходя из нее.
Configuration Validation	Выберите учетную запись пользователя, входящего в группу, указанную выше, чтобы проверить корректность конфигурации. Введите имя пользователя в поле **User Name** и нажмите кнопку **Test**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

17.3 Сводный экран Group

Группы пользователей могут включать в себя обычных пользователей (access users) и другие группы пользователей. Добавлять администраторов в группы пользователей нельзя. Экран **Group** содержит сводную информацию обо всех группах пользователей. Кроме того, этот экран позволяет создавать, редактировать и удалять группы пользователей. Чтобы открыть этот экран, выполните вход на устройство через Web-конфигуратор и выберите в меню **Configuration > Object > User/Group > Group**.

Рисунок 112 Экран Configuration > Object > User/Group > Group



Поля экрана описаны в следующей таблице.

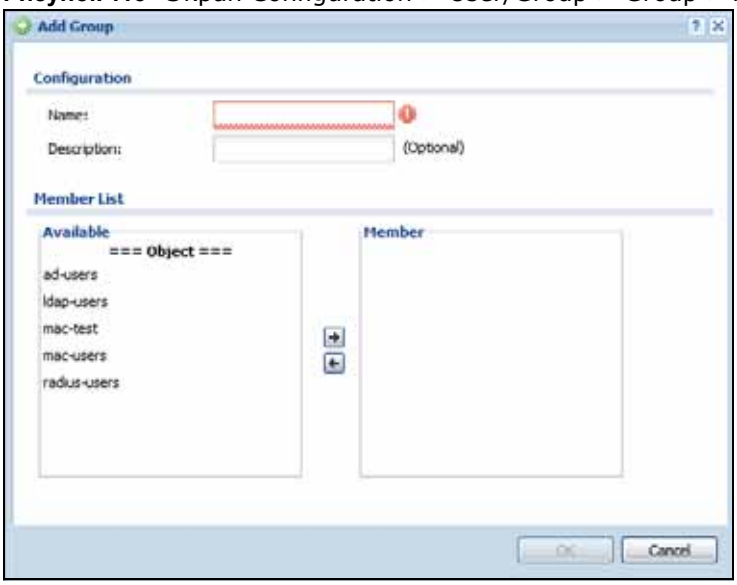
Таблица 100 Экран Configuration > Object > User/Group > Group

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Удаление группы не означает удаления учетных записей пользователей, входящих в нее.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с какой-либо пользовательской группой.
Group Name	Это поле показывает имя каждой пользовательской группы.
Description	Это поле содержит описание для каждой пользовательской группы.
Member	Это поле содержит список участников пользовательской группы. В качестве разделителя в списке используется запятая.

17.3.1 Экран Add/Edit Group

С помощью этого экрана можно создавать новые группы пользователей и редактировать существующие. Чтобы открыть этот экран, перейдите на экран **Group** и нажмите на пиктограмму **Add** или пиктограмму **Edit**.

Рисунок 113 Экран Configuration > User/Group > Group > Add/Edit Group



Поля экрана описаны в следующей таблице.

Таблица 101 Экран Configuration > User/Group > Group > Add/Edit Group

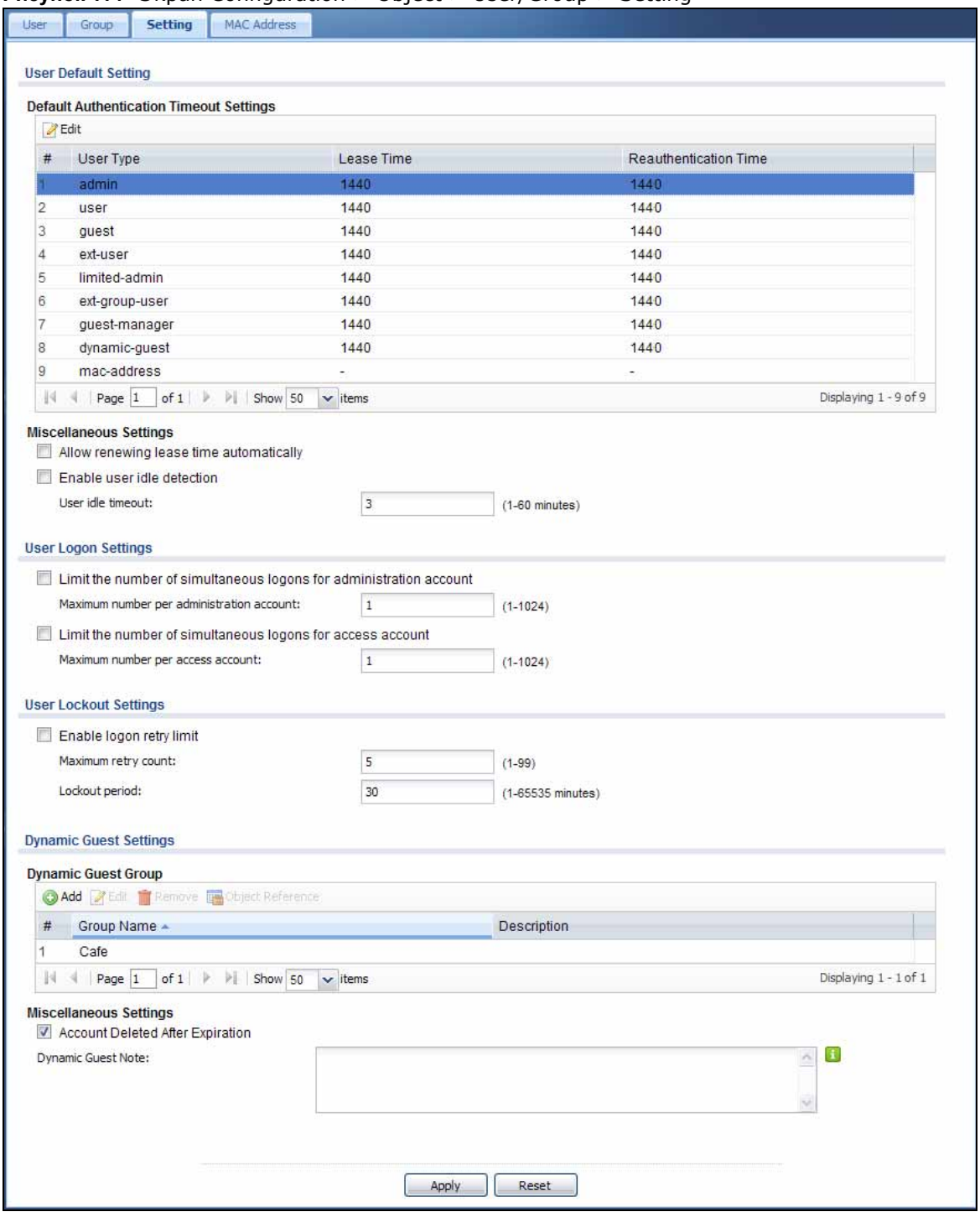
ПОЛЕ	ОПИСАНИЕ
Name	Введите имя для этой группы пользователей. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру. Имена групп пользователей не могут совпадать с именами пользователей.
Description	Введите описание группы пользователей (если требуется). Длина описания может составлять не более 60 символов, в описании можно использовать знаки пунктуации и пробелы.
Member List	Поле **Member** List содержит список имен пользователей и групп пользователей, которые были добавлены в данную группу пользователей. Порядок участников группы не имеет значения. Выберите в списке **Available** пользователей и группы, которые необходимо включить в данную группу, и переместите их в список **Member**. Можно дважды щелкнуть по одной записи, чтобы перенести ее, или воспользоваться клавишами [Shift] или [Ctrl], чтобы выбрать две и более записей и перенести их. Переместите пользователей, которых необходимо исключить из группы, в список **Available**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

17.4 Экран Setting

Этот экран служит для управления настройками по умолчанию, настройками входа в систему, настройками блокировок и другими пользовательскими настройками устройства NXC. Кроме того, на этом экране можно указать, какие пользователи должны выполнить вход на устройство NXC, прежде чем оно будет направлять им трафик.

Чтобы открыть этот экран, выполните вход на устройство через Web-конфигуратор и выберите в меню **Configuration > Object > User/Group > Setting**.

Рисунок 114 Экран Configuration > Object > User/Group > Setting



Поля экрана описаны в следующей таблице.

Таблица 102 Экран Configuration > Object > User/Group > Setting

ПОЛЕ	ОПИСАНИЕ
User Default Settings	
Default Authentication Timeout Settings	Эти параметры тайм-аута для аутентификации используются по умолчанию при создании учетной записи нового пользователя. Кроме того, они определяют настройки любых существующих учетных записей пользователей, если для них выбраны настройки по умолчанию. В любом случае остается возможность изменить настройки тайм-аута аутентификации любой учетной записи пользователя вручную.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
User Type	Существует несколько типов учетных записей пользователей, которые поддерживает устройство NXC. • **admin** – этот пользователь может просматривать и менять конфигурацию устройства NXC • **limited-admin** – этот пользователь может просматривать конфигурацию устройства NXC, но не может менять ее • **user** – этот пользователь имеет доступ к службам NXC, но не может просматривать конфигурацию. • **guest** – этот пользователь имеет доступ к службам NXC, но не может просматривать конфигурацию. • **ext-user** – учетная запись пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **ext-group-user** – учетная запись пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **guest-manager** – этот пользователь может выполнить вход на устройство на экране Web-конфигуратора и создать динамические гостевые учетные записи с помощью всплывающего экрана **Master Manager**. • **dynamic-guest** – этот пользователь имеет доступ к службам устройства NXC в течение определенного периода времени, но не может просматривать конфигурацию. • **mac-address** – внешний сервер осуществляет аутентификацию беспроводных клиентов по их MAC-адресам. После аутентификации устройство NXC сопоставляет беспроводному клиенту учетную запись пользователя типа mac-address (роль MAC). Функции, привязанные к имени пользователя, управляют доступом пользователя учетной записи типа mac-address к определенным ресурсам. Для учетных записей пользователей этого типа не нужно задавать время аренды и время повторной аутентификации.
Lease Time	Это время аренды по умолчанию в минутах для каждого типа учетных записей пользователей. Оно определяет интервал в минутах, в течение которого пользователь должен обновить текущую сессию, чтобы она не прервалась. Сессия администраторов обновляется каждый раз при обновлении основного экрана Web-конфигуратора. Обычные пользователи могут обновить сессию, нажав кнопку **Renew** на экране. Если обычным пользователям разрешено обновлять сессию автоматически, то у них появляется возможность установить соответствующий переключатель на экране. В этом случае сессия будет автоматически обновляться до истечения срока аренды.
Reauthentication Time	Это время повторной аутентификации по умолчанию в минутах для каждого типа учетных записей пользователей. Оно определяет интервал в минутах, на протяжении которого пользователь может быть подключен к устройству NXC в пределах одной сессии и по истечении которого пользователь должен снова выполнить вход на устройство. В отличие от параметра **Lease Time** у пользователя нет возможности обновить сессию, не выходя из нее.
Miscellaneous Settings	

Таблица 102 Экран Configuration > Object > User/Group > Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
Allow renewing lease time automatically	Установите этот переключатель, если необходимо предоставить обычным пользователям возможность обновлять время аренды не только вручную, но и автоматически, путем установки переключателя **Updating lease time automatically** на экране.
Enable user idle detection	Этот параметр применим к обычным пользователям. Установите этот переключатель, чтобы устройство NXC отслеживало период неактивности всех обычных пользователей на протяжении данной сессии (другими словами, время, в течение которого отсутствует трафик для этого обычного пользователя). Устройство NXC автоматически разрывает сессию обычного пользователя при достижении времени, указанного в параметре **User idle timeout**.
User idle timeout	Этот параметр применим к обычным пользователям. Это поле используется в случае выбора опции **Enable user idle detection**. Укажите интервал в минутах, на протяжении которого сессия каждого обычного пользователя может находиться в неактивном состоянии до того, как устройство NXC ее автоматически прервет.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Установите этот переключатель, если необходимо ограничить количество одновременных входов в систему для администраторов. Если этого не сделать, то администраторы смогут входить в систему столько раз, сколько захотят, в том числе одновременно, с одних и тех же или различающихся IP-адресов.
Maximum number per administration account	Это поле используется в случае выбора опции **Limit ... for administration account**. Укажите максимальное количество одновременных входов в систему для каждого администратора.
Limit the number of simultaneous logons for access account	Установите этот переключатель, если необходимо ограничить количество одновременных входов в систему для пользователей, не являющихся администраторами. Если этого не сделать, то обычные пользователи смогут входить в систему столько раз, сколько захотят, при условии, что они используют разные IP-адреса.
Maximum number per access account	Это поле используется в случае выбора опции **Limit ... for access account**. Укажите максимальное количество одновременных входов в систему для каждого обычного пользователя.
User Lockout Settings	
Enable logon retry limit	Установите этот переключатель, если необходимо ограничить количество неудачных попыток входа в систему для каждого пользователя (например, по причине неправильного ввода пароля). При достижении заданного числа неудачных попыток IP-адрес, с которого они исходят, будет заблокирован на указанный период времени.
Maximum retry count	Это поле используется в случае выбора опции **Enable logon retry limit**. Укажите, сколько неудачных попыток входа в систему может совершить каждый пользователь до момента, пока его IP-адрес не будет заблокирован на время, указанное в поле **lockout period**. Число выбирается в диапазоне от 1 до 99.
Lockout period	Это поле используется в случае выбора опции **Enable logon retry limit**. Укажите, сколько времени в минутах придется подождать пользователю, прежде чем он снова сможет попробовать совершить вход в систему, если выбрана опция **logon retry limit**, и достигнуто количество неуспешных попыток входа в систему, указанное в поле **maximum retry count**. Значение в этом поле должно лежать в диапазоне от 1 до 65535 (около 45,5 дней).
Dynamic Guest Settings	
Add	Нажатие на этот значок позволяет создать новую запись.

Таблица 102 Экран Configuration > Object > User/Group > Setting (продолжение)

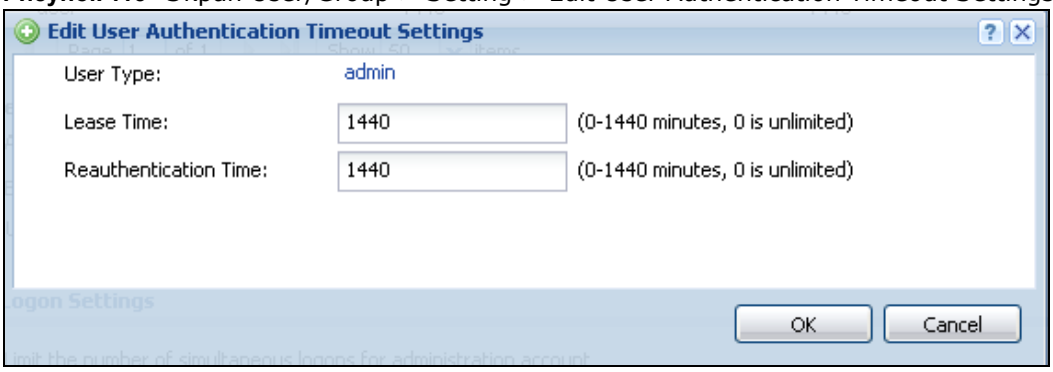
ПОЛЕ	ОПИСАНИЕ
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Удаление группы не означает удаления учетных записей пользователей, входящих в нее.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с какой-либо пользовательской группой.
Group Name	Это поле показывает имя каждой динамической гостевой группы.
Description	Это поле показывает описание каждой динамической гостевой группы.
Account Deleted After Expiration	Установите этот переключатель, если необходимо удалять динамические гостевые записи с экрана **Monitor > System Status > Dynamic Guest** по истечении срока их действия.
Dynamic Guest Note	Введите примечания (например, идентификатор SSID и ключ безопасности, которые динамические гостевые пользователи могут использовать для доступа к службам сети), которые будут напечатаны на бумажной памятке вместе с информацией об учетной записи. Эти памятки распечатывают и вручают динамическим гостевым пользователям. Примечание может содержать до 1024 ASCII-символов.
Apply	Нажмите **Apply**, чтобы сохранить эти настройки.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

17.4.1 Экран Edit User Authentication Timeout Settings

Этот экран позволяет указать настройки тайм-аута аутентификации по умолчанию для выбранного типа учетных записей пользователей. Эти параметры, кроме прочего, определяют настройки любых существующих учетных записей пользователей, если для них выбраны настройки по умолчанию. В любом случае остается возможность изменить настройки тайм-аута аутентификации любой учетной записи пользователя вручную.

Чтобы открыть этот экран, перейдите к экрану **Configuration > Object > User/Group > Setting** и нажмите на одну из пиктограмм **Edit** в разделе **Default Authentication Timeout Settings**.

Рисунок 115 Экран User/Group > Setting > Edit User Authentication Timeout Settings



Поля экрана описаны в следующей таблице.

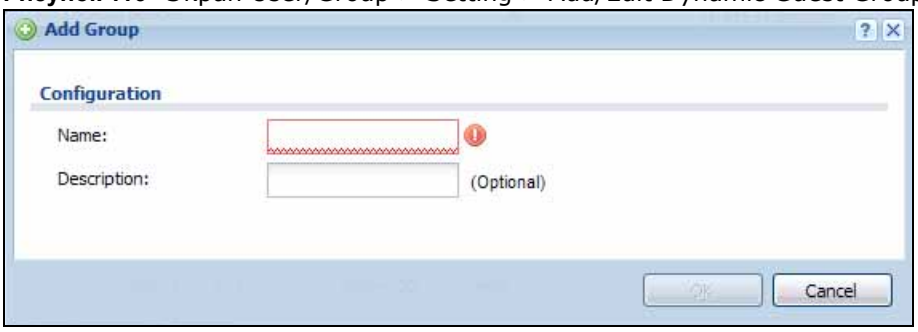
Таблица 103 Экран User/Group > Setting > Edit User Authentication Timeout Settings

ПОЛЕ	ОПИСАНИЕ
User Type	Это поле, доступное только для чтения, идентифицирует тип учетной записи пользователя, для которого устанавливаются параметры по умолчанию. • **admin** – этот пользователь может просматривать и менять конфигурацию устройства NXC • **limited-admin** – этот пользователь может просматривать конфигурацию устройства NXC, но не может менять ее • **user** – этот пользователь имеет доступ к службам NXC, но не может просматривать конфигурацию. • **guest** – этот пользователь имеет доступ к службам NXC, но не может просматривать конфигурацию. • **ext-user** – учетная запись этого пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **ext-group-user** – учетная запись пользователя хранится на удаленном сервере, например, на сервере RADIUS или LDAP. • **guest-manager** – этот пользователь может выполнить вход на устройство на экране Web-конфигуратора и создать динамические гостевые учетные записи с помощью всплывающего экрана **Master Manager**. • **dynamic-guest** – этот пользователь имеет доступ к службам устройства NXC в течение определенного периода времени, но не может просматривать конфигурацию.
Lease Time	Укажите интервал в минутах, в течение которого пользователь, работающий под учетной записью данного типа, должен обновить текущую сессию, чтобы она не прервалась. Длительность интервала может составлять от 1 до 1440 минут. 0 будет означать неограниченную продолжительность сессии. Сессия администраторов обновляется каждый раз при обновлении основного экрана Web-конфигуратора. Обычные пользователи могут обновить сессию, нажав кнопку **Renew** на экране. Если обычным пользователям разрешено обновлять сессию автоматически, то у них появляется возможность установить соответствующий переключатель на экране. В этом случае сессия будет автоматически обновляться до истечения срока аренды.
Reauthentication Time	Укажите интервал в минутах, на протяжении которого пользователь, работающий под учетной записью данного типа, может быть подключен к устройству NXC в пределах одной сессии и по истечении которого пользователь должен снова выполнить вход на устройство. Длительность интервала может составлять от 1 до 1440 минут. 0 будет означать неограниченную продолжительность сессии. В отличие от параметра **Lease Time** у пользователя нет возможности обновить сессию, не выходя из нее.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

17.4.2 Экран Add/Edit Dynamic Guest Group

С помощью этого экрана можно создавать новые динамические гостевые группы пользователей и редактировать существующие. Чтобы открыть этот экран, перейдите к экрану **Configuration > Object > User/Group > Setting** и нажмите на пиктограмму **Add** или на пиктограмму **Edit** в разделе **Dynamic Guest Group**.

Рисунок 116 Экран User/Group > Setting > Add/Edit Dynamic Guest Group



Поля экрана описаны в следующей таблице.

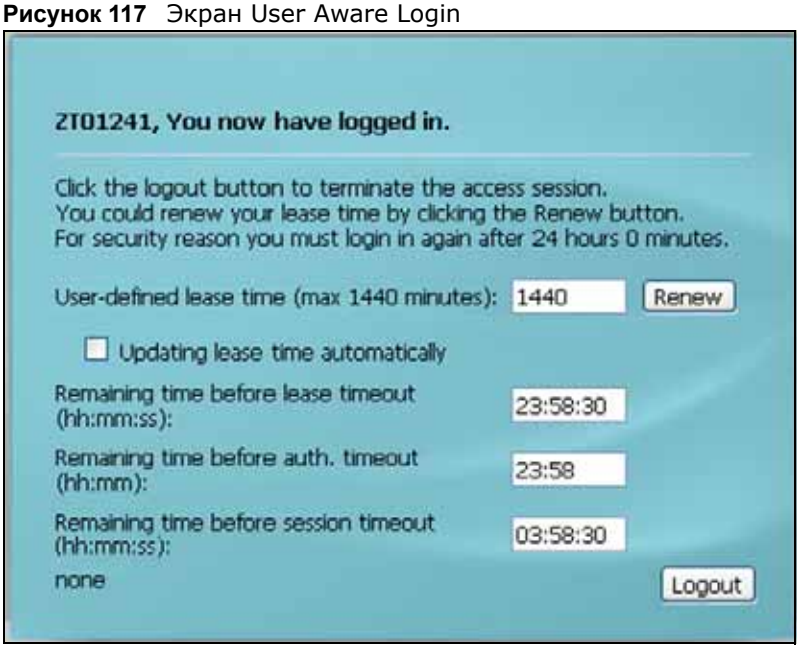
Таблица 104 Экран User/Group > Setting > Add/Edit Dynamic Guest Group

ПОЛЕ	ОПИСАНИЕ
Name	Укажите имя, которое будет идентифицировать динамическую гостевую группу.
Description	Введите описание динамической гостевой группы.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

17.4.3 Пример входа в систему с учетом информации о пользователе

Обычные пользователи не могут использовать Web-конфигуратор для просмотра конфигурации устройства NXC. Вместо этого после входа на устройство NXC обычные пользователи попадают на следующий экран с информацией о пользователе.

Рисунок 117 Экран User Aware Login



Поля экрана описаны в следующей таблице.

Таблица 105 Экран User Aware Login

ПОЛЕ	ОПИСАНИЕ
User-defined lease time (max ... minutes)	Обычные пользователи могут указать время аренды, которое меньше или равно интервалу времени, указанному вами. Значение по умолчанию соответствует времени аренды, указанному вами.
Renew	Обычные пользователи могут нажать на эту кнопку, чтобы сбросить время аренды, то есть количество времени, остающееся до того момента, пока устройство NXC автоматически прервет их сессию. Устройство NXC задает значение в этом поле в соответствии со следующими настройками • Значение поля **User-defined lease time** на текущем экране. • Значение поля **Lease time** на экране **User Add/Edit**. • Значение поля **Lease time** на экране **Setting > Edit**.
Updating lease time automatically	Этот переключатель появляется на экране при выборе опции **Allow renewing lease time automatically** на экране **Setting**. Обычные пользователи могут установить этот переключатель, если они хотят автоматически сбрасывать время аренды за 30 секунд до его истечения. В противном случае обычным пользователям придется нажимать кнопку **Renew** для сброса времени аренды.
Remaining time before lease timeout	Это поле отображает время аренды, оставшееся до прерывания сессии, при этом пользователь может иметь возможность его сбросить.
Remaining time before auth. timeout	Это поле показывает время, оставшееся до того момента, когда устройство NXC автоматически прервет сессию обычного пользователя, независимо от времени аренды.
Remaining time before session timeout	Это поле показывает, сколько времени пользователь может еще работать в рамках данной сессии до того, как устройство NXC автоматически прервет ее.

17.4.4 Пример входа в систему под именем администратора гостевых пользователей (Guest Manager)

Если необходимо создать гостевые учетные записи пользователей, введите учетные данные администратора гостевых пользователей (guest-manager) на экране входа в систему Web-конфигуратора. После успешного входа в систему откроется следующий экран Guest Manager.

Рисунок 118 Экран Guest Manager Login

Поля экрана описаны в следующей таблице.

Таблица 106 Экран Guest Manager Login

ПОЛЕ	ОПИСАНИЕ
Create account	Укажите количество (не более 32) динамических гостевых учетных записей, которые необходимо создать.
Guest Name	Это поле доступно только в случае, если необходимо создать одну учетную запись. Введите имя для гостевой учетной записи.
Phone	Это поле доступно только в случае, если необходимо создать одну учетную запись. Введите номер телефона для гостевой учетной записи.
E-mail	Это поле доступно только в случае, если необходимо создать одну учетную запись. Введите адрес электронной почты для гостевой учетной записи.
Company	Введите название компании (не более 64 символов) для гостевой учетной записи (или записей).
Address	Введите географический адрес (не более 64 символов) для гостевой учетной записи (или записей).
Other	Введите дополнительную информацию (не более 60 символов) для гостевой учетной записи (или записей).
Account Expiration Date	Выберите дату окончания срока действия данной записи (или записей).
Account Expiration Time	Выберите время окончания срока действия данной записи (или записей).
Dynamic Guest User Group	Выберите динамическую гостевую группу, с которой необходимо ассоциировать эту динамическую гостевую учетную запись (или записи).
Apply	Нажмите на эту пиктограмму, чтобы создать данную учетную запись (или записи).
Logout	Нажмите эту пиктограмму, чтобы выйти и вернуть на экран входа в систему Web-конфигуратор.

17.4.4.1 Guest Account List

После нажатия на кнопку **Apply** для создания динамических гостевых учетных записей откроется следующий экран со списком гостевых учетных записей.

Рисунок 119 Экран Guest Account List

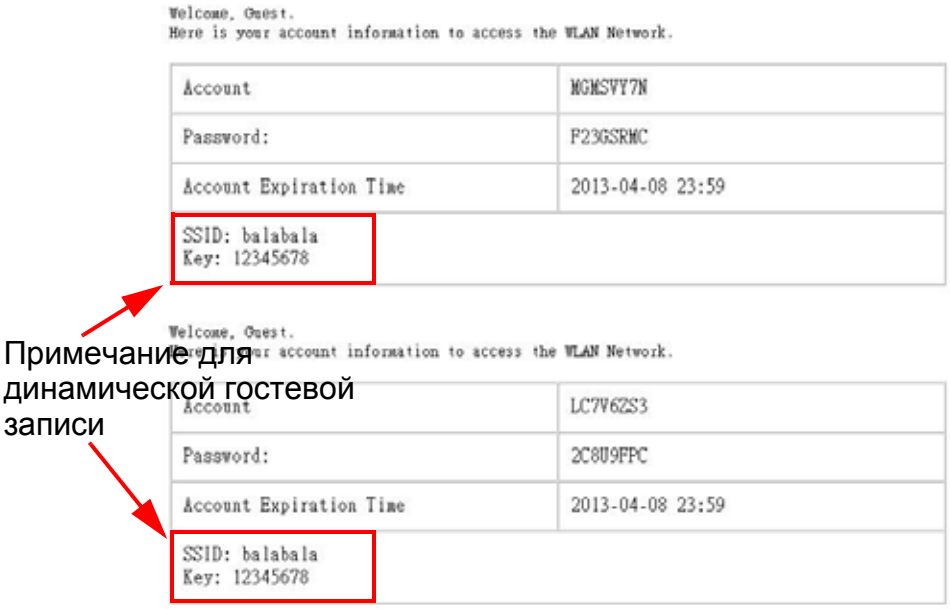
Поля экрана описаны в следующей таблице.

Таблица 107 Экран Guest Account List

ПОЛЕ	ОПИСАНИЕ
#	Это ранг учетной записи в списке.
Guest Name	Это имя-описание учетной записи.
User Name	Это имя пользователя для учетной записи.
Password	Это пароль для учетной записи.
Guest(s) Print	Нажмите на эту пиктограмму, чтобы распечатать сведения об учетной записи и примечания, которые были введены на экране **User/Group > Setting** для динамических гостевых пользователей.
Return	Нажмите на эту пиктограмму, чтобы вернуться на предыдущий экран.

На рисунке ниже изображен пример распечатанной памятки для динамической гостевой учетной записи.

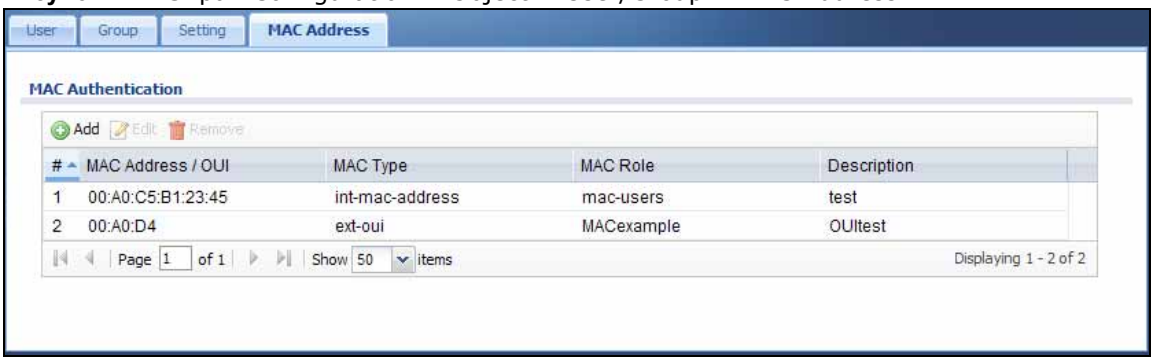
Рисунок 120 Внешний вид распечатанной памятки для динамической гостевой учетной записи



17.5 Экран MAC Address

Экран The **MAC Address** содержит информацию о привязке MAC-адресов беспроводных клиентов к ролям MAC (учетным записям пользователей типа mac-address). Более подробную информацию об учетных записях типа mac-address и ролях MAC можно найти в разделе «Учетные записи типа mac-address» на стр. 210. Выберите в меню **Configuration > Object > User/Group > MAC Address**, чтобы открыть этот экран.

Рисунок 121 Экран Configuration > Object > User/Group > MAC Address



Поля экрана описаны в следующей таблице.

Таблица 108 Экран Configuration > Object > User/Group > MAC Address

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.

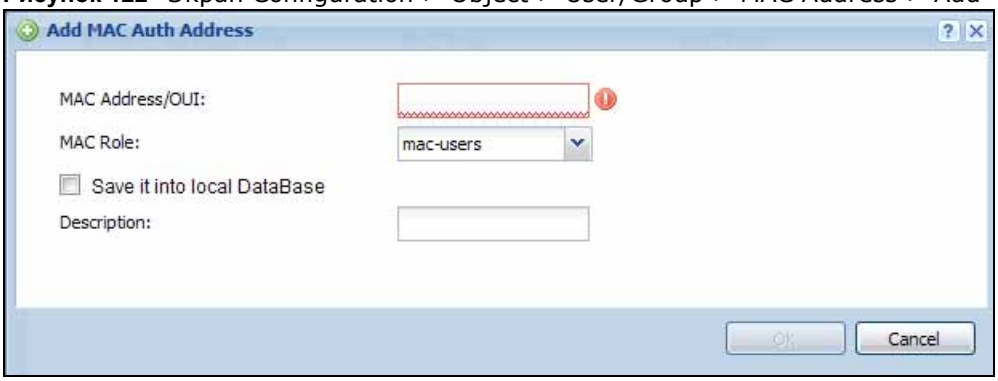
Таблица 108 Экран Configuration > Object > User/Group > MAC Address (продолжение)

ПОЛЕ	ОПИСАНИЕ
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
MAC Address/ OUI	MAC-адрес или идентификатор OUI (Organizationally Unique Identifier, уникальный идентификатор в пределах организации) беспроводного клиента. Идентификатор OUI содержит первые три октета MAC-адреса и уникальным образом идентифицирует производителя сетевого устройства.
MAC Type	Это поле говорит о том, какой тип идентификатора выбран для данной записи – MAC-адрес или OUI. **ext-mac-address** – это MAC-адрес, аутентификация которого осуществляется на внешнем сервере. **int-mac-address** – это MAC-адрес, аутентификация которого осуществляется с использованием локальной базы данных пользователей устройства NXC. **ext-oui** – это идентификатор OUI, аутентификация которого осуществляется на внешнем сервере. **int-oui** – это идентификатор OUI, аутентификация которого осуществляется с использованием локальной базы данных устройства NXC.
MAC Role	Учетная запись пользователя типа mac-address, к которой устройство NXC привязывает MAC-адрес или идентификатор OUI данной записи.
Description	Это поле содержит описание для каждой привязки.

17.5.1 Экран Add/Edit MAC Address

Используйте экран **MAC Address Add/Edit** для привязки MAC-адреса или идентификатора OUI беспроводного клиента к роли MAC (учетной записи типа mac-address).

Рисунок 122 Экран Configuration > Object > User/Group > MAC Address > Add



Поля экрана описаны в следующей таблице.

Таблица 109 Экран Configuration > Object > User/Group > MAC Address > Add/Edit

ПОЛЕ	ОПИСАНИЕ
MAC Address/ OUI	Укажите MAC-адрес или идентификатор OUI (Organizationally Unique Identifier, уникальный идентификатор в пределах организации) беспроводного клиента. Идентификатор OUI содержит первые три октета MAC-адреса и уникальным образом идентифицирует производителя сетевого устройства.
MAC Role	Выберите одну из созданных учетных записей типа mac-address, к которой необходимо привязать MAC-адрес или идентификатор OUI данной записи.

Таблица 109 Экран Configuration > Object > User/Group > MAC Address > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Save it into Local Database	Используйте эту опцию, если необходимо сохранить настройки привязки в локальной базе данных пользователей устройства NXCи выбрать вариант аутентификации MAC-адреса или идентификатора OUI с использованием локальной базы данных пользователей устройства NXC.
Description	Введите описание для данной привязки (если требуется).
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

18

Профили точек доступа

18.1 Обзор

В этой главе описан процесс настройки заранее созданных профилей для точек доступа (Access Points, AP), подключенных к беспроводной сети устройства NXC.

18.1.1 О чем рассказывается в этой главе

- Экран **Radio** (разд. 18.2 на стр. 231) позволяет создавать конфигурации радиомодуля, которые могут использовать точки доступа.
- Экран **SSID** (разд. 18.3 на стр. 237) позволяет настраивать три различных типа профилей для точек доступа, подключенных к сети.

18.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Беспроводные профили

Основным элементом конфигурации всех беспроводных точек доступа на устройстве NXC являются профили. Профиль представляет собой группу сохраненных настроек, которые можно использовать для любого числа подключенных точек доступа. Допускается создание беспроводных профилей следующих типов:

- **Radio** – Профиль этого типа описывает свойства радиопередатчика точки доступа. Всего на устройстве NXC может быть создано не более 32 профилей типа Radio.
- **SSID** – Профиль этого типа описывает свойства сигнала одной беспроводной сети, формируемого одной точкой доступа. Каждый радиопередатчик на одной точке доступа может осуществлять вещание в нескольких беспроводных сетях (не более 8). Всего на устройстве NXC может быть создано не более 32 профилей типа SSID.
- **Security** – Профиль этого типа описывает параметры безопасности, используемые одной беспроводной сетью. Он определяет метод шифрования, который должен использовать беспроводной клиент для ассоциации с этой беспроводной сетью. Всего на устройстве NXC может быть создано не более 32 профилей типа Security.
- **MAC Filtering** – Этот профиль обеспечивает дополнительный уровень безопасности для беспроводной сети благодаря возможности блокировать или разрешать доступ беспроводного клиента к данной беспроводной сети исходя из его MAC-адреса. Если MAC-адрес клиента присутствует в соответствующем списке, то ему либо разрешается, либо запрещается доступ к сети, в зависимости от настроек профиля типа MAC Filtering. Всего на устройстве NXC может быть создано не более 32 профилей типа MAC Filtering.

- **Layer-2 Isolation** – Этот профиль можно использовать для блокировки контактов между беспроводными клиентами, подключенными к беспроводной сети (или сетям) устройства NXC, в которой включена функция изоляции второго уровня, если только эти беспроводные клиенты не присутствуют в списке изоляции второго уровня.

SSID

SSID (Service Set IDentifier, идентификатор набора служб) – это имя, которое идентифицирует набор служб, с которым ассоциирована беспроводная станция. Беспроводные станции, которые хотят установить ассоциацию с определенной точкой доступа, должны иметь одинаковый идентификатор SSID. Иными словами, SSID – это название беспроводной сети, которое клиенты используют для подключения к ней.

WEP

Шифрование по методу WEP (Wired Equivalent Privacy) скремблирует все пакеты данных, которыми обменивается данная точка доступа и ассоциированные с ней беспроводные станции, с целью обеспечения конфиденциальности сетевых коммуникаций. И беспроводные станции, и точки доступа должны использовать одинаковый ключ WEP для шифрования и дешифрации данных.

WPA и WPA2

Wi-Fi Protected Access (WPA) – это подраздел стандарта IEEE 802.11i. WPA2 (IEEE 802.11i) – это стандарт безопасности для беспроводной связи, который описывает более строгие методы шифрования, аутентификации и управления ключами по сравнению с WPA. В первую очередь WPA(2) отличается от WEP более мощным методом шифрования данных и более строгими правилами аутентификации пользователей.

IEEE 802.1x

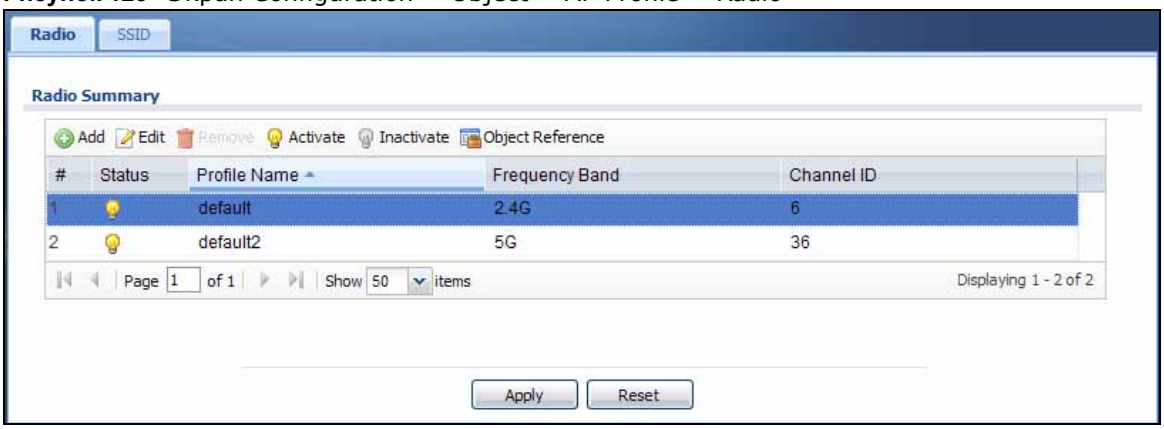
Стандарт IEEE 802.1x описывает расширенные методы обеспечения безопасности для аутентификации беспроводных станций и управления ключами шифрования. Аутентификация осуществляется с помощью внешнего сервера RADIUS.

18.2 Экран Radio

Этот экран позволяет создавать радиопрофили для точек доступа в сети. Радиопрофиль представляет собой список параметров, которые поддерживаемая управляемая точка доступа (например, NWA5121-N) может использовать для настройки любого из двух своих радиопередатчиков. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > AP Profile**.

Примечание: Всего на устройстве NXC может быть создано не более 32 профилей типа Radio.

Рисунок 123 Экран Configuration > Object > AP Profile > Radio



Поля экрана описаны в следующей таблице.

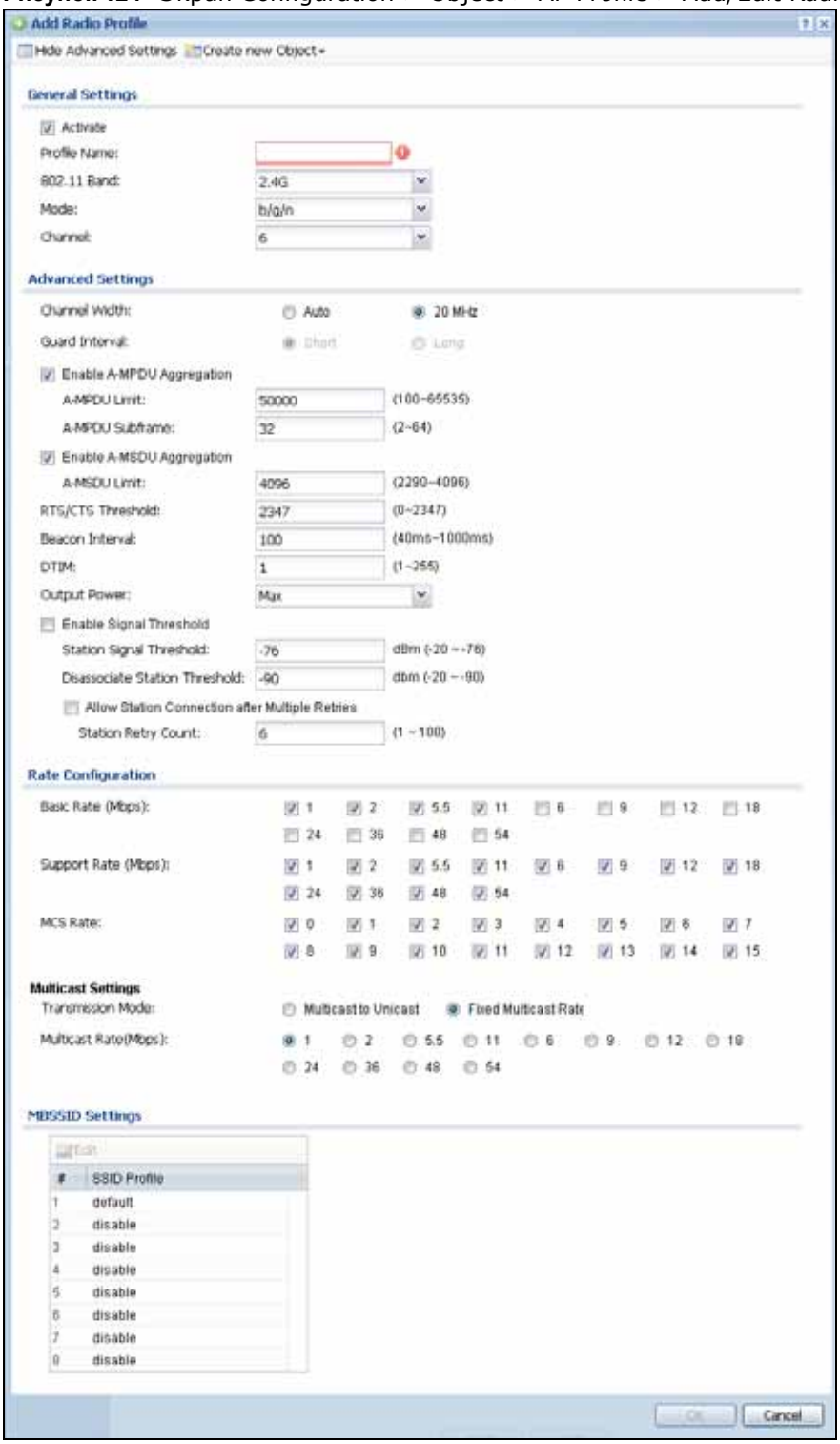
Таблица 110 Экран Configuration > Object > AP Profile > Radio

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новый радиопрофиль.
Edit	Нажмите эту кнопку, чтобы изменить свойства выбранного радиопрофиля.
Remove	Нажмите эту кнопку, чтобы удалить выбранный радиомодуль.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Object Reference	С помощью этой кнопки можно посмотреть, какие объекты ссылаются на выбранный радиопрофиль.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Profile Name	В этом поле отображается имя, которое присвоено данному радиопрофилю.
Frequency Band	Это поле показывает частотный диапазон, в котором работает данный радиопрофиль.
Channel ID	Это поле показывает широковещательный канал, который использует данный радиопрофиль.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

18.2.1 Экран Add/Edit Radio Profile

С помощью этого экрана можно создавать новые и редактировать существующие радиопрофили. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите радиопрофиль из списка и нажмите кнопку **Edit**.

Рисунок 124 Экран Configuration > Object > AP Profile > Add/Edit Radio Profile



Поля экрана описаны в следующей таблице.

Таблица 111 Экран Configuration > Object > AP Profile > Add/Edit Radio Profile

ПОЛЕ	ОПИСАНИЕ
Hide / Show Advanced Settings	С помощью этой кнопки можно скрыть или показать раздел **Advanced Settings** в этом окне.
Create New Object	Выберите нужный пункт из выпадающего списка, чтобы создать новый объект данного типа. Любые объекты, созданные таким образом, будут автоматически ссылаться на этот радиопрофиль.
General Settings	
Activate	Выберите эту опцию, чтобы сделать данный профиль активным.
Profile Name	Введите имя профиля, состоящее из алфавитно-цифровых символов, всего не более 31. Допускается использование символов пробела и подчеркивания.
802.11 Band	Выберите беспроводной диапазон, который должен использовать данный радиопрофиль. Беспроводные клиенты IEEE 802.11b/g/n используют частоту 2,4 ГГц. Беспроводные клиенты IEEE 802.11a/n используют частоту 5 ГГц.
Mode	Выберите метод подключения беспроводных клиентов к данной точке доступа. Для диапазона 2,4 ГГц выберите опцию **b/g**, чтобы обеспечить возможность подключения к данной точке доступа беспроводных устройств, совместимых со стандартами IEEE 802.11b и IEEE 802.11g. Для диапазона 2,4 ГГц выберите опцию **b/g/n**, чтобы обеспечить возможность подключения к данной точке доступа беспроводных устройств, совместимых со стандартами IEEE 802.11b, IEEE 802.11g и IEEE 802.11n. Для диапазона 5 ГГц выберите опцию **a**, чтобы обеспечить возможность подключения к данной точке доступа только беспроводных устройств, совместимых со стандартом IEEE 802.11a. Для диапазона 5 ГГц выберите опцию **a/n**, чтобы обеспечить возможность подключения к данной точке доступа беспроводных устройств, совместимых со стандартами IEEE 802.11a и IEEE 802.11n.
Channel	Выберите беспроводной канал, который должен использовать данный радиопрофиль. Рекомендуется выбирать канал, который в наименьшей степени используют другие точки радиодоступа в местности, где предполагается внедрить свой профиль. Это позволит уменьшить уровень помех между беспроводными клиентами и точкой доступа, которой назначен данный профиль. Некоторые беспроводные устройства, работающие в диапазоне 5 ГГц, имеют наклейку «**Только для использования внутри помещений**». Они предназначены исключительно для работы с точками доступа, размещенными внутри помещений. Не используйте их в сочетании с наружными точками доступа.
Advanced Settings	
Channel Width	Выберите пропускную способность канала для беспроводной сети. Выберите опцию **Auto**, чтобы устройство NXC автоматически выбирало пропускную способность канала – 40 МГц или 20 МГц – в зависимости от условий в сети. Выберите опцию **20 MHz**, если необходимо уменьшить уровень радиопомех с другими беспроводными устройствами, работающими неподалеку

Таблица 111 Экран Configuration > Object > AP Profile > Add/Edit Radio Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Guard Interval	Укажите, каким должен быть охранный интервал для данного радиопрофиля – коротким или длинным. Охранный интервал – это интервал между передачей данных, осуществляемой разными пользователями, который служит для снижения помех. Сокращение интервала приводит к увеличению скорости передачи данных, но способствует и повышению уровня помех. Увеличение интервала уменьшает скорость передачи данных, но в то же время снижает и уровень помех.
Enable A-MPDU Aggregation	Выберите эту опцию, чтобы включить функцию агрегации A-MPDU. Агрегация MPDU (Message Protocol Data Unit, блок данных протокола сообщения) обеспечивает сбор кадров Ethernet вместе с их заголовками 802.11n и их обертывание в MAC-заголовок 802.11n. Этот метод бывает полезен для увеличения пропускной способности в условиях, способствующих высокому уровню ошибок.
A-MPDU Limit	Укажите максимальный размер кадра для агрегации.
A-MPDU Subframe	Укажите максимальное количество кадров для однократной агрегации.
Enable A-MSDU Aggregation	Выберите эту опцию, чтобы включить функцию агрегации A-MSDU. Агрегация MSDU (Mac Service Data Unit) обеспечивает сбор кадров Ethernet без заголовков 802.11n и оборачивание полученных полезных данных без заголовков в один MAC-заголовок 802.11n. Этот метод полезен для увеличения пропускной способности. Он более эффективен, чем метод A-MPDU, за исключением условий, способствующих высокому уровню ошибок.
A-MSDU Limit	Укажите максимальный размер кадра для агрегации.
RTS/CTS Threshold	Функцию RTS/CTS используют для снижения уровня коллизий в беспроводной сети, если беспроводные клиенты подключены к одной точке доступа, но при этом находятся вне диапазона по отношению друг к другу. Если эта опция включена, беспроводной клиент отправляет запрос RTS (Request To Send, готовность к передаче) и не начинает передачу до тех пор, пока не получит ответ CTS (Clear To Send, готовность к приему). Это позволяет исключить ситуацию, когда беспроводные клиенты передают пакеты одновременно и вызывают таким образом коллизии. Беспроводной клиент будет посылать запрос RTS для всех пакетов, чей размер превышает количество байт, указанных в этом поле. Установите значение RTS/CTS равным или выше порога фрагментации, чтобы отключить функцию RTS/CTS.
Beacon Interval	При отправке сообщения типа beacon («маяк») устройство, подключенное к беспроводной сети, включает в это сообщение интервал отправки beacon. Этот интервал указывает период времени, через который данное устройство вновь отправит сообщение типа beacon. Этот интервал уведомляет принимающие устройства в сети, сколько времени они могут находиться в режиме ожидания с низким энергопотреблением, прежде чем снова перейти в активный режим для обработки следующего сообщения типа beacon. Большое значение интервала beacon позволяет снизить энергопотребление точки доступа.
DTIM	Сообщение DTIM (Delivery Traffic Indication Message, сообщение индикации доставки трафика) – это период времени, по истечении которого широковещательные и многоадресные пакеты передаются мобильным клиентам в режиме активного управления мощностью (Active Power Management). Если указать в поле DTIM слишком большое значение, это может привести к потере клиентами связи с сетью. Значение выбирается в диапазоне от 1 до 255.

Таблица 111 Экран Configuration > Object > AP Profile > Add/Edit Radio Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Output Power	В этом поле задается выходная мощность точки доступа. Если в обслуживаемой зоне наблюдается высокая концентрация точек доступа, уменьшите выходную мощность управляемой точки доступа, чтобы избежать взаимных помех с другими точками доступа. Выберите одно из следующих значений: **Max**, **-3db (50%)**, **-6db (25%)**, **-9dB (12.5%)** или **Min**. Более подробную информацию о настройках выходной мощности устройства NXC можно найти в спецификации к продукту. Примечание: Уменьшение выходной мощности приводит к сокращению эффективного радиуса вещания устройства NXC.
Enable Signal Threshold	Установите этот переключатель, если необходимо установить пороговое значение сигнала для обеспечения высокой пропускной способности беспроводных клиентов. Эта опция позволяет разрешить подключение к данной точке доступа только беспроводных клиентов с высоким уровнем сигнала. Снимите выделение с этого переключателя, чтобы не устанавливать ограничение на минимальную силу сигнала для беспроводных клиентов, которые хотят подключиться к данной точке доступа.
Station Signal Threshold	Укажите минимальную силу сигнала для клиента. Беспроводной клиент сможет подключиться к данной точке доступа только в том случае, если его сила сигнала превосходит значение, указанное в этом поле. -20 dBm – это максимальное, а -76 – минимальное пороговое значение, которое можно указать.
Disassociate Station Threshold	Укажите минимальную силу сигнала, при которой происходит разрыв соединения. Если сила сигнала беспроводного клиента падает ниже указанного порогового значения, устройство NXC отключает беспроводной клиент от данной точки доступа. -20 dBm – это максимальное, а -90 – минимальное пороговое значение, которое можно указать.
Allow Station Connection after Multiple Retries	Выберите эту опцию, если необходимо разрешить беспроводным клиентам попытки повторного подключения к данной точке доступа после их отключения из-за малой силы сигнала.
Station Retry Count	Укажите максимальное число попыток повторного подключения к данной точке доступа, которые может совершить беспроводной клиент
Rate Configuration	Этот раздел описывает скорости передачи данных, которые разрешены для клиентов. Для каждого типа скорости (**Rate**) выберите нужную опцию из списка. Типы скоростей: • **Basic Rate (Mbps)** – Укажите базовую скорость в Мбит/с. • **Support Rate (Mbps)** – Укажите дополнительную скорость в Мбит/с. • **MCS Rate** – Укажите параметры для скорости MCS. Стандарт IEEE 802.11n поддерживает много различных скоростей передачи данных, которые называются скоростями MCS. Аббревиатура MCS расшифровывается как «Modulation and Coding Scheme» («схема модуляции и кодирования»). Это функция 802.11n, которая улучшает производительность беспроводной сети в части пропускной способности.
Multicast Settings	Этот раздел определяет режим передачи и максимальную скорость для многоадресного трафика.

Таблица 111 Экран Configuration > Object > AP Profile > Add/Edit Radio Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Transmission Mode	Укажите, каким образом точка доступа должна обрабатывать многоадресный трафик. Выберите опцию **Multicast to Unicast**, если необходимо передавать беспроводной многоадресный трафик всем беспроводным клиентам как одноадресный трафик. Одноадресный трафик в динамическом режиме меняет скорость передачи данных исходя из требований конкретного приложения к пропускной способности. Механизм повторной передачи одноадресного трафика обеспечивает более надежную передачу многоадресного трафика, хотя он и способствует появлению дублированных пакетов. Выберите опцию **Fixed Multicast Rate**, если необходимо передавать беспроводной многоадресный трафик с одинаковой скоростью. В этом случае должны быть известны требования приложения многоадресной рассылки к пропускной способности, которые необходимо будет указать в следующем поле.
Multicast Rate (Mbps)	Если был выбран режим фиксированной скорости для передачи многоадресного трафика, укажите значение скорости в этом поле. Например, чтобы обеспечить передачу видеотрафика со скоростью 4 Мбит/с, выберите для фиксированной скорости многоадресного трафика значение более 4 Мбит/с.
MBSSID Settings	Этот раздел позволяет ассоциировать профиль SSID с радиопрофилем.
Edit	Выберите профиль SSID и нажмите эту кнопку, чтобы переназначить его. Выбранный профиль SSID становится редактируемым при щелчке мышью.
SSID Profile	Выберите профиль SSID, который нужно ассоциировать с этим радиопрофилем.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

18.3 Экран SSID

Экраны SSID позволяют настроить профили трех различных типов для точек доступа, подключенных к сети: список SSID, который позволяет назначить определенные конфигурации SSID точкам доступа; список безопасности, который позволяет ассоциировать определенные методы шифрования с точками доступа при принятии решения о том, разрешать ли беспроводным клиентам подключение к ним; и список MAC-фильтров, который позволяет ограничивать подключение беспроводных клиентов к точке доступа по MAC-адресам.

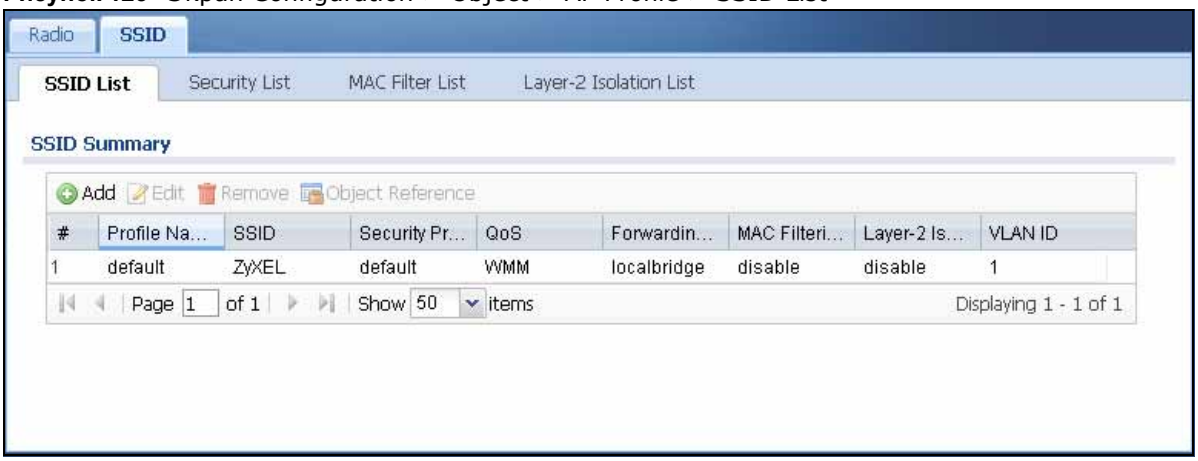
18.3.1 Экран SSID List

Этот экран позволяет создавать конфигурации SSID, которые могут быть использованы точками доступа, и управлять такими конфигурациями. SSID, или Service Set IDentifier (идентификатор набора служб), по сути представляет собой имя беспроводной сети, к которой могут подключаться беспроводные клиенты. Для любого устройства, способного сканировать радиочастоты (такого, как адаптер Wi-Fi на ноутбуке), SSID предстает в виде читаемого текста и отображается как имя беспроводной сети при подключении.

Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > AP Profile > SSID**.

Примечание: Всего на устройстве NXC может быть создано не более 32 профилей SSID.

Рисунок 125 Экран Configuration > Object > AP Profile > SSID List



Поля экрана описаны в следующей таблице.

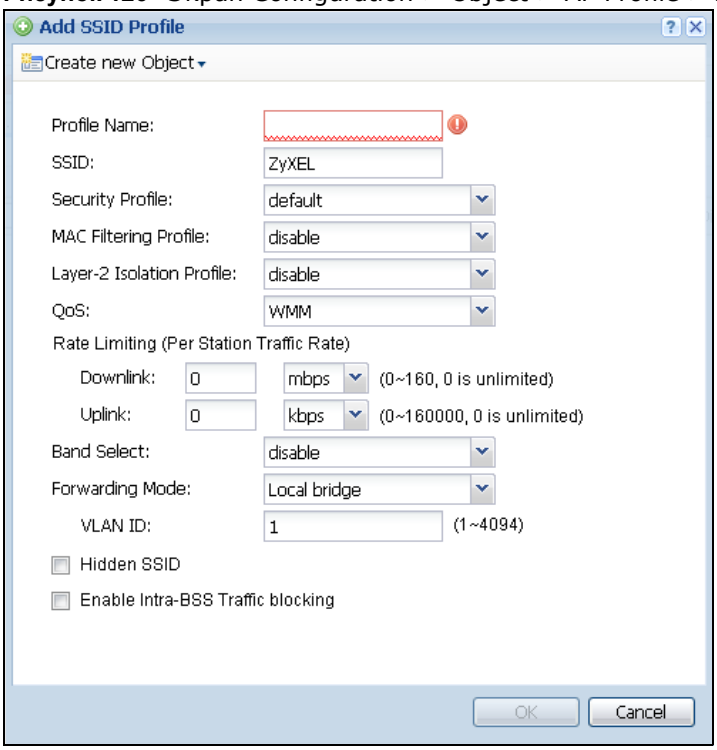
Таблица 112 Экран Configuration > Object > AP Profile > SSID List

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новый профиль SSID.
Edit	Нажмите эту кнопку, чтобы изменить свойства выбранного профиля SSID.
Remove	Нажмите эту кнопку, чтобы удалить выбранный профиль SSID.
Object Reference	С помощью этой кнопки можно посмотреть, какие объекты ссылаются на выбранный профиль SSID (например, радиопрофиль).
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю SSID.
SSID	Это поле отображает имя SSID в том виде, в котором оно предстает для беспроводных клиентов.
Security Profile	Это поле указывает на профиль безопасности (если таковой есть), который ассоциирован с данным профилем SSID.
QoS	Это поле указывает на тип управления качеством обслуживания (QoS), ассоциированный с данным профилем SSID.
Forwarding Mode	Это поле показывает режим пересылки (локальный мост **Local Bridge** или туннель **Tunnel**), ассоциированный с данным профилем SSID.
MAC Filtering Profile	Это поле показывает, какой профиль фильтрации MAC (если таковой есть) ассоциирован с данным профилем SSID.
Layer-2 Isolation Profile	Это поле показывает, какой профиль изоляции второго уровня (если таковой есть) ассоциирован с данным профилем SSID.
VLAN ID	Это поле показывает, какой идентификатор виртуальной локальной сети (VLAN ID) ассоциирован с данным профилем SSID.

18.3.1.1 Экран Add/Edit SSID Profile

С помощью этого экрана можно создавать новые и редактировать существующие профили SSID. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите профиль SSID из списка и нажмите кнопку **Edit**.

Рисунок 126 Экран Configuration > Object > AP Profile > Add/Edit SSID Profile



Поля экрана описаны в следующей таблице.

Таблица 113 Экран Configuration > Object > AP Profile > Add/Edit SSID Profile

ПОЛЕ	ОПИСАНИЕ
Create new Object	Выберите тип объекта из списка, чтобы создать новый объект, ассоциированный с данным профилем SSID.
Profile Name	Введите имя профиля, состоящее из алфавитно-цифровых символов (не более 31). Это имя видно только в Web-конфигураторе и только для целей управления. Допускается использование символов пробела и подчеркивания.
SSID	Укажите имя SSID для данного профиля. Это имя будут видеть беспроводные клиенты в сети. Введите имя длиной не более 32 символов, в имени также можно использовать пробелы и подчеркивания.
Security Profile	Выберите из списка профиль безопасности, который необходимо ассоциировать с данным профилем SSID. Если профиля безопасности еще нет, создайте его с помощью меню **Create new Object**. Примечание: Настоятельно рекомендуется создать профили безопасности для всех профилей SSID для повышения уровня безопасности сети.
MAC Filtering Profile	Выберите из списка профиль фильтрации MAC, который необходимо ассоциировать с данным профилем SSID. Если профиля фильтрации MAC еще нет, можно создать его с помощью меню **Create new Object**. Фильтрация MAC позволяет ограничить возможность подключения беспроводных клиентов к сети через сеть с определенным SSID по MAC-адресам. Запрещается подключение любых клиентов, MAC-адреса которых отсутствуют в списке разрешенных адресов профиля фильтрации MAC. Если эту опцию отключить, то фильтрация MAC использоваться не будет.

Таблица 113 Экран Configuration > Object > AP Profile > Add/Edit SSID Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Layer-2 Isolation Profile	Выберите из списка профиль изоляции второго уровня, который необходимо ассоциировать с данным профилем SSID. Если профиля фильтрации MAC еще нет, можно создать его с помощью меню **Create new Object**. Если эту опцию отключить, то изоляция второго уровня использоваться не будет.
QoS	Выберите категорию доступа к управлению качеством обслуживания (QoS), которую необходимо ассоциировать с данным профилем SSID. Категории доступа уменьшают задержку при передаче пакетов данных по беспроводной сети. Определенные категории, такие, как голос и данные, имеют более высокий приоритет, поскольку эти приложения обладают высокой чувствительностью к задержке. Существуют следующие категории доступа к управлению качеством обслуживания (QoS): **disable**: Управление качеством обслуживания для данного профиля SSID не осуществляется. Все пакеты данных обрабатываются с одинаковым приоритетом и не помечаются тегами категорий доступа. **WMM**: Включает автоматическое добавление тегов к пакетам данных. Устройство NXC назначает категории доступа для данной сети SSID на основе анализа данных, передаваемых через устройство, и прилагает максимальные усилия для их скорейшей передачи. Если какие-то пакеты напоминают, к примеру, видеотрафик, то к ним добавляются следующие теги. **WMM_VOICE**: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как голосовые данные. Эту категорию рекомендуется использовать в случае, если сеть с идентификатором SSID служит для совершения и приема голосовых VoIP-вызовов. **WMM_VIDEO**: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как данные видео. Эту категорию рекомендуется использовать в случае, если сеть с идентификатором SSID служит для организации видеоконференций. **WMM_BEST_EFFORT**: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как «best effort» («без гарантий»); это означает, что данные пойдут по наиболее оптимальному маршруту, но так, чтобы не препятствовать трафику с более высоким приоритетом. Эта категория доступа хорошо подходит для тех случаев, когда необходимости в обеспечении наивысшей пропускной способности нет, например, при серфинге в сети Интернет. **WMM_BACKGROUND**: Весь беспроводной трафик, направляемый в сеть с идентификатором SSID, помечается тегами как низкоприоритетный или «background traffic» («фоновый трафик»); это означает, что все трафик всех остальных категорий имеет приоритет над трафиком этой категории. Если трафик из сети с данным идентификатором SSID не предъявляет жестких требований к пропускной способности, то рекомендуется использовать эту категорию доступа. Например, это может быть сеть, к которой подключены исключительно сетевые принтеры.
Rate Limiting	
Downlink	Укажите максимальную скорость передачи входящего трафика (в Мбит/с или в Кбит/с) для каждой станции.
Uplink	Укажите максимальную скорость передачи исходящего трафика (в Мбит/с или в Кбит/с) для каждой станции.

Таблица 113 Экран Configuration > Object > AP Profile > Add/Edit SSID Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Band Select	Можно включить эту функцию, позволяющую использовать в первую очередь диапазон 5 ГГц, для повышения производительности сети и уменьшения помех в частотном диапазоне 2,4 ГГц. Для радиопрофилей 2,4 ГГц и 5 ГГц необходимо задать одинаковые параметры SSID и безопасности. Выберите опцию **standard**, чтобы точка доступа совершала попытки подключить беспроводных клиентов к сети с тем же SSID, используя диапазон 5 ГГц. Подключения к сети с тем же SSID в диапазоне 2,4 ГГц тем не менее все равно разрешены. Выберите опцию **force**, чтобы беспроводные клиенты всегда подключались к сети с определенным SSID, используя диапазон 5 ГГц. Подключения к сети с определенным SSID в диапазоне 2,4 ГГц в этом случае не разрешены. Рекомендуется выбирать эту опцию, если данная точка доступа и беспроводные клиенты могут работать в обоих частотных диапазонах. В противном случае выберите опцию **disable**, чтобы отключить эту функцию.
Forwarding Mode	Выберите режим пересылки трафика из сети с данным SSID.
VLAN ID	При выборе режима пересылки **Local Bridge** укажите идентификатор сети VLAN, которая будет добавлять теги в любой трафик, идущий от сети с данным SSID, если эта сеть VLAN отличается от «родной» сети VLAN.
VLAN Interface	При выборе режима пересылки **Tunnel** укажите интерфейс VLAN.
Hidden SSID	Выберите эту опцию, если необходимо «скрыть» имя SSID от беспроводных клиентов. В этом случае все беспроводные клиенты, находящиеся поблизости от точки доступа, использующей этот профиль SSID, получают команду не показывать имя SSID данной сети как потенциальную сеть для подключения. Не все беспроводные клиенты выполняют эту команды, некоторые все равно показывают этот SSID. Если SSID «скрыт», и беспроводные клиенты его не видят, то единственный способ подключиться к сети с этим SSID – это вручную указать данное имя SSID на экране настроек беспроводного подключения (он может выглядеть по-разному в зависимости от типа клиента, программного обеспечения, используемого для подключения к сети и операционной системы).
Enable Intra-BSS Traffic Blocking	Выберите эту опцию, если необходимо запретить перекрестный трафик из сети с тем же SSID. Примечание: Если ассоциировать профиль изоляции второго уровня с профилем SSID, эта опция будет выбрана автоматически и станет нередактируемой.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

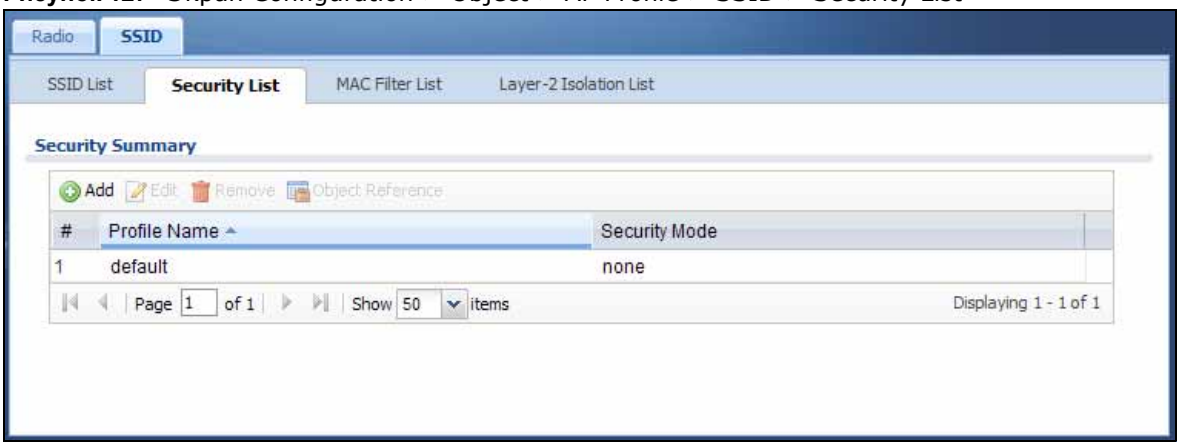
18.3.2 Экран Security List

Этот экран позволяет управлять конфигурациями безопасности, которые можно использовать в беспроводных сетях. Схема безопасности в беспроводной сети реализуется строго между точкой доступа, формирующей сеть с данным SSID, и подключенными к ней станциями.

Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > AP Profile > SSID > Security List**.

Примечание: Всего на устройстве NXC может быть создано не более 32 профилей безопасности.

Рисунок 127 Экран Configuration > Object > AP Profile > SSID > Security List



Поля экрана описаны в следующей таблице.

Таблица 114 Экран Configuration > Object > AP Profile > SSID > Security List

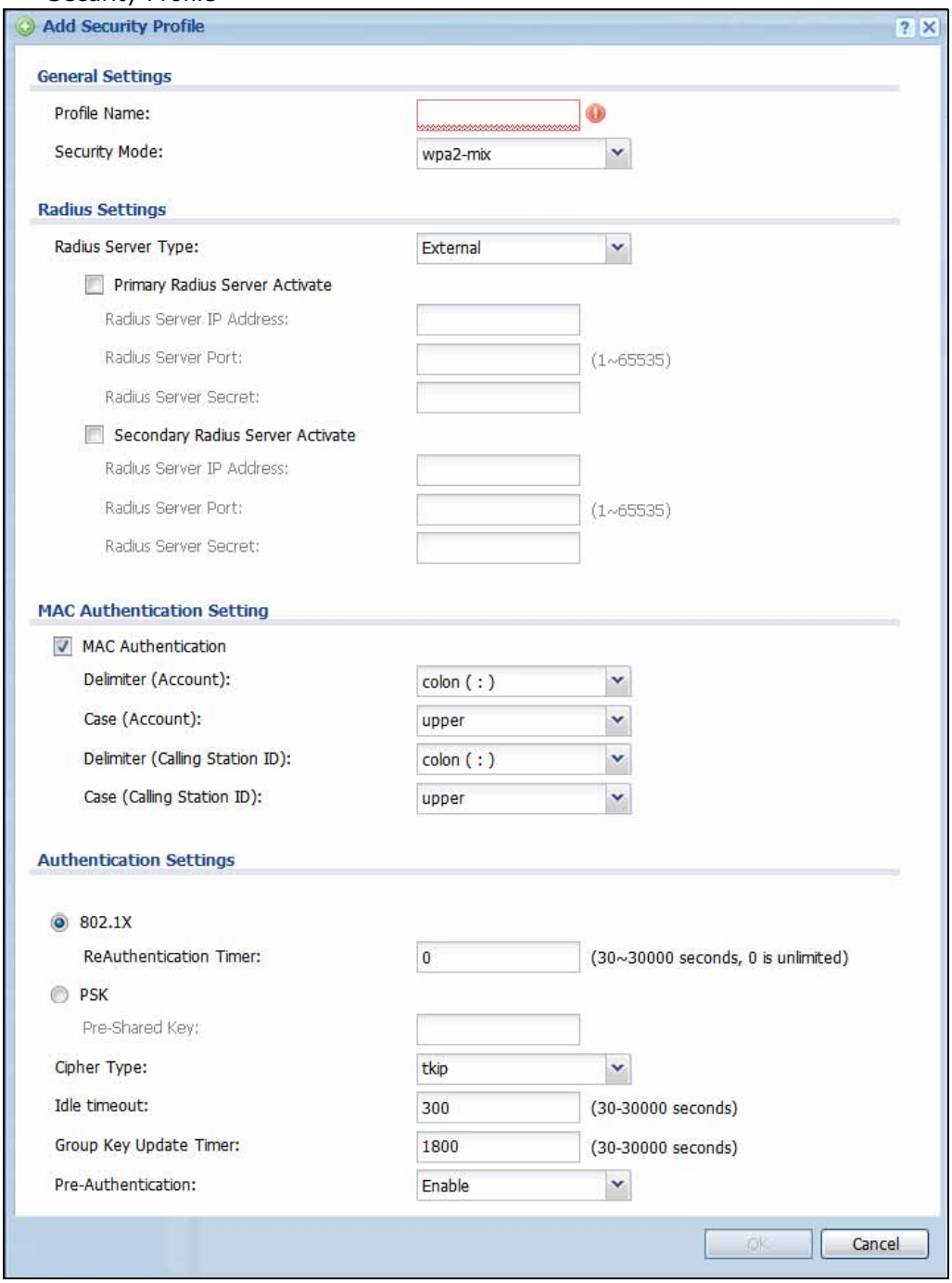
ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новый профиль безопасности.
Edit	Нажмите эту кнопку, чтобы изменить свойства выбранного профиля безопасности.
Remove	Нажмите эту кнопку, чтобы удалить выбранный профиль безопасности.
Object Reference	С помощью этой кнопки можно посмотреть, какие объекты связаны с выбранным профилем безопасности (например, профиль SSID).
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю безопасности.
Security Mode	Это поле указывает на режим безопасности данного профиля (если таковой есть).

18.3.2.1 Экран Add/Edit Security Profile

С помощью этого экрана можно создать новый или отредактировать существующий профиль безопасности. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите профиль безопасности из списка и нажмите кнопку **Edit**.

Примечание: Перечень опций, доступных на экране, зависит от выбранного режима безопасности (значения в поле **Security Mode**). Здесь показан только экран по умолчанию.

Рисунок 128 Экран Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile



Поля экрана описаны в следующей таблице.

Таблица 115 Экран Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	Введите имя профиля, состоящее из алфавитно-цифровых символов (не более 31). Это имя видно только в Web-конфигураторе и только для целей управления. Допускается использование символов пробела и подчеркивания.
Security Mode	Выберите режим безопасности из списка: **wep**, **wpa**, **wpa2** и **wpa2-mix**.
Radius Server Type	Выберите опцию **Internal**, если необходимо использовать для аутентификации внутреннюю базу устройства NXC, или опцию **External**, если необходимо использовать для аутентификации внешний сервер RADIUS.
Primary / Secondary Radius Server Activate	Выберите эту опцию, чтобы устройство NXC использовало указанный сервер RADIUS.
Radius Server IP Address	Укажите IP-адрес сервера RADIUS, который будет использоваться для аутентификации.
Radius Server Port	Укажите номер порта сервера RADIUS, который будет использоваться для аутентификации.
Radius Server Secret	Укажите общий секретный пароль для сервера RADIUS, который будет использоваться для аутентификации.
Аутентификация по MAC-адресу	Выберите эту опцию, если необходимо использовать внешний сервер для аутентификации беспроводных клиентов по MAC-адресам. В случае, если пройти аутентификацию по MAC-адресу не удалось, пользователь не получит IP-адрес. Подробную информацию об учетных записях пользователей типа mac-address можно найти на стр. 210. Для аутентификации по MAC-адресам внешний сервер может использовать учетную запись беспроводного клиента (имя пользователя/пароль) или идентификатор вызывающей станции (Calling Station ID). Укажите значения для тех параметров, которые использует внешний сервер.
Auth. Method	Это поле доступно только в том случае, если в поле RADIUS server type выбрана опция **Internal**. Выберите метод аутентификации, если хотя бы один такой метод был создан на экране **Configuration > Object > Auth. Method**.
Delimiter (Account)	Выберите разделитель, который внешний сервер будет использовать при обработке двухсимвольных пар внутри MAC-адресов учетных записей.
Case (Account)	Выберите регистр (верхний **upper** или нижний **lower**), в котором внешний сервер принимает буквы, содержащиеся в MAC-адресах учетных записей.
Delimiter (Calling Station ID)	Серверы RADIUS могут запросить значение MAC-адреса, содержащееся в атрибуте RADIUS идентификатора вызывающей станции (Calling Station ID). Выберите разделитель, который внешний сервер будет использовать при обработке двухсимвольных пар внутри MAC-адресов вызывающих станций.
Case (Calling Station ID)	Выберите регистр (верхний **upper** или нижний **lower**), в котором внешний сервер принимает буквы, содержащиеся в MAC-адресах вызывающих станций.
Authentication Settings	
802.1X	Выберите эту опцию, чтобы включить безопасную аутентификацию 802.1x.
Reauthentication Timer	Укажите длительность интервала между запросами на аутентификацию (в секундах). 0 будет означать бесконечный интервал.
Idle Timeout	Укажите длительность интервала (в секундах), в течение которого клиент может быть неактивным без необходимости пройти аутентификацию еще раз.
Authentication Type	Выберите метод аутентификации WEP. Возможные варианты: **Open** и **Share** key.

Таблица 115 Экран Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile (продолжение)

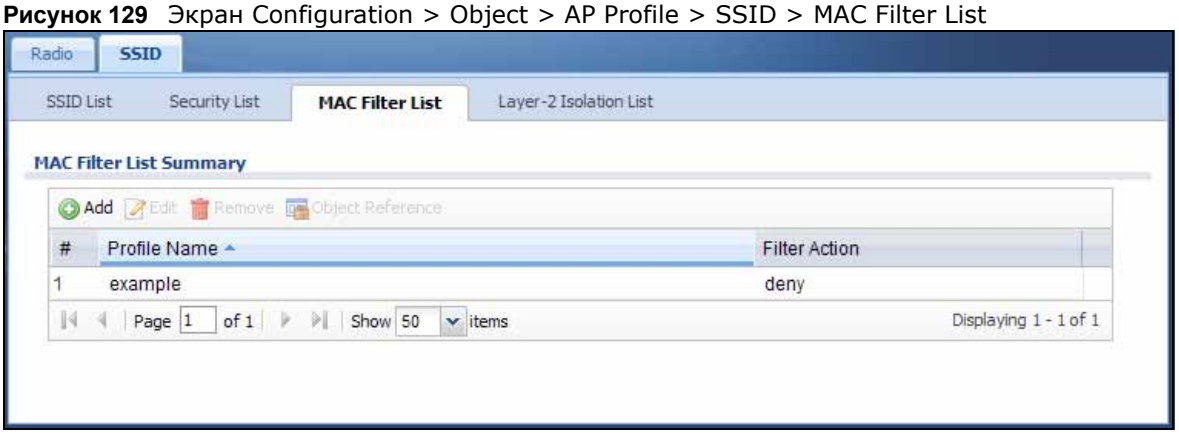
ПОЛЕ	ОПИСАНИЕ
Key Length	Выберите длину ключа (в битах), который будет использоваться для шифрования WEP-соединений. Если выбран вариант **WEP-64**: • Введите 10 шестнадцатеричных цифр в диапазоне «A-F», «a-f» и «0-9» (например, 0x11AA22BB33) для каждого используемого ключа. или • Введите 5 ASCII-символов (чувствительных к регистру) в диапазоне «a-z», «A-Z» и «0-9» (например, MyKey) для каждого используемого ключа. Если выбран вариант **WEP-128**: • Введите 26 шестнадцатеричных цифр в диапазоне «A-F», «a-f» и «0-9» (например, 0x00112233445566778899AABBCC) для каждого используемого ключа. или • Введите 13 ASCII-символов (чувствительных к регистру) в диапазоне «a-z», «A-Z» и «0-9» (например, MyKey12345678) для каждого используемого ключа.
Key 1~4	В зависимости от варианта, выбранного в поле **Key Length**, введите шестнадцатеричный или ASCII-ключ соответствующей длины.
PSK	Выберите эту опцию, если необходимо использовать предварительно выданный ключ (Pre-Shared Key) с шифрованием WPA.
Pre-Shared Key	Введите предварительно выданный ключ (от 8 до 63 ASCII-символов, чувствительных к регистру, включая пробелы и символы или 64 шестнадцатеричных символа).
Cipher Type	Выберите тип шифра из списка. • **auto** – Система автоматически выберет оптимальный из доступных шифров с учетом того, какой шифр использует беспроводной клиент, пытающийся установить соединение. • **tkip** – Это метод шифрования по протоколу TKIP (Temporal Key Integrity Protocol, протокол обеспечения целостности со временным ключом), который позже был разработан как дополнение к протоколу шифрования WEP для обеспечения большей безопасности. Не все беспроводные клиенты поддерживают этот протокол. • **aes** – Это метод шифрования по стандарту AES (Advanced Encryption Standard). Этот протокол был разработан позднее протокола TKIP и является значительно более устойчивым. Не все беспроводные клиенты поддерживают этот протокол.
Group Key Update Timer	Укажите длительность интервала (в секундах), по истечении которого точка доступа обновляет групповой ключ шифрования WPA.
Pre-Authentication	Это поле будет доступным, если в поле **Security Mode** выбрана одна из опций **wpa2** или **wpa2-mix** и включен режим аутентификации 802.1x. Включите (**Enable**) или отключите (**Disable**) предварительную аутентификацию, чтобы данная точка доступа отправляла сведения об аутентификации другим точкам доступа в сети, позволяя подключенным беспроводным клиентам переходить от одной точки доступа к другой без прохождения повторной аутентификации.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

18.3.3 Экран MAC Filter List

С помощью этого экрана можно создавать профили фильтрации MAC, предназначенные для беспроводных сетей, и управлять ими. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Примечание: Всего на устройстве NXC может быть создано не более 32 профилей типа фильтрации MAC.

Рисунок 129 Экран Configuration > Object > AP Profile > SSID > MAC Filter List



Поля экрана описаны в следующей таблице.

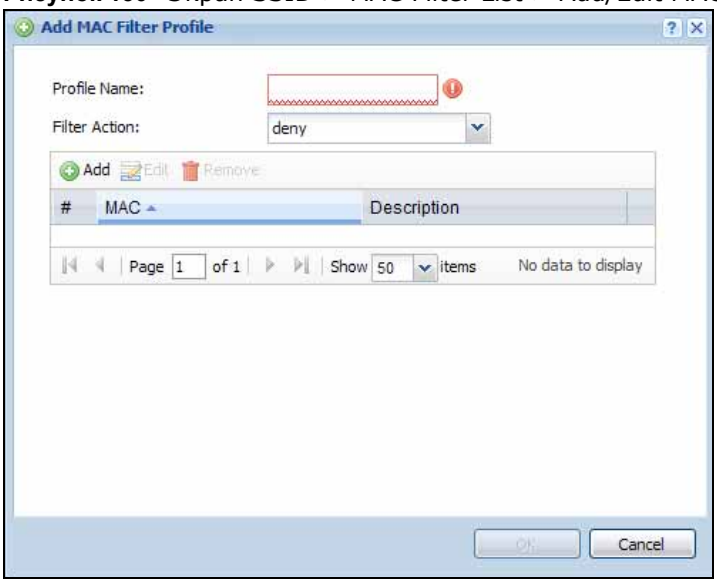
Таблица 116 Экран Configuration > Object > AP Profile > SSID > MAC Filter List

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите на эту кнопку, чтобы создать новый профиль фильтрации MAC.
Edit	Нажмите эту кнопку, чтобы изменить свойства выбранного профиля фильтрации MAC.
Remove	Нажмите эту кнопку, чтобы удалить выбранный профиль фильтрации MAC.
Object Reference	С помощью этой кнопки можно посмотреть, какие объекты ссылаются на выбранный профиль фильтрации MAC (например, профиль SSID).
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю фильтрации MAC.
Filter Action	Это поле показывает действие фильтрации для данного профиля (если таковое есть).

18.3.3.1 Экран Add/Edit MAC Filter Profile

С помощью этого экрана можно создать новый или отредактировать существующий профиль фильтрации MAC. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите нужный профиль фильтрации MAC из списка и нажмите кнопку **Edit**.

Рисунок 130 Экран SSID > MAC Filter List > Add/Edit MAC Filter Profile



Поля экрана описаны в следующей таблице.

Таблица 117 Экран SSID > MAC Filter List > Add/Edit MAC Filter Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	Введите имя профиля, состоящее из алфавитно-цифровых символов (не более 31). Это имя видно только в Web-конфигураторе и только для целей управления. Допускается использование символов пробела и подчеркивания.
Filter Action	Выберите опцию **allow**, если необходимо разрешить беспроводным клиентам, чьи MAC-адреса указаны в этом профиле, подключиться к сети с идентификатором SSID; выберите опцию **deny**, если необходимо заблокировать доступ со стороны беспроводных клиентов, чьи MAC-адреса указаны в этом профиле.
Add	Нажмите эту кнопку, чтобы добавить MAC-адрес в список профиля.
Edit	Нажмите эту кнопку, чтобы изменить выбранный MAC-адрес в списке профиля.
Remove	Нажмите эту кнопку, чтобы удалить выбранный MAC-адрес из списка профиля.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
MAC	Это поле содержит MAC-адрес, ассоциированный с данным профилем.
Description	Это поле содержит описание для MAC-адреса, ассоциированного с данным профилем. Чтобы сделать поле описания редактируемым, достаточно щелкнуть по нему. Длина описания может составлять не более 60 символов, в описании также можно использовать пробелы и подчеркивания.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

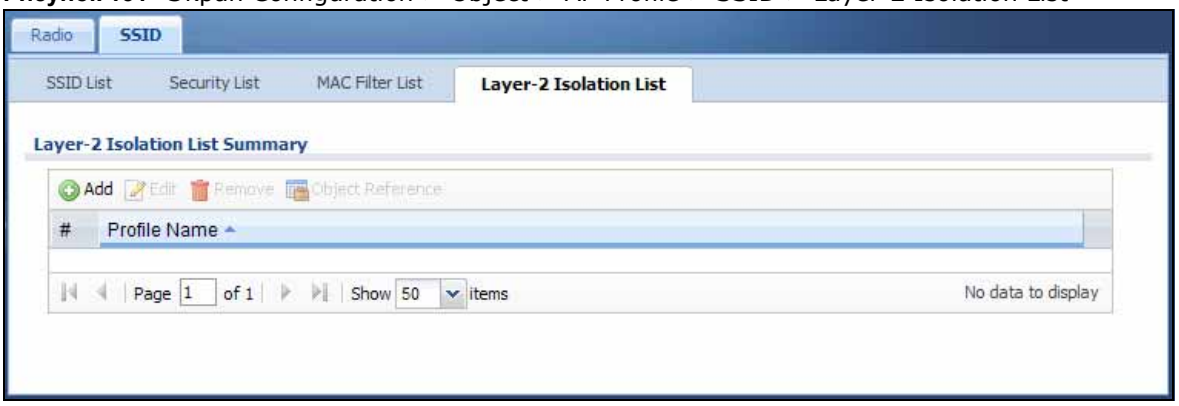
18.3.4 Экран Layer-2 Isolation List

С помощью этого экрана можно создавать профили изоляции второго уровня, предназначенные для беспроводных сетей, и управлять ими. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > AP Profile > SSID > Layer-2 Isolation List**.

Если MAC-адрес устройства НЕ присутствует в списке профиля изоляции второго уровня, то это устройство не сможет установить связь с другими устройствами в сети с тем же SSID, если в ней включена функция изоляции второго уровня.

Примечание: Всего на устройстве NXC может быть создано не более 32 профилей изоляции второго уровня.

Рисунок 131 Экран Configuration > Object > AP Profile > SSID > Layer-2 Isolation List



Поля экрана описаны в следующей таблице.

Таблица 118 Экран Configuration > Object > AP Profile > SSID > Layer-2 Isolation List

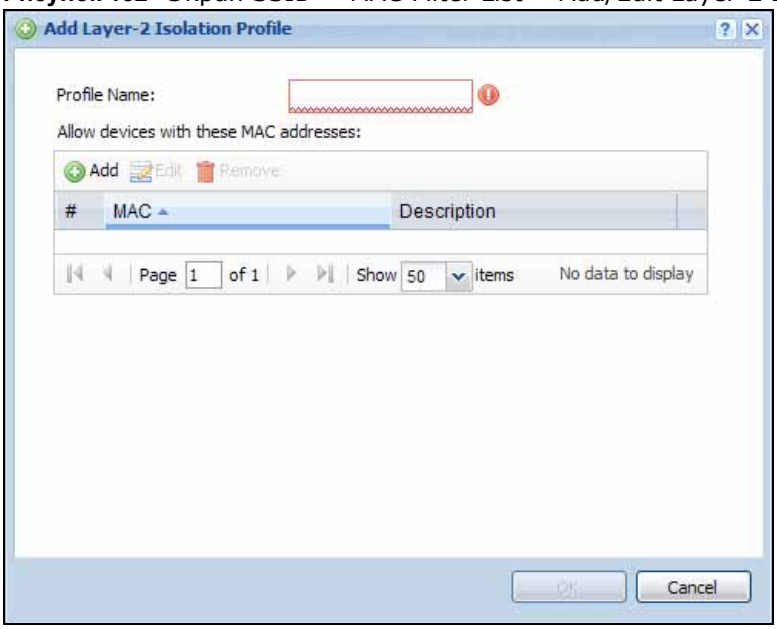
ПОЛЕ	ОПИСАНИЕ
Add	Нажмите на эту кнопку, чтобы создать новый профиль изоляции второго уровня.
Edit	Нажмите на эту кнопку, чтобы изменить выбранный профиль изоляции второго уровня.
Remove	Нажмите на эту кнопку, чтобы удалить выбранный профиль изоляции второго уровня.
Object Reference	С помощью этой кнопки можно посмотреть, какие объекты связаны с выбранным профилем изоляции второго уровня (например, профиль SSID).
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю изоляции второго уровня.

18.3.4.1 Экран Add/Edit Layer-2 Isolation Profile

С помощью этого экрана можно создать новый или отредактировать существующий профиль изоляции второго уровня. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите нужный профиль изоляции второго уровня из списка и нажмите кнопку **Edit**.

Примечание: Необходимо знать MAC-адреса всех устройств, к которым требуется разрешить доступ со стороны других устройств в сети с тем же SSID, если к этой сети применен профиль изоляции второго уровня.

Рисунок 132 Экран SSID > MAC Filter List > Add/Edit Layer-2 Isolation Profile



Поля экрана описаны в следующей таблице.

Таблица 119 Экран SSID > MAC Filter List > Add/Edit Layer-2 Isolation Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	Введите имя профиля, состоящее из алфавитно-цифровых символов (не более 31). Это имя видно только в Web-конфигураторе и только для целей управления. В этом поле можно использовать подчеркивания.
Add	Нажмите эту кнопку, чтобы добавить MAC-адрес в список профиля.
Edit	Нажмите эту кнопку, чтобы изменить выбранный MAC-адрес в списке профиля.
Remove	Нажмите эту кнопку, чтобы удалить выбранный MAC-адрес из списка профиля.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
MAC	Это поле содержит MAC-адрес, ассоциированный с данным профилем.
Description	Это поле содержит описание для MAC-адреса, ассоциированного с данным профилем. Чтобы сделать поле описания редактируемым, достаточно щелкнуть по нему. Длина описания может составлять не более 60 символов, в описании также можно использовать пробелы и подчеркивания.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

19

Профили мониторинга

19.1 Обзор

Экран MON Profile позволяет настроить конфигурации режима мониторинга, которые позволят беспроводным точкам, подключенным к устройству, выполнять сканирование других беспроводных устройств, работающих поблизости. При обнаружении таких устройств можно воспользоваться экраном MON Mode (гл. 7 на стр. 99), чтобы классифицировать их как мошеннические или дружеские, и далее поступать с ними надлежащим образом.

19.1.1 О чем рассказывается в этой главе

Экран **MON Profile** (разд. 19.2 на стр. 250) позволяет создать готовые конфигурации режима мониторинга для точек доступа.

19.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Активное сканирование

Беспроводное устройство мониторинга, совместимое со стандартом 802.11, выполняет активное сканирование в том случае, если ему отдана явная команда произвести сканирование указанного канала или нескольких каналов на предмет наличия других беспроводных устройств, вещающих на частотах, определенных стандартом 802.11, путем отправки кадров зондирующих запросов.

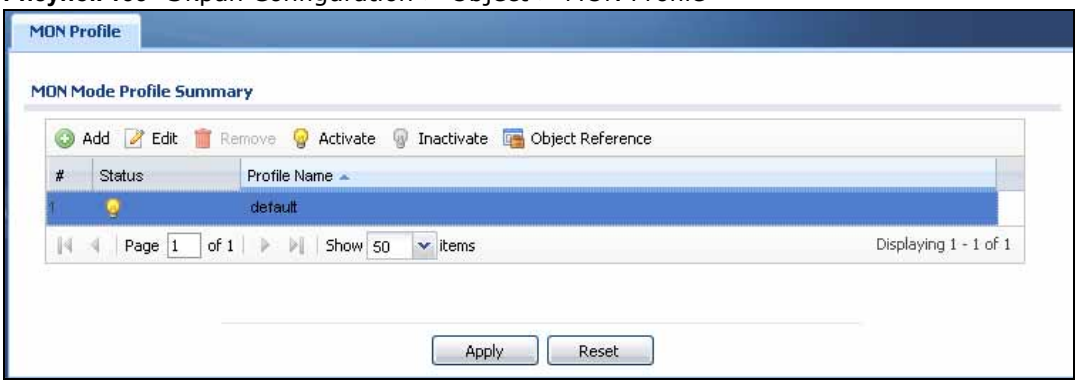
Пассивное сканирование

Беспроводное устройство мониторинга, совместимое со стандартом 802.11, выполняет активное сканирование в том случае, если оно периодически прослушивает указанный канал или несколько каналов на предмет наличия других беспроводных устройств, вещающих на частотах, определенных стандартом 802.11.

19.2 Экран MON Profile

С помощью этого экрана можно создавать конфигурации режимов мониторинга для точек доступа. Чтобы открыть этот экран, выполните вход на устройство через Web-конфигуратор и выберите в меню **Configuration > Object > MON Profile**.

Рисунок 133 Экран Configuration > Object > MON Profile



Поля экрана описаны в следующей таблице.

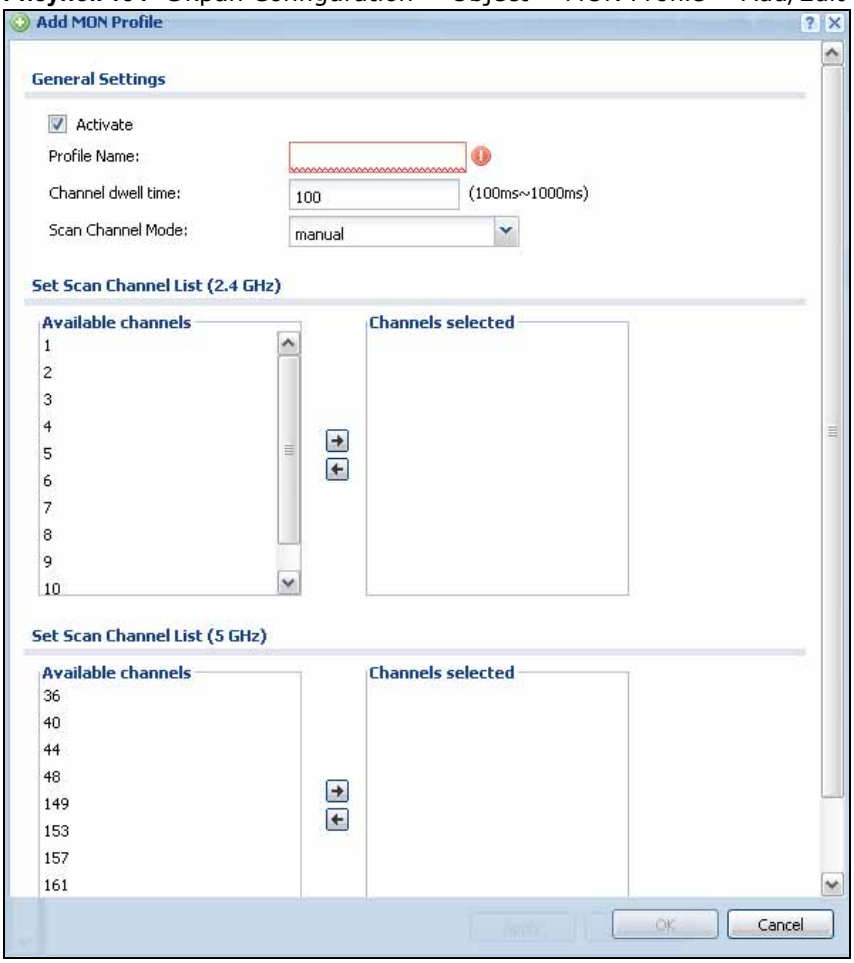
Таблица 120 Экран Configuration > Object > MON Profile

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новый профиль режима мониторинга.
Edit	Нажмите эту кнопку, чтобы изменить выбранный профиль режима мониторинга.
Remove	Нажмите эту кнопку, чтобы удалить выбранный профиль режима мониторинга.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
Object Reference	С помощью этой кнопки можно посмотреть, какие объекты связаны с выбранным профилем режима мониторинга (например, профиль управления точками доступа).
#	В этом поле содержится порядковое значение, не связанное с каким-либо пользователем.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю мониторинга.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

19.2.1 Экран Add/Edit MON Profile

С помощью этого экрана можно создать новый или отредактировать существующий профиль режима мониторинга. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите существующий профиль режима мониторинга и нажмите кнопку **Edit**.

Рисунок 134 Экран Configuration > Object > MON Profile > Add/Edit MON Profile



Поля экрана описаны в следующей таблице.

Таблица 121 Экран Configuration > Object > MON Profile > Add/Edit MON Profile

ПОЛЕ	ОПИСАНИЕ
Activate	Выберите эту опцию, чтобы активировать данный профиль режима мониторинга.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю режима мониторинга.
Channel dwell time	Укажите интервал (в миллисекундах), по истечении которого точка доступа переключается на другой канал для мониторинга.
Scan Channel Mode	Выберите опцию **auto**, чтобы точка доступа переключалась на следующий по порядку канал по истечении интервала, указанного в поле **Channel dwell time**. Выберите опцию **manual**, если необходимо составить список конкретных каналов, на которые будет в циклическом режиме переключаться точка доступа по истечении интервала, указанного в поле **Channel dwell time**. При выборе этой опции становятся доступными опции **Scan Channel List**.
Set Scan Channel List (2.4 GHz)	Переместите канал из столбца **Available channels** в столбец **Channels selected**, чтобы точки доступа, использующие этот профиль, сканировали этот канал, если в поле **Scan Channel Mode** выбрана опция manual. Эти каналы ограничены диапазоном 2 ГГц (802.11 b/g/n).

Таблица 121 Экран Configuration > Object > MON Profile > Add/Edit MON Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Set Scan Channel List (5 GHz)	Переместите канал из столбца **Available channels** в столбец **Channels selected**, чтобы точки доступа, использующие этот профиль, сканировали этот канал, если в поле **Scan Channel Mode** выбрана опция manual. Эти каналы ограничены диапазоном 5 ГГц (802.11 a/n).
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

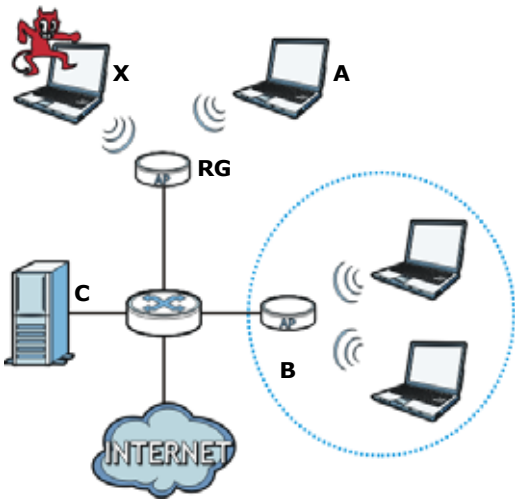
19.3 Справочная техническая информация

В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

Мошеннические точки доступа

Мошенническими называют точки доступа, которые действуют в зоне покрытия сети и при этом не контролируются администраторами сети. Они могут стать причиной возникновения брешей в политике безопасности сети. Злоумышленники могут воспользоваться более слабой (или вообще отсутствующей) защитой мошеннической точки доступа для проникновения в сеть или создать собственные мошеннические точки доступа для получения информации от беспроводных клиентов. Если сканирование выявило мошенническую точку доступа, можно воспользоваться коммерческим программным обеспечением для определения ее физического местоположения.

Рисунок 135 Пример мошеннической точки доступа



В приведенном выше примере безопасность корпоративной сети оказалась под угрозой из-за мошеннической точки доступа (**RG**), установленной одним из сотрудников на своей рабочей станции с целью подключения ноутбука к беспроводной сети (**A**). Легитимная беспроводная сеть компании (пунктирный эллипс **B**) надежно защищена, но беспроводная точка доступа использует слабые средства защиты, которые с легкостью обходит злоумышленник (**X**) с помощью специального программного обеспечения для взлома системы шифрования. В этом

примере злоумышленник получает доступ к сети компании, в том числе и к файловому серверу (**C**), на котором хранятся важные данные.

Дружественные точки доступа

Если беспроводная сеть включает в себя две и более точек доступа, следует также составить список «дружественных» точек доступа. Дружественными точками доступа называют другие точки доступа, которые обнаружены в сети, а также любые другие точки доступа, о которых известно, что они не представляют угрозы (например, точки доступа из распознанных сетей). Рекомендуется часто экспортировать (сохранять) список дружественных точек доступа, особенно если сеть насчитывает большое количество точек доступа.

20

Профили ZyMesh

20.1 Обзор

Эта глава описывает процесс настройки на устройстве NXC профилей ZyMesh, которые можно применить к управляемым точкам доступа.

ZyMesh – это внутрифирменная функция ZyXEL. При использовании функции ZyMesh две и более управляемых точек доступа формируют структуру WDS (Wireless Distribution System, систему беспроводного распространения) для расширения беспроводной сети и предоставления служб или пересылки трафика между устройством NXC и беспроводными клиентами. ZyMesh позволяет устройству the NXC использовать протокол CAPWAP для автоматического обновления настроек на управляемых точках доступа (в режиме повторителя) по беспроводным соединениям. Конфигурирование управляемых точек доступа (в режиме повторителя) осуществляется переход за переходом (hop by hop).

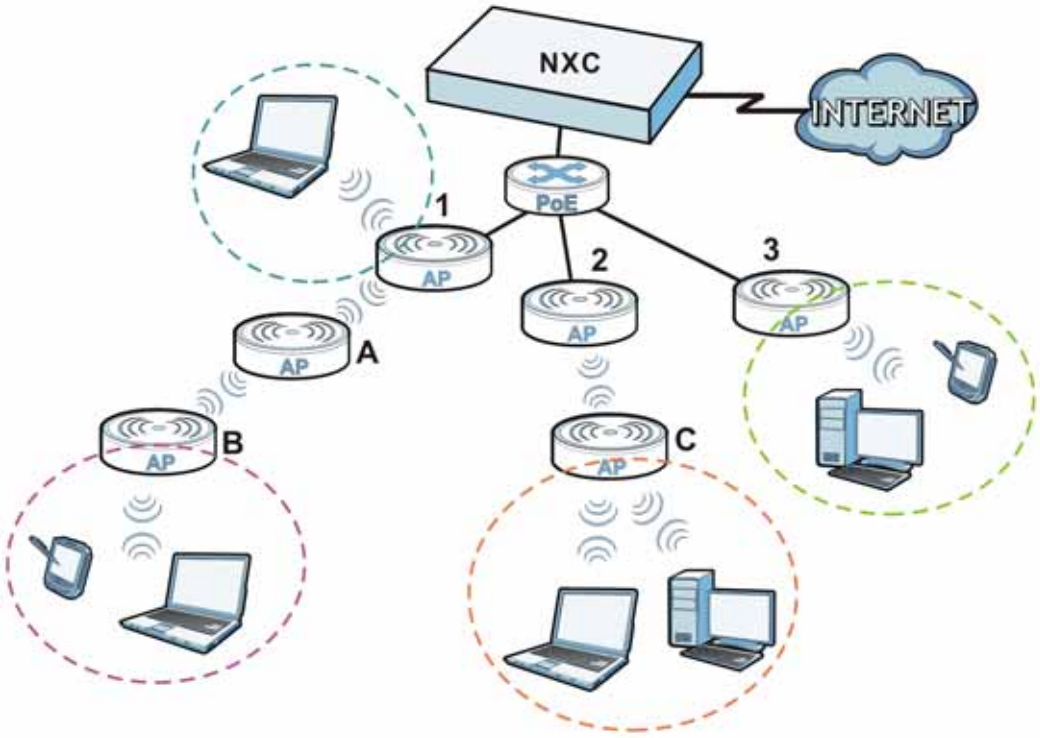
Управляемые точки доступа в структуре WDS или ZyMesh должны использовать одинаковый идентификатор SSID, номер канала и предварительно выданный ключ. Управляемая точка доступа может выступать в сети ZyMesh либо в качестве корневой точки доступа, либо в качестве повторителя.

Примечание: Перед развертыванием в структуре ZyMesh/WDS все управляемые точки доступа должны быть непосредственно подключены к устройству NXC для получения файлов конфигурации. После изменения режима работы управляемой точки доступа на экране **Configuration > Wireless > AP Management** (см. разд. 7.3 на стр. 101) ее необходимо перегрузить.

- Корневая точка доступа: управляемая точка доступа, которая может передавать и получать данные от устройства NXC по проводному соединению Ethernet.
- Повторитель: управляемая точка доступа, которая передает и/или получает данные от устройства NXC по беспроводному соединению через корневую точку доступа.

Примечание: При первом развертывании управляемых точек доступа для формирования структуры ZyMesh/WDS корневая точка доступа должна быть подключена к контроллеру точек доступа (устройству NXC).

В примере, приведенном ниже, управляемые точки доступа **1** и **2** выступают в качестве корневой точки доступа, а управляемые точки доступа **A**, **B** и **C** играют роль повторителей.



Максимально допустимое количество переходов (повторителей между беспроводным клиентом и корневой точкой доступа) в структуре ZyMesh зависит от того, какое количество беспроводных клиентов поддерживает управляемая точка доступа.

Примечание: Чем больше переходов включает в себя соединение в структуре ZyMesh/WDS, тем меньше его пропускная способность.

Примечание: Если беспроводное соединение между корневой точкой доступа и повторителем активно, то повторитель не может передавать данные через собственные порты Ethernet во избежание появления мостовых петель. Соответственно, повторитель может только запитываться от устройства PoE, если для подачи питания на управляемую точку доступа через 8-контактный кабель Ethernet используется технология PoE.

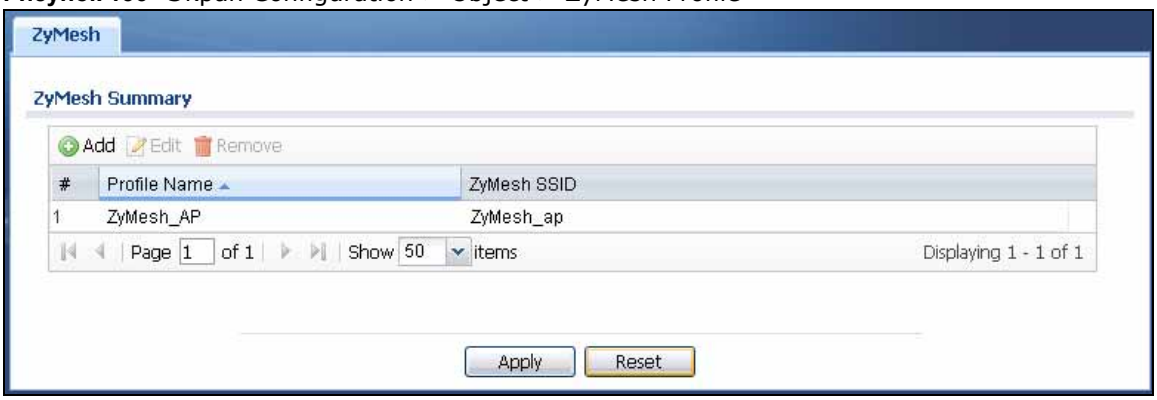
20.1.1 О чем рассказывается в этой главе

Экран **ZyMesh Profile** (разд. 20.2 на стр. 256) позволяет создавать готовые конфигурации ZyMesh для устройства NXC.

20.2 Экран ZyMesh Profile

С помощью этого экрана можно создавать профили ZyMesh, которые могут быть использованы точками доступа, и управлять этими профилями. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > ZyMesh Profile**.

Рисунок 136 Экран Configuration > Object > ZyMesh Profile



Поля экрана описаны в следующей таблице.

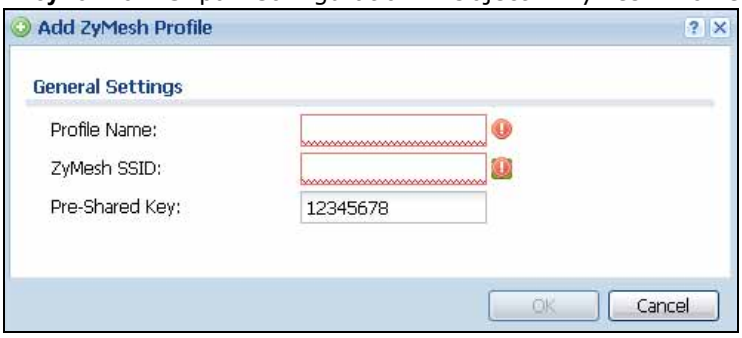
Таблица 122 Экран Configuration > Object > ZyMesh Profile

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новый профиль.
Edit	Нажмите эту кнопку, чтобы изменить выбранный профиль.
Remove	Нажмите эту кнопку, чтобы удалить выбранный профиль.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным профилем.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю.
ZyMesh SSID	Это поле показывает идентификатор SSID, указанный для данного профиля ZyMesh.

20.2.1 Экран Add/Edit ZyMesh Profile

С помощью этого экрана можно создать новый или отредактировать существующий профиль ZyMesh. Чтобы открыть этот экран, нажмите кнопку **Add** или выберите существующий профиль и нажмите кнопку **Edit**.

Рисунок 137 Экран Configuration > Object > ZyMesh Profile > Add/Edit ZyMesh Profile



Поля экрана описаны в следующей таблице.

Таблица 123 Экран Configuration > Object > ZyMesh Profile > Add/Edit ZyMesh Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	Введите имя профиля, состоящее из алфавитно-цифровых символов (не более 31).
ZyMesh SSID	Введите идентификатор сети (SSID), с которым управляемую точку доступа необходимо подключить к корневой точке доступа или повторителю для создания соединения ZyMesh. Примечание: Идентификатор SSID структуры ZyMesh скрыт в исходящем кадре типа beacon, поэтому беспроводное устройство не может получить этот SSID путем сканирования с использованием средств анализа площадок.
Pre-Shared Key	Введите предварительно выданный ключ (от 8 до 63 ASCII-символов, чувствительных к регистру, включая пробелы и специальные символы, или 64 шестнадцатеричных символа). Этот ключ используется для шифрования беспроводного трафика между точками доступа.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

21

Адреса

21.1 Обзор

Адресные объекты могут представлять единичный IP-адрес или диапазон IP-адресов.

21.1.1 О чем рассказывается в этой главе

- Экран **Address** (разд. 21.2 на стр. 259) содержит сводную информацию обо всех адресах на устройстве NXC.
- Сводный экран **Address Group** (разд. 21.3 на стр. 261) и экран **Address Group Add/Edit** позволяют управлять группами адресов устройства NXC.

21.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Адреса

Адресные объекты и группы адресов используются при настройке динамических маршрутов и правил межсетевого экрана. Более подробную информацию о том, как динамические маршруты и правила межсетевого экрана используют адресные объекты и группы адресов, можно найти в соответствующих разделах настоящего документа.

Группы адресов включают в себя адресные объекты и другие группы адресов. Порядок участников в адресной группе не имеет значения.

21.2 Общая информация об адресах

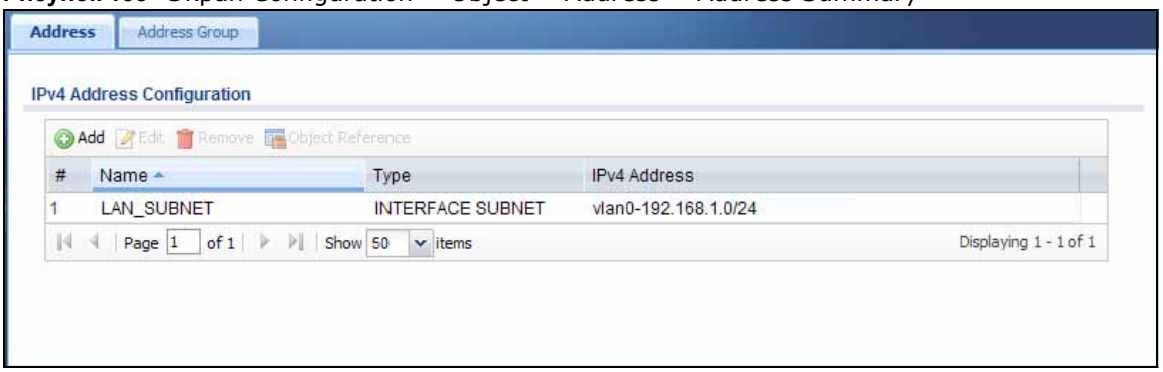
Экраны адресов позволяют создавать адреса, удалять их и управлять ими. Существует несколько типов адресных объектов.

- **HOST** (ХОСТ) – адрес хоста, определяемый IP-адресом **IP Address**.
- **RANGE** (ДИАПАЗОН) – диапазон адресов, определяемый начальным **Starting IP Address** и конечным **Ending IP Address** адресами.
- **SUBNET** (ПОДСЕТЬ) – сетевой адрес, определяемый IP-адресом сети **Network** и маской подсети **Netmask**.

Экран **Address** содержит сводную информацию обо всех адресах устройства NXC. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object** > **Address > Address**. Щелкните по заголовку столбца, чтобы отсортировать записи в таблице по полю,

представленному этим столбцом. Чтобы поменять порядок сортировки на обратный, щелкните по заголовку столбца еще раз.

Рисунок 138 Экран Configuration > Object > Address > Address Summary



Поля экрана описаны в следующей таблице.

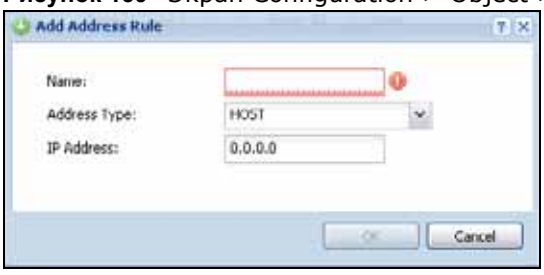
Таблица 124 Экран Configuration > Object > Address > Address Summary

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным адресом.
Name	Это поле показывает заданное имя каждого адресного объекта.
Type	Это поле показывает тип каждого адресного объекта. Опция «**INTERFACE**» означает, что объект использует настройки одного из интерфейсов устройства NXC.
IPv4 Address	Это поле показывает IP-адреса, представленные всеми адресными объектами. Если настройки объекта взяты с одного из интерфейсов устройства NXC, то в этом поле отображается вначале имя этого интерфейса, а затем текущие адресные настройки объекта.

21.2.1 Экран Add/Edit Address

С помощью экрана **Add/Edit Address** можно создавать новые или редактировать существующие адреса. Чтобы открыть этот экран, перейдите на экран **Address** и нажмите на пиктограмму **Add** или пиктограмму **Edit**.

Рисунок 139 Экран Configuration > Object > Address > Address > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 125 Экран Configuration > Object > Address > Address > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя, которое будет использоваться для ссылки на этот адрес. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
Address Type	Выберите тип адреса, который необходимо создать. Возможные варианты: **HOST**, **RANGE**, **SUBNET**, **INTERFACE IP**, **INTERFACE SUBNET** и **INTERFACE GATEWAY**. Примечание: Устройство NXC автоматически обновляет адресные объекты, созданные на основе IP-адреса, подсети или шлюза какого-либо интерфейса, при изменении настроек IP-адреса этого интерфейса. Например, если изменить IP-адрес интерфейса ge1, устройство NXC автоматически обновит соответствующий объект адреса локальной подсети, ссылающийся на этот интерфейс.
IP Address	Это поле становится доступным, если в поле **Address Type** выбрана опция **HOST**. Поле является обязательным для заполнения. Введите IP-адрес, который представляет данный адресный объект.
Starting IP Address	Это поле становится доступным, если в поле **Address Type** выбрана опция **RANGE**. Поле является обязательным для заполнения. Введите начальный адрес диапазона IP-адресов, который представляет данный адресный объект.
Ending IP Address	Это поле становится доступным, если в поле **Address Type** выбрана опция **RANGE**. Поле является обязательным для заполнения. Введите конечный адрес диапазона IP-адресов, который представляет данный адресный объект.
Network	Это поле становится доступным, если в поле **Address Type** выбрана опция **SUBNET**, и в этом случае оно является обязательным для заполнения. Введите IP-адрес сети, которую представляет данный адресный объект.
Netmask	Это поле становится доступным, если в поле **Address Type** выбрана опция **SUBNET**, и в этом случае оно является обязательным для заполнения. Введите маску подсети, которую представляет данный адресный объект. При вводе значений нужно использовать точечно-десятичный формат.
Interface	Если в поле **Address Type** выбрана одна из опций **INTERFACE IP**, **INTERFACE SUBNET** или **INTERFACE GATEWAY**, укажите в этом поле сетевой интерфейс, который представляет данный адресный объект.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

21.3 Сводный экран Address Group

Экран **Address Group** содержит сводную информацию обо всех адресных группах. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object** > **Address > Address Group**. Щелкните по заголовку столбца, чтобы отсортировать записи в таблице по полю, представленному этим столбцом. Чтобы поменять порядок сортировки на обратный, щелкните по заголовку столбца еще раз.

Рисунок 140 Экран Configuration > Object > Address > Address Group

Поля экрана описаны в следующей таблице.

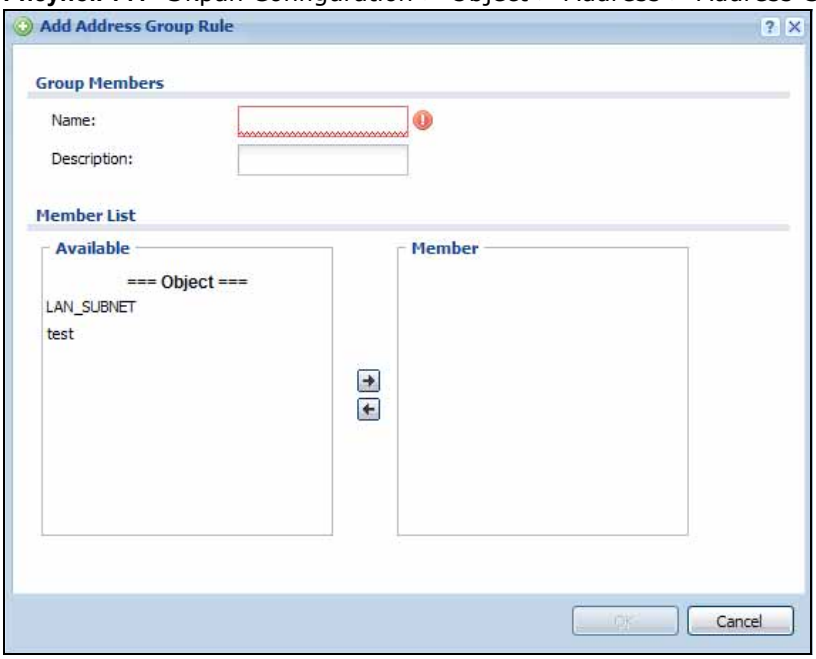
Таблица 126 Экран Configuration > Object > Address > Address Group

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с какой-либо адресной группой.
Name	Это поле показывает имя каждой адресной группы.
Description	Это поле показывает описание каждой адресной группы (если таковое есть).

21.3.1 Экран Add/Edit Address Group Rule

С помощью экрана **Add/Edit Address Group Rule** можно создавать новые или редактировать существующие адресные группы. Чтобы открыть этот экран, перейдите к экрану **Address Group** и нажмите на пиктограмму **Add** icon или на пиктограмму **Edit**.

Рисунок 141 Экран Configuration > Object > Address > Address Group > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 127 Экран Configuration > Object > Address > Address Group > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя адресной группы. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
Description	Это поле показывает описание каждой адресной группы (если таковое есть). Длина описания может составлять не более 60 символов, в описании можно использовать знаки пунктуации и пробелы.
Member List	Поле **Member** List показывает имена объектов адресов и адресных групп, которые были добавлены в данную адресную группу. Порядок участников группы не имеет значения. Выберите в списке **Available** объекты, которые необходимо включить в данную группу, и переместите их в список **Member**. Можно дважды щелкнуть по одной записи, чтобы перенести ее, или воспользоваться клавишами [Shift] или [Ctrl], чтобы выбрать две и более записей и перенести их. Переместите пользователей, которых необходимо исключить из группы, в список **Available**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

22

Службы

22.1 Обзор

Объекты служб используют для описания приложений TCP, приложений UDP и сообщений ICMP. Кроме того, можно создавать группы служб, которые могут ссылаться на два и более объектов служб, задействованных в других функциях.

22.1.1 О чем рассказывается в этой главе

- Экраны **Service** (разд. 22.2 на стр. 266) позволяют просматривать, создавать и менять службы на устройстве NXC.
- Экраны **Service Group** (разд. 22.2 на стр. 266) позволяют просматривать, создавать и менять группы служб на устройстве NXC.

22.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Стек протоколов IP

В основе протоколов из стека IP лежит восьмибитовое протокольное поле из заголовка пакета IP. Это поле представляет протокол следующего уровня, который пересылается в этом пакете. В этом разделе рассматриваются три протокола IP из числа наиболее распространенных.

Компьютеры используют протоколы TCP (Transmission Control Protocol, IP protocol 6) и UDP (User Datagram Protocol, IP protocol 17) для взаимного обмена данными. TCP гарантирует надежную доставку, но он работает более медленно и является более сложным. Примером использования TCP могут служить такие протоколы, как FTP, HTTP, SMTP и TELNET. UDP проще и быстрее, но он отличается меньшей надежностью. В качестве примеров его использования можно назвать такие протоколы, как DHCP, DNS, RIP и SNMP.

TCP создает соединения между компьютерами для обмена данными. После установки соединения компьютеры выполняют обмен данными. Если блок данных приходит вне очереди или отсутствует, TCP помещает его в очередь или ожидает повторной передачи этого блока данных. По окончании обмена соединение разрывается.

При использовании протокола UDP компьютеры посылают друг другу короткие сообщения. Доставка сообщения в свою очередь, как и доставка сообщения вообще при этом не гарантируется.

И TCP, и UDP используют порты для идентификации источника и назначения. Каждый порт представляет собой 16-разрядное число. Некоторые номера портов стандартизированы и используются системными процессами низкого уровня; многие другие порты не имеют специального значения.

В отличие от TCP и UDP, протокол ICMP (Internet Control Message Protocol, IP protocol 1) используется преимущественно для отправки сообщений об ошибках или для анализа проблем. Например, ICMP используется для отправки ответа, если компьютер становится недоступным. Еще один вариант применения – ping. ICMP не гарантирует доставку, но в сетях сообщения ICMP часто обрабатываются по-разному, иногда сетевые устройства изучают содержимое сообщения, чтобы решить, куда его отправлять.

Объекты служб и группы служб

Объекты служб используют для описания протоколов IP.

- приложения TCP
- приложения UDP
- приложения ICMP
- службы, созданные пользователями (для других типов протоколов IP)

Эти объекты используют в маршрутах на основе политик.

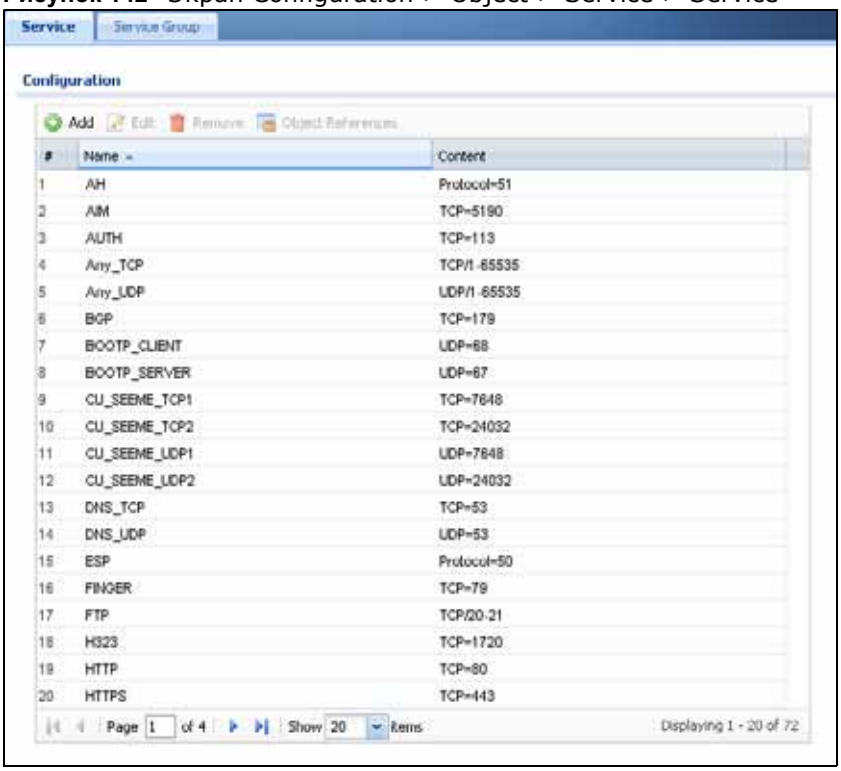
Группы служб уместно использовать в тех случаях, когда необходимо создать одно правило для нескольких служб вместо того, чтобы создавать отдельные правила для каждой службы. Группы служб могут включать в себя службы и другие группы служб. Порядок участников в группе служб не имеет значения.

22.2 Сводный экран Service

Сводный экран **Service** содержит сводную информацию обо всех службах и их описания. Кроме того, этот экран позволяет добавлять, изменять и удалять службы.

Чтобы открыть этот экран, выполните вход на устройство через Web-конфигуратор, а затем выберите в меню **Configuration > Object > Service > Service**. Щелкните по заголовку столбца, чтобы отсортировать записи в таблице по полю, представленному этим столбцом. Чтобы поменять порядок сортировки на обратный, щелкните по заголовку столбца еще раз.

Рисунок 142 Экран Configuration > Object > Service > Service



Поля экрана описаны в следующей таблице.

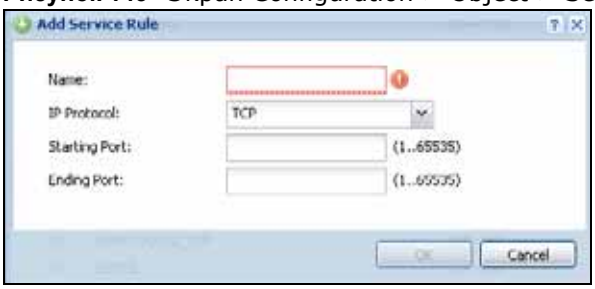
Таблица 128 Экран Configuration > Object > Service > Service

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с какой-либо конкретной службой.
Name	В этом поле отображается название каждой службы.
Content	В этом поле отображается описание каждой службы.

22.2.1 Экран Add/Edit Service Rule

С помощью экрана **Add/Edit Service Rule** можно создавать новые или редактировать существующие службы. Чтобы открыть этот экран, перейдите на экран **Service** и нажмите на пиктограмму **Add** или на пиктограмму **Edit**.

Рисунок 143 Экран Configuration > Object > Service > Service > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 129 Экран Configuration > Object > Service > Service > Add/Edit

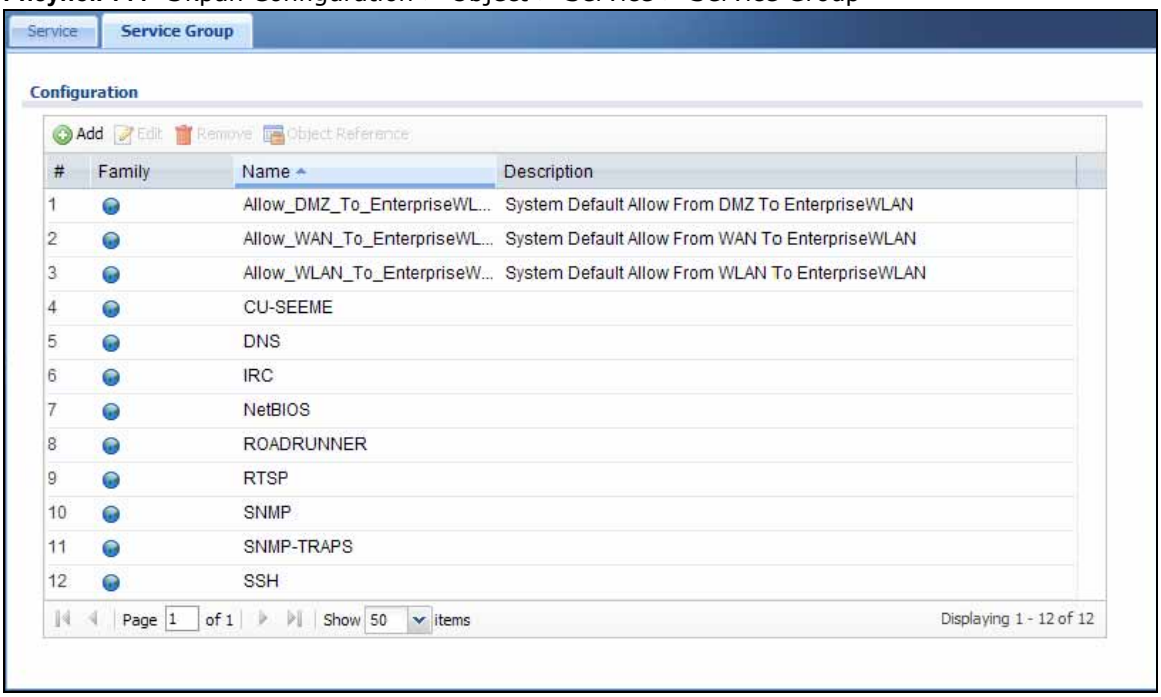
ПОЛЕ	ОПИСАНИЕ
Name	Введите имя, которое будет использоваться для ссылки на эту службу. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
IP Protocol	Выберите протокол, используемый данной службой. Возможные варианты: **TCP**, **UDP**, **ICMP** и **User Defined** (Задано пользователем).
Starting Port Ending Port	Это поле появляется на экране, если в поле **IP Protocol** выбрана опция **TCP** или опция **UDP**. Укажите номер порта (или номера портов), который использует данная служба. Если заполнить одно из этих полей, это будет означать, что служба использует этот порт. Если заполнить оба поля, это будет означать, что служба использует диапазон портов, определяемый этими двумя значениями.
ICMP Type	Это поле появляется на экране, если в поле **IP Protocol** выбрана опция **ICMP Type**. Выберите сообщение ICMP, которое использует данная служба. Это поле показывает текст сообщения (а не его номер).
IP Protocol Number	Это поле появляется на экране, если в поле **IP Protocol** выбрана опция **User Defined**. Введите номер протокола следующего уровня (протокола IP). Значения можно выбирать из диапазона от 0 до 255.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

22.3 Сводный экран Service Group

Экран **Service Group** содержит сводную информацию обо всех группах служб. Кроме того, этот экран позволяет создавать, редактировать и удалять группы служб.

Чтобы открыть этот экран, выполните вход на устройство через Web-конфигуратор, а затем выберите в меню **Configuration > Object** > **Service** > **Service Group**.

Рисунок 144 Экран Configuration > Object > Service > Service Group



Поля экрана описаны в следующей таблице.

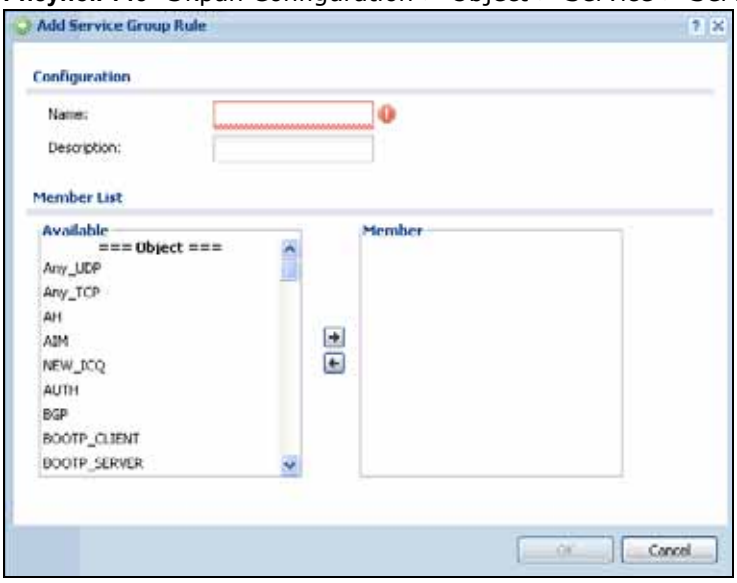
Таблица 130 Экран Configuration > Object > Service > Service Group

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с какой-либо группой служб.
Name	Это поле показывает имя каждой группы служб.
Description	Это поле показывает описание каждой группы служб (если таковое есть).

22.3.1 Экран Add/Edit Service Group Rule

С помощью экрана **Add/Edit Service Group Rule** можно создавать новые или редактировать существующие группы служб. Чтобы открыть этот экран, перейдите к экрану **Service Group** и нажмите на пиктограмму **Add** или на пиктограмму **Edit**.

Рисунок 145 Экран Configuration > Object > Service > Service Group > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 131 Экран Configuration > Object > Service > Service Group > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя группы служб. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
Description	Введите описание группы служб (если таковое есть). В поле можно ввести до 60 печатных символов ASCII.
Member List	Поле **Member** показывает имена объектов служб и групп служб, которые были добавлены в данную группу служб. Порядок участников группы не имеет значения. Выберите в списке **Available** объекты, которые необходимо включить в данную группу, и переместите их в список **Member**. Можно дважды щелкнуть по одной записи, чтобы перенести ее, или воспользоваться клавишами [Shift] или [Ctrl], чтобы выбрать две и более записей и перенести их. Переместите пользователей, которых необходимо исключить из группы, в список **Available**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

23

Расписания

23.1 Обзор

Расписания используют для настройки однократного и периодического применения маршрутов на основе политик. Устройство NXC поддерживает однократные и повторяющиеся расписания. Однократные расписания действуют только один раз, повторяющиеся расписания обычно выполняются многократно. Расписания обоих типов используют текущие настройки даты и времени устройства NXC.

Примечание: Расписания используют текущие настройки даты и времени устройства NXC.

23.1.1 О чем рассказывается в этой главе

- Экран **Schedule** (разд. 23.2 на стр. 271) показывает список всех расписаний на устройстве NXC.
- Экран **One-Time Schedule Add/Edit** (разд. 23.2.1 на стр. 272) служит для создания и редактирования однократных расписаний.
- Экран **Recurring Schedule Add/Edit** (разд. 23.2.2 на стр. 273) служит для создания и редактирования повторяющихся расписаний.

23.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Однократные расписания

Однократные расписания начинают и заканчивают действовать в определенные дату и время. Однократные расписания бывают полезны в течение продолжительных выходных и каникул.

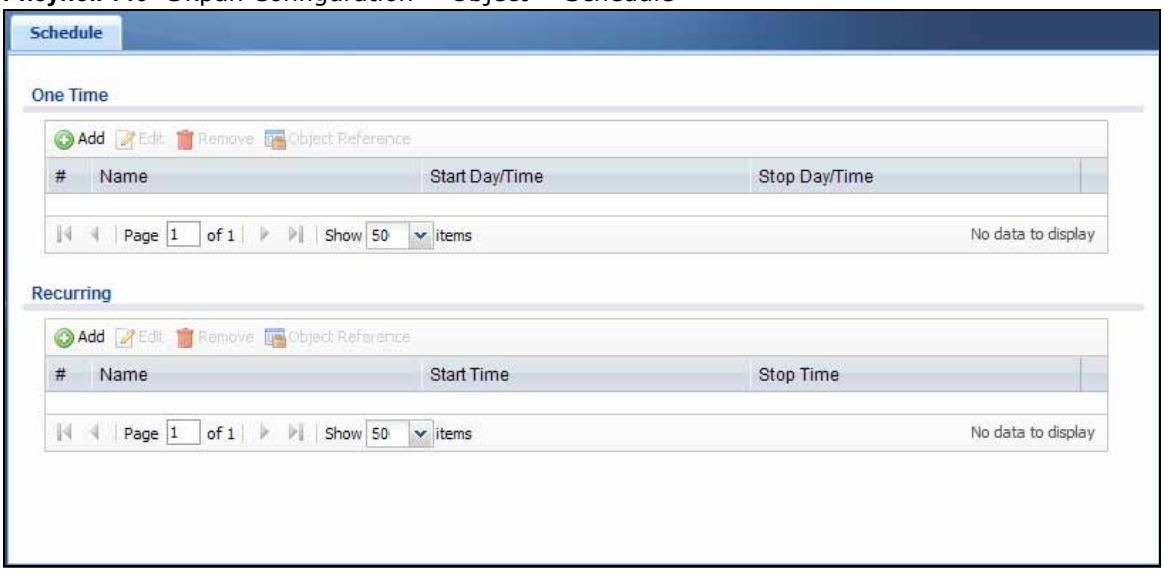
Повторяющиеся расписания

Повторяющиеся расписания начинают и заканчивают действовать в определенное время и действуют в выбранные дни недели (воскресенье, понедельник, вторник, среда, четверг, пятницу и субботу). Повторяющиеся расписания всегда начинают и заканчивают действовать в один и тот же день. Повторяющиеся расписания удобно использовать для выполнения периодических действий в рабочее и нерабочие часы.

23.2 Сводный экран Schedule

Экран **Schedule** содержит сводную информацию обо всех расписаниях устройства NXC. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object** > **Schedule**.

Рисунок 146 Экран Configuration > Object > Schedule



Поля экрана описаны в следующей таблице.

Таблица 132 Экран Configuration > Object > Schedule

ПОЛЕ	ОПИСАНИЕ
One Time	
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным расписанием.
Name	Это поле показывает имя расписания, которое используется для ссылки на него.
Start Day / Time	Это поле показывает дату и время начала действия расписания.
Stop Day / Time	Это поле показывает дату и время окончания действия расписания.
Recurring	
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.

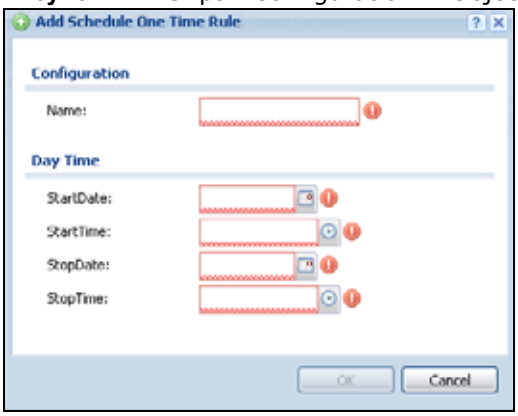
Таблица 132 Экран Configuration > Object > Schedule (продолжение)

ПОЛЕ	ОПИСАНИЕ
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным расписанием.
Name	Это поле показывает имя расписания, которое используется для ссылки на него.
Start Time	Это поле показывает время начала действия расписания.
Stop Time	Это поле показывает время окончания действия расписания.

23.2.1 Экран Add/Edit Schedule One-Time Rule

С помощью экрана **Add/Edit Schedule One-Time Rule** можно создать новые или отредактировать существующие однократные расписания. Чтобы открыть этот экран, перейдите к экрану **Schedule** и нажмите на пиктограмму **Add** или пиктограмму **Edit** в разделе **One Time**.

Рисунок 147 Экран Configuration > Object > Schedule > Add/Edit (One-Time)



Поля экрана описаны в следующей таблице.

Таблица 133 Экран Configuration > Object > Schedule > Add/Edit (One-Time)

ПОЛЕ	ОПИСАНИЕ
Configuration	
Name	Введите имя, которое будет использоваться для ссылки на это однократное расписание. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
Date Time	
StartDate	Укажите год, месяц и день даты начала действия расписания. **Year** (год): 1900-2999 **Month** (месяц): 1-12 **Day** (день): 1-31 (при этом указать несуществующие дни, например, 31 февраля, не получится)
StartTime	Укажите час и минуту времени начала действия расписания. **Hour** (час): 0-23 **Minute** (минута): 0-59

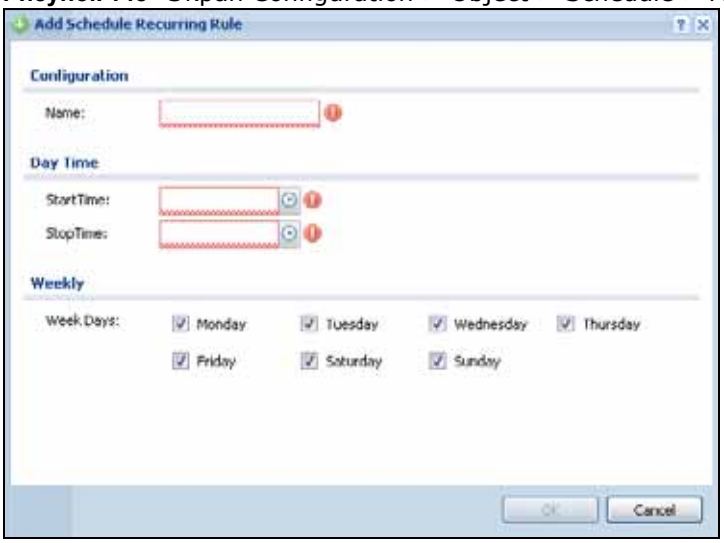
Таблица 133 Экран Configuration > Object > Schedule > Add/Edit (One-Time) (продолжение)

ПОЛЕ	ОПИСАНИЕ
StopDate	Укажите год, месяц и день даты окончания действия расписания. **Year** (год): 1900-2999 **Month** (месяц): 1-12 **Day** (день): 1-31 (при этом указать несуществующие дни, например, 31 февраля, не получится)
StopTime	Укажите час и минуту времени окончания действия расписания. **Hour** (час): 0-23 **Minute** (минута): 0-59
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

23.2.2 Экран Add/Edit Schedule Recurring Rule

С помощью экрана **Add/Edit Schedule Recurring Rule** можно создать новые или отредактировать существующие повторяющиеся расписания. Чтобы открыть этот экран, перейдите к экрану **Schedule** и нажмите на пиктограмму **Add** или на пиктограмму **Edit** в разделе **Recurring**.

Рисунок 148 Экран Configuration > Object > Schedule > Add/Edit (Recurring)



Столбцы **Year**, **Month** и **Day** для повторяющихся расписаний не используются и недоступны для редактирования на этом экране. В таблице ниже приведено описание остальных полей на этом экране.

Таблица 134 Экран Configuration > Object > Schedule > Add/Edit (Recurring)

ПОЛЕ	ОПИСАНИЕ
Configuration	
Name	Введите имя, которое будет использоваться для ссылки на это повторяющееся расписание. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.

Таблица 134 Экран Configuration > Object > Schedule > Add/Edit (Recurring) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Date Time	
StartTime	Укажите время начала ежедневного действия расписания в часах и минутах. **Hour** (час): 0-23 **Minute** (минута): 0-59
StopTime	Укажите время окончания ежедневного действия расписания в часах и минутах. **Hour** (час): 0-23 **Minute** (минута): 0-59
Weekly	
Week Days	Выберите дни недели, по которым будет действовать это повторяющееся расписание.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

24

Сервер аутентификации, авторизации и учета (AAA)

24.1 Обзор

Для управления доступом к сети можно использовать сервер AAA (Authentication, Authorization, Accounting). В качестве сервера AAA может выступать сервер Active Directory, LDAP или RADIUS. Экраны **AAA Server** служат для создания объектов, содержащих настройки для работы с серверами AAA, и управления этими объектами. Объекты серверов AAA используют при настройке пользовательских объектов типа ext-group-user и объектов методов аутентификации.

24.1.1 О чем рассказывается в этой главе

- Экраны **Active Directory** / **LDAP** (разд. 24.2 на стр. 278) служат для настройки объектов серверов Active Directory и LDAP.
- Экран **RADIUS** (разд. 24.3 на стр. 283) позволяет настроить параметры внешнего сервера RADIUS по умолчанию, используемого для аутентификации пользователей.

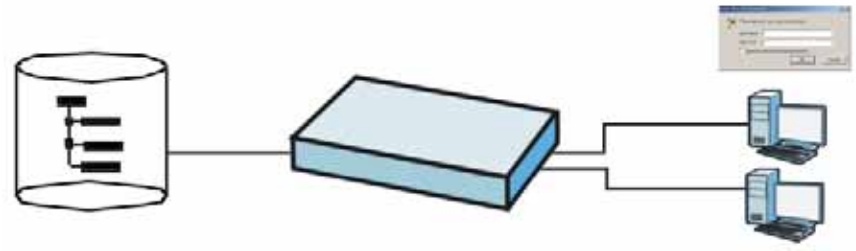
24.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Служба каталогов (AD/LDAP)

LDAP/AD позволяет клиенту (устройству NXC) подключаться к серверу для получения информации из каталога. Пример сетевой инфраструктуры показан ниже.

Рисунок 149 Пример: Клиент и сервер службы каталогов



Ниже описана процедура аутентификации пользователей с использованием сервера LDAP/AD.

1 Пользователь выполняет вход в систему, указав имя пользователя и пароль.

2 Устройство NXC пытается выполнить привязку (или вход) к серверу LDAP/AD.

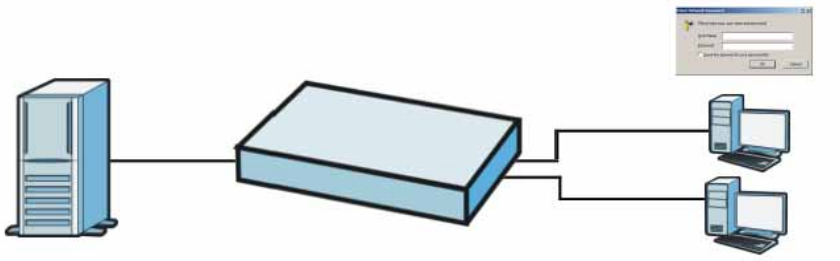
3 В случае успешной привязки устройство NXC ищет информацию о пользователе в каталоге сервера по сочетанию имени и пароля.

4 Если соответствие найдено, пользователю разрешается вход в систему. В противном случае доступ блокируется.

Сервер RADIUS

Служба аутентификации RADIUS – это популярный протокол, который используется для аутентификации пользователей путем обращения к внешнему серверу вместо внутренней базы данных пользователей устройства, которая ограничена емкостью памяти этого устройства (внешний сервер может также использоваться в дополнение к внутренней базе данных). По сути, аутентификация RADIUS позволяет идентифицировать большое количество пользователей с помощью единой централизованной службы.

Рисунок 150 Пример сетевой инфраструктуры с использованием сервера RADIUS



Список методов аутентификации

Этот список содержит перечень методов аутентификации, которые может использовать устройство NXC:

Таблица 135 Список методов аутентификации

	МЕТОД ВНУТРЕННЕЙ АУТЕНТИФИКАЦИИ			ВНЕШНЯЯ АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ СЕРВЕРА RADIUS
	AD	LDAP	RADIUS	
EAP-TLS	O	O	O	O
EAP-TTLS (Mschapv2/Mschap)	O[A]	O	O	O
EAP-TTLS (eap)	X	X	X	O
EAP-TTLS (pap)	O	O	O	O
EAP-PEAP (Mschapv2)	O[A]	O	O	O
EAP-PEAP (TLS)	X	X	X	O
EAP-MD5	X	X	X	O

A. Необходимо включить доменную аутентификацию.

Серверы AAA, поддерживаемые устройством NXC

Ниже приведены типы серверов аутентификации, которые поддерживает устройство NXC.

- Локальная база данных пользователей

  Устройство NXC использует встроенную локальную базу данных пользователей для аутентификации администраторов, осуществляющих вход на устройство NXC через Web-конфигуратор, или обычных пользователей, выполняющих вход в сеть через устройство NXC.

- Служба каталогов (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) – это служба каталогов, которая представляет собой одновременно и каталог, и протокол для управления доступом к сети. Каталог содержит базу данных, специально адаптированную для быстрого поиска и фильтрации информации. Можно создавать и хранить профили пользователей и учетные данные для входа на внешнем сервере.

- RADIUS

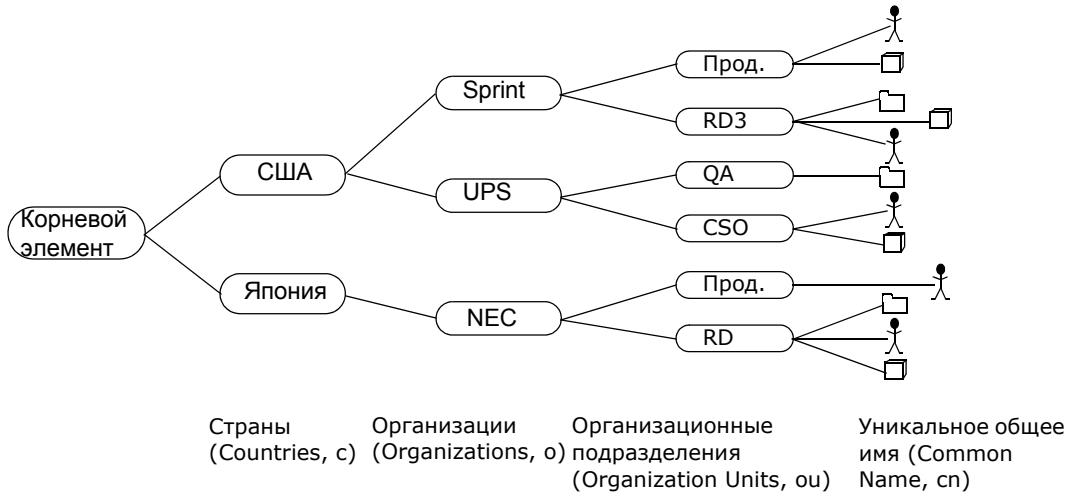
  RADIUS (Remote Authentication Dial-In User Service) – это популярный протокол, используемый для аутентификации пользователей посредством внешнего или встроенного сервера RADIUS. Аутентификация RADIUS позволяет идентифицировать большое количество пользователей с помощью единой централизованной службы.

Примечание: У устройства NXC имеется внутренняя база данных для аутентификации, которая позволяет создавать локальные учетные записи, не рассчитывая на внешний сервер для аутентификации. Встроенный сервер аутентификации поддерживает протоколы PEAP/EAP-TLS/EAP-TTLS.

Структура каталогов

Записи в каталоге хранятся в иерархическом порядке, весьма напоминающем древовидную структуру. Как правило, структура каталога отражает географическую или организационную структуру компании. На рисунке ниже приведен пример простой древовидной структуры каталога, включающей в себя страны, организации, структурные подразделения и сотрудников.

Рисунок 151 Простая структура каталога



Отличительное имя (Distinguished Name, DN)

Имя DN уникальным образом идентифицирует запись в пределах каталога. Имя DN состоит из пар «атрибут-значение», разделенных запятыми. Крайний слева атрибут называется относительным отличительным именем (Relative Distinguished Name, RDN). Этот атрибут содержит уникальное имя для записей с совпадающим «родительским DN» («`cn=domain1.com`, `ou=Sales, o=MyCompany`» в примерах ниже).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Базовое отличительное имя (Base DN)

Базовое отличительное имя описывает каталог. Базовое отличительное имя обычно содержит такие сведения, как название организации, доменное имя и/или название страны. Например, `o=MyCompany`, `c=UK`, где `o` означает «организация», а `c` – «страна».

Отличительное имя привязки (Bind DN)

Отличительное имя привязки используется для аутентификации с использованием сервера LDAP/AD. Например, отличительное имя привязки `cn=zyAdmin` позволяет устройству NXC выполнить вход на сервер LDAP/AD с использованием имени `zyAdmin`. Отличительное имя привязки используют в сочетании с паролем привязки. Если отличительное имя привязки не задано, устройство NXC попробует выполнить вход под именем анонимного пользователя. Если пароль привязки указан неверно, выполнить вход на сервер получится.

24.2 Экраны Active Directory / LDAP

С помощью экрана **Active Directory** или **LDAP** можно управлять списком серверов AD или LDAP, которые устройство NXC может использовать при аутентификации пользователей.

Примечание: Оба экрана, Active Directory и LDAP, имеют идентичный вид, невзирая на то, что они расположены на разных вкладках. Описание, приведенное в этом разделе, применимо к обоим экранам.

Выберите в меню **Configuration > Object > AAA Server > Active Directory/LDAP**, чтобы открыть экран **Active Directory** / **LDAP**.

Рисунок 152 Экран Configuration > Object > AAA Server > Active Directory/LDAP

Поля экрана описаны в следующей таблице.

Таблица 136 Экран Configuration > Object > AAA Server > Active Directory/LDAP

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле отображается порядковый номер.
Name	Здесь отображается имя, которое было указано для идентификации сервера.
Server Address	Это поле содержит адрес сервера AD или LDAP.
Base DN	Это поле указывает каталог. Например, `o=ZyXEL, c=US`.

24.2.1 Экраны Add/Edit Active Directory / LDAP Server

Выберите в меню **Object > AAA Server > Active Directory/LDAP**, чтобы открыть экран **Active Directory** (или **LDAP**). Нажмите на пиктограмму **Add** или пиктограмму **Edit**, чтобы открыть следующий экран. С помощью этого экрана можно создать новую запись или отредактировать существующую.

Примечание: Экраны настроек для серверов Active Directory и LDAP практически идентичны, соответственно, в этом разделе описаны поля и функции, присутствующие на обоих экранах.

Рисунок 153 Экран Configuration > Object > AAA Server > Active Directory > Add/Edit

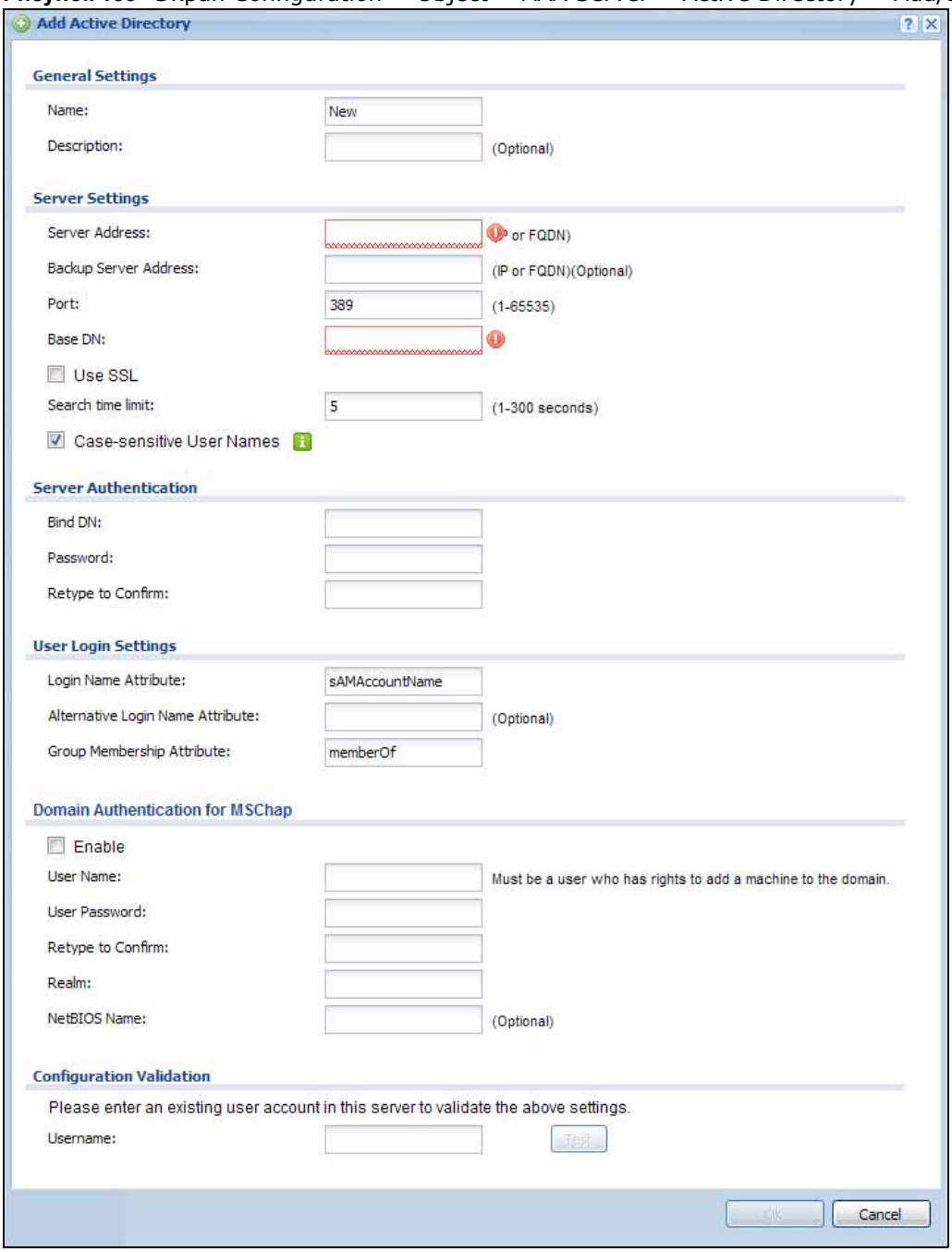
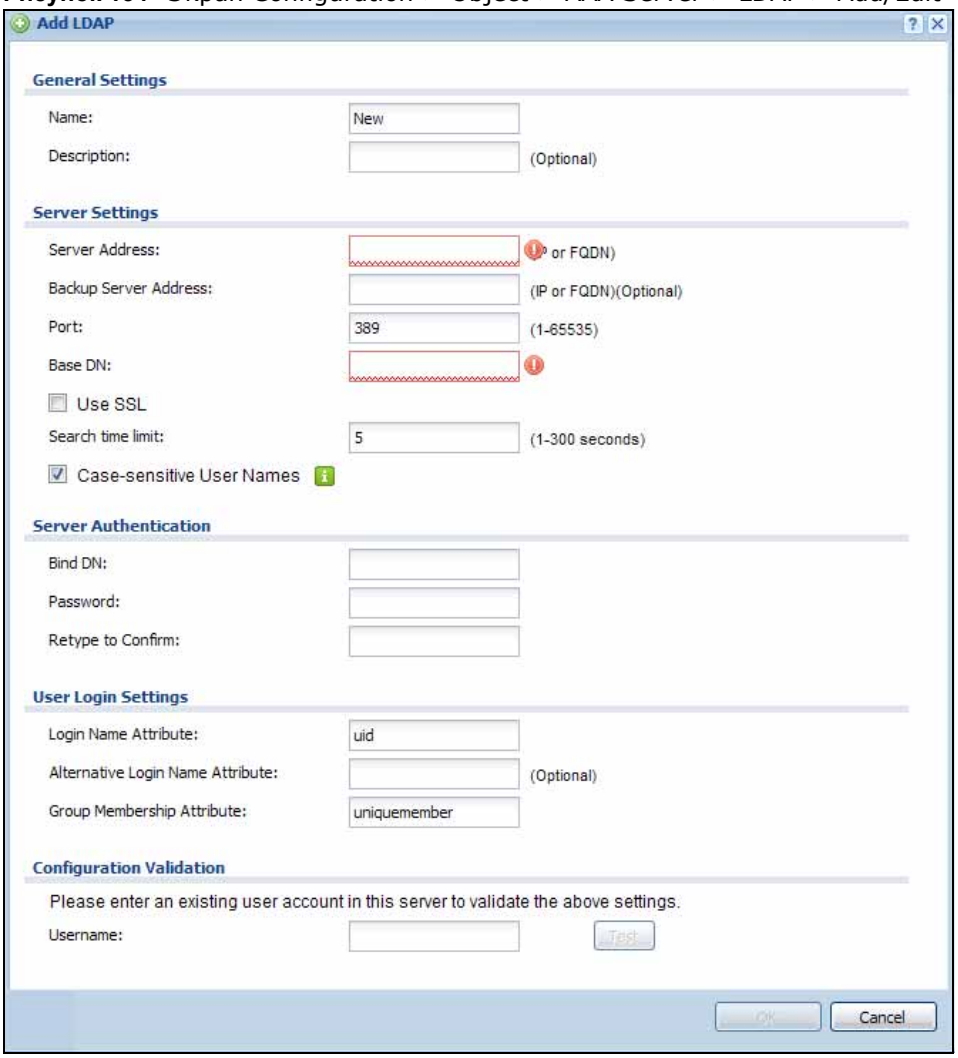


Рисунок 154 Экран Configuration > Object > AAA Server > LDAP > Add/Edit



Поля этих экранов описаны в следующей таблице.

Таблица 137 Экран Configuration > Object > AAA Server > Active Directory (или LDAP) > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя-описание (до 63 алфавитно-цифровых символов) для идентификации.
Description	Введите описание для каждого из серверов, если требуется. В поле можно ввести до 60 печатных символов ASCII.
Server Address	Введите адрес сервера AD или LDAP.
Backup Server Address	Если у сервера AD или LDAP есть резервный сервер, укажите в этом поле его адрес.
Port	Укажите номер порта на сервере AD или LDAP, на который устройство NXC отправляет запросы на аутентификацию. Введите значение в диапазоне от 1 до 65535. Указанный номер порта должен быть одинаковым на всех серверах AD или LDAP в этой группе.
Base DN	Укажите каталог (не более 127 алфавитно-цифровых символов). Например, `o=ZyXEL, c=US`.

Таблица 137 Экран Configuration > Object > AAA Server > Active Directory (или LDAP) > Add/ Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Use SSL	Выберите опцию **Use SSL**, если необходимо установить защищенное соединение с сервером (или серверами) AD или LDAP.
Search time limit	Укажите интервал тайм-аута (значение в диапазоне от 1 до 300 секунд), по истечении которого устройство NXC отключается от сервера AD. В этом случае пользователь не может пройти аутентификацию. Тайм-аут поиска может произойти либо если информация о пользователе отсутствует на сервере AD или LDAP, либо если сервер AD или LDAP недоступен.
Case-sensitive User Names	Выберите эту опцию, чтобы сервер учитывал регистр имен пользователей.
Bind DN	Укажите отличительное имя привязки (bind DN) для входа на сервер AD или LDAP. Имя должно состоять не более чем из 127 алфавитно-цифровых символов. Например, значение `cn=zyAdmin` задает имя пользователя `zyAdmin`.
Password	Если требуется, введите пароль (не более 15 алфавитно-цифровых символов), необходимый для привязки (или входа) устройства NXC на сервер AD или LDAP.
Retype to Confirm	Введите еще раз новый пароль для подтверждения.
Login Name Attribute	Укажите тип идентификатора, который пользователи должны использовать для входа. Например, «name» («имя») или «e-mail address» («адрес электронной почты»).
Alternative Login Name Attribute	Если имеется второй тип идентификатора, который пользователи могут использовать для входа, укажите его в этом поле. Например, «name» («имя») или «e-mail address» («адрес электронной почты»).
Group Membership Attribute	Введите название атрибута, по которому устройство NXC должно определять принадлежность пользователя к той или иной группе. Значение этого атрибута называется идентификатором группы; оно определяет, к какой группе относится пользователь. Можно добавлять пользовательские объекты типа **ext-group-user** для идентификации групп по значению идентификатора группы. Например, может использоваться атрибут «memberOf» со значениями типа «sales» («Отдел продаж»), «RD» («Отдел НИОКР») и «management» («Руководство»). В этом случае можно создать пользовательский объект типа **ext-group-user** для каждой группы. Один – со значением идентификатора группы «sales», второй – со значением «RD» и третий – со значением «management».
Enable	Выберите эту опцию, если необходимо разрешить доменную аутентификацию для протокола MSChap. MS-CHAP Microsoft CHAP (Challenge Handshake Authentication Protocol) использует механизм «запрос-отклик», где отклик передается в зашифрованном виде. Примечание: Это поле используется только при аутентификации на сервере **Active Directory**.
User Name	Введите имя пользователя, который имеет права на добавление машины в домен. Примечание: Это поле используется только при аутентификации на сервере **Active Directory**.
User Password	Введите пароль для указанного имени пользователя. Примечание: Это поле используется только при аутентификации на сервере **Active Directory**.
Retype to Confirm	Введите еще раз новый пароль для подтверждения.

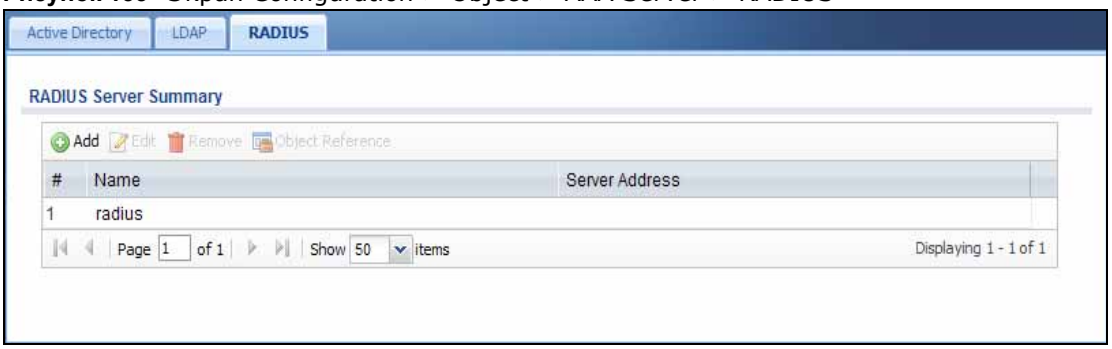
Таблица 137 Экран Configuration > Object > AAA Server > Active Directory (или LDAP) > Add/ Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Realm	Укажите ареал (realm) сервера AD (сетевой домен). Примечание: Это поле используется только при аутентификации на сервере **Active Directory**.
NetBIOS Name	Укажите имя NetBIOS для сервера AD или LDAP. Если указать имя NetBIOS, устройство NXC использует его в формате NetBIOS\USERNAME для выполнения аутентификации. Если не указывать имя NetBIOS, устройство NXC использует для аутентификации строку в формате USERNAME@realm.
Configuration Validation	Используйте учетную запись пользователя с сервера, указанного выше, для проверки правильности конфигурации. Введите имя учетной записи пользователя в поле **Username** и нажмите кнопку **Test**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения.
Cancel	Нажмите кнопку **Cancel**, чтобы отменить изменения.

24.3 Экран RADIUS

С помощью экрана **RADIUS** можно управлять списком серверов RADIUS, которые устройство NXC может использовать для аутентификации пользователей. Выберите в меню **Configuration > Object > AAA Server > RADIUS**, чтобы открыть экран **RADIUS**.

Рисунок 155 Экран Configuration > Object > AAA Server > RADIUS



Поля экрана описаны в следующей таблице.

Таблица 138 Экран Configuration > Object > AAA Server > RADIUS

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле отображается порядковый номер.

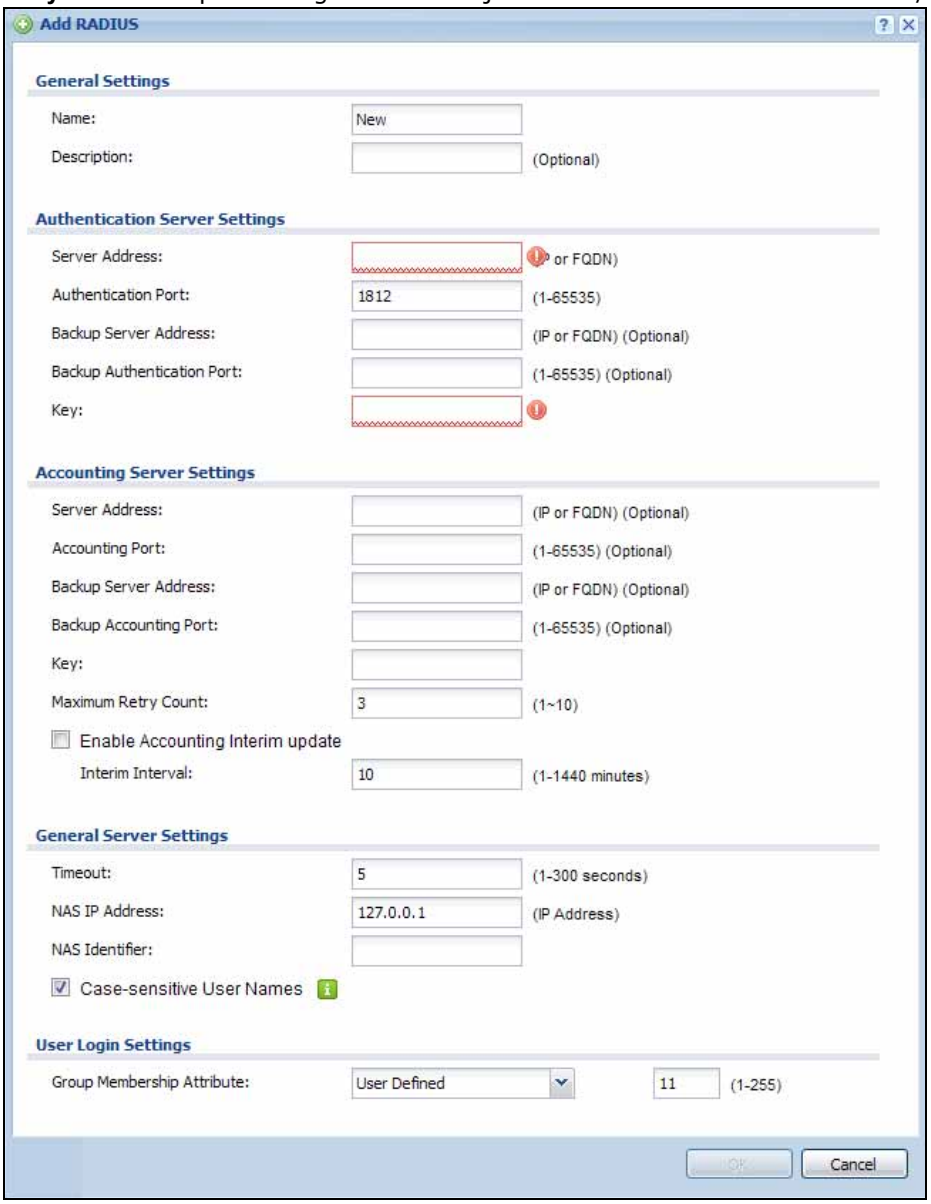
Таблица 138 Экран Configuration > Object > AAA Server > RADIUS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name	Это имя записи для сервера RADIUS.
Server Address	Это поле содержит адрес сервера AD или LDAP.

24.3.1 Экран Add/Edit RADIUS

Выберите в меню **Configuration > Object > AAA Server > RADIUS**, чтобы открыть экран **RADIUS**. Нажмите на пиктограмму **Add** или пиктограмму **Edit**, чтобы открыть следующий экран. С помощью этого экрана можно создать новую запись или отредактировать существующую.

Рисунок 156 Экран Configuration > Object > AAA Server > RADIUS > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 139 Экран Configuration > Object > AAA Server > RADIUS > Add/Edit

ПОЛЕ	ОПИСАНИЕ
General Settings	
Name	Введите имя-описание (до 63 алфавитно-цифровых символов) для идентификации.
Description	Введите описание для каждого из серверов, если требуется. В поле можно ввести до 60 печатных символов ASCII.
Authentication Server Settings	
Server Address	Введите адрес сервера аутентификации RADIUS.
Authentication Port	Укажите номер порта на сервере RADIUS, на который устройство NXC отправляет запросы на аутентификацию. Введите значение в диапазоне от 1 до 65535.
Backup Server Address	Если у данного сервера RADIUS есть резервный сервер аутентификации, укажите в этом поле его адрес.
Backup Authentication Port	Укажите номер порта на сервере RADIUS, на который устройство NXC отправляет запросы на аутентификацию. Введите значение в диапазоне от 1 до 65535.
Key	Введите пароль (до 15 алфавитно-цифровых символов) который будет служить общим ключом для внешнего сервера аутентификации и устройства NXC. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере аутентификации и устройстве NXC.
Accounting Server Settings	
Server Address	Введите IP-адрес или полное доменное имя (Fully-Qualified Domain Name, FQDN) сервера учета RADIUS.
Accounting Port	Укажите номер порта на сервере RADIUS, на который устройство NXC отправляет учетную информацию. Введите значение в диапазоне от 1 до 65535.
Backup Server Address	Если у данного сервера RADIUS есть резервный сервер учета, укажите в этом поле его адрес.
Backup Accounting Port	Укажите номер порта на сервере RADIUS, на который устройство NXC отправляет учетную информацию. Введите значение в диапазоне от 1 до 65535.
Key	Введите пароль (до 15 алфавитно-цифровых символов) который будет служить общим ключом для внешнего сервера аутентификации и устройства NXC. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере аутентификации и устройстве NXC.
Maximum Retry Count	В некоторых случаях устройство NXC не сможет установить связь с основным сервером учета RADIUS. Укажите, сколько попыток повторного подключения к основному серверу RADIUS должно совершить устройство NXC перед тем, как переключиться на резервный сервер RADIUS. Этот параметр определяет также, сколько попыток подключения к резервному серверу RADIUS должно совершить устройство NXC. Например, можно ввести в это поле значение 3. Если устройство NXC не получает ответа от основного сервера RADIUS, оно пробует установить связь с ним максимум три раза. Если отклика от сервера так и нет, устройство NXC пытается установить связь с резервным сервером RADIUS (тоже не более трех раз). Если все три попытки оказались неудачными, устройство NXC прекращает попытки аутентифицировать абонента. Абонент увидит сообщение, извещающее его о том, что сервер RADIUS не обнаружен.
Enable Accounting Interim update	Выберите эту опцию, чтобы устройство NXC периодически, через указанный интервал, посылало обновленные сведения о состоянии абонента серверу RADIUS.

Таблица 139 Экран Configuration > Object > AAA Server > RADIUS > Add/Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Interim Interval	Укажите интервал, через который устройство NXC должно отправлять обновленные сведения о состоянии абонента серверу RADIUS.
General Server Settings	
Timeout	Укажите интервал тайм-аута (значение в диапазоне от 1 до 300 секунд), по истечении которого устройство NXC отключается от сервера RADIUS. В этом случае пользователь не может пройти аутентификацию. Тайм-аут поиска может произойти либо если информация о пользователе отсутствует на сервере RADIUS, либо если сервер RADIUS недоступен.
NAS IP Address	Если сервер RADIUS требует от устройства NXC предоставить атрибут Network Access Server IP address (IP-адрес сервера сетевого доступа) с определенным значением, укажите его здесь.
NAS Identifier	Если сервер RADIUS требует от устройства NXC предоставить атрибут Network Access Server identifier (Идентификатор сервера сетевого доступа) с определенным значением, укажите его здесь.
Case-sensitive User Names	Выберите эту опцию, чтобы сервер учитывал регистр имен пользователей.
User Login Settings	
Group Membership Attribute	Сервер RADIUS описывает атрибуты для своих учетных записей. Выберите название и номер атрибута, по которому устройство NXC должно определять принадлежность пользователя к той или иной группе. Если название и номер атрибута не видны, выберите опцию **User Defined** и укажите номер атрибуты. Значение этого атрибута называется идентификатором группы; оно определяет, к какой группе относится пользователь. Можно добавлять пользовательские объекты типа **ext-group-user** для идентификации групп по значению идентификатора группы. Например, может использоваться атрибут «memberOf» со значениями типа «sales» («Отдел продаж»), «RD» («Отдел НИОКР») и «management» («Руководство»). В этом случае можно создать пользовательский объект типа **ext-group-user** для каждой группы. Один – со значением идентификатора группы «sales», второй – со значением «RD» и третий – со значением «management».
OK	Нажмите кнопку **OK**, чтобы сохранить изменения.
Cancel	Нажмите кнопку **Cancel**, чтобы отменить изменения.

25

Методы аутентификации

25.1 Обзор

Объекты методов аутентификации определяют, каким образом устройство NXC аутентифицирует беспроводных клиентов, клиентов HTTP/HTTPS и клиентов, заходящих через непокидаемый портал. В зависимости от настроек объектов методов аутентификации устройство NXC будет использовать локальную базу данных пользователей и/или серверы аутентификации и группы серверов аутентификации, указанные в объектах серверов AAA. По умолчанию, аутентификация пользователей, чьи учетные записи создаются и хранятся на устройстве NXC, осуществляется локально.

25.1.1 О чем рассказывается в этой главе

Экран **Auth. Method** (разд. 25.2 на стр. 287) служит для создания объектов методов аутентификации и управления ими.

25.1.2 Подготовительные действия

Перед созданием объектов методов аутентификации необходимо создать объекты серверов AAA.

25.2 Экран Authentication Method

Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > Auth. Method**.

Примечание: Всего можно создать не более 16 объектов методов аутентификации.

Рисунок 157 Экран Configuration > Object > Auth. Method

Поля экрана описаны в следующей таблице.

Таблица 140 Экран Configuration > Object > Auth. Method

ПОЛЕ	ОПИСАНИЕ
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле отображается порядковый номер.
Method Name	В этом поле отображается имя-описание для идентификации.
Method List	Это поле показывает метод (или методы) аутентификации для данной записи.

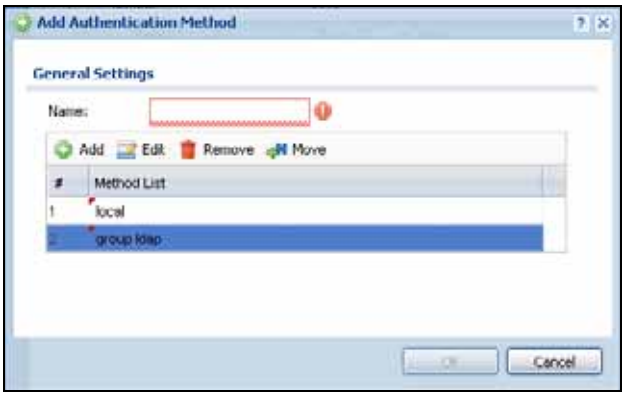
25.2.1 Экран Add Authentication Method

Чтобы создать объект метода аутентификации, проделайте следующее.

1. Выберите в меню **Configuration > Object > Auth. Method**.
2. Нажмите кнопку **Add**.
3. Укажите имя-описание в поле **Name** для идентификации. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру. Например, «My_Device».
4. Нажмите кнопку **Add**, чтобы вставить метод аутентификации в таблицу.
5. Выберите объект сервера в выпадающем списке **Method List**.
6. В таблицу можно добавить не более четырех объектов серверов. Порядок в столбце **Method List** имеет большое значение. Устройство NXC выполняет аутентификацию пользователей с использованием баз данных (локальной базы данных пользователей или внешнего сервера аутентификации) в том порядке, в каком они показаны на экране.

   Если две учетных записи с одним и тем же именем пользователя существуют на двух указанных серверах аутентификации, устройство NXC не будет выполнять поиск на втором сервере аутентификации, если было введено имя пользователя и пароль, которые не соответствуют имени пользователя и паролю для данной учетной записи на первом сервере аутентификации.

7 Нажмите кнопку **OK**, чтобы сохранить изменения, или кнопку **Cancel**, чтобы отменить все изменения и вернуться к предыдущему экрану.



Поля экрана описаны в следующей таблице.

Таблица 141 Экран Configuration > Object > Auth. Method > Add

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя-описание для идентификации. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру. Например, «My_Device».
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции.
Move	Чтобы изменить позицию метода в нумерованном списке, выберите этот метод и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести этот метод. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести метод на указанную позицию. Порядок расположения методов имеет большое значение, поскольку устройство NXC выполняет аутентификацию пользователей с использованием методов аутентификации в том порядке, в котором они показаны на экране.
#	В этом поле отображается порядковый номер.
Method List	Выберите объект сервера из выпадающего списка. Создать объект сервера можно на экране **AAA Server**. Устройство NXC выполняет аутентификацию пользователей с использованием баз данных (локальной базы данных пользователей или внешнего сервера аутентификации) в том порядке, в каком они показаны на экране. Если две учетных записи с одним и тем же именем пользователя существуют на двух указанных серверах аутентификации, устройство NXC не будет выполнять поиск на втором сервере аутентификации, если было введено имя пользователя и пароль, которые не соответствуют имени пользователя и паролю для данной учетной записи на первом сервере аутентификации.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения.
Cancel	Нажмите кнопку **Cancel**, чтобы отменить изменения.

26

Сертификаты

26.1 Обзор

Устройство NXC может использовать сертификаты (именуемые также цифровыми идентификаторами) для аутентификации пользователей. Основу механизма сертификатов составляют пары открытого и секретного ключей. Сертификат содержит идентификатор владельца сертификата и его открытый ключ. Сертификаты предлагают способ обмена открытыми ключами, который можно использовать для аутентификации.

26.1.1 О чем рассказывается в этой главе

- Экраны **My Certificate** (разд. 26.2 на стр. 293) служат для генерации и экспорта самоподписанных сертификатов или запросов на сертификаты и импорта на устройство NXC сертификатов, подписанных ЦС (CA, Certificate Authority, центр сертификации).
- Экраны **Trusted Certificates** (разд. 26.3 на стр. 302) позволяют сохранить сертификаты ЦС и сертификаты доверенных удаленных хостов на устройство NXC. Устройство NXC доверяет любому действующему сертификату, который был импортирован как доверенный сертификат. Кроме того, оно доверяет любому действующему сертификату, подписанному любым из сертификатов, который был импортирован как доверенный сертификат.

26.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Использование криптографии на основе открытых ключей для аутентификации предусматривает наличие у каждого хоста двух ключей. Одни ключ является открытым и может быть доступен всем. Другой ключ является секретным, и его надлежит хранить в безопасном месте.

В сочетании эти ключи действуют как подпись, поставленная вручную (фактически сертификаты часто называют «цифровыми подписями»). Только в вашем исполнении подпись может выглядеть так, как она должна выглядеть. Если люди знают, как выглядит подпись, они могут определить, был ли документ подписан вами или кем-то другим. Аналогичным образом, секретный ключ «ставит» вашу цифровую подпись, а открытый ключ дает людям возможность понять, были ли данные подписаны вами или кем-то другим.

Этот процесс работает следующим образом:

1 Тим хочет отправить сообщение Дженни. Он хочет, чтобы Дженни была уверена: письмо действительно пришло от Тима, и его содержание не было изменено по дороге кем-то другим. Тим генерирует пару с открытым ключом (один открытый ключ и один секретный ключ).

2 Тим сохраняет секретный ключ у себя, а открытый ключ делает общедоступным. Таким образом, каждый адресат сообщения, предположительно полученного от Тима, может прочитать его и удостовериться, действительно ли оно пришло от него, или нет.

3 Тим подписывает сообщение с помощью секретного ключа и отправляет его Дженни.

4 Дженни получает сообщение и использует открытый ключ Тима для его проверки. Дженни понимает, что сообщение действительно пришло от Тима, и, хотя кто-то мог прочесть его по дороге, содержимое сообщения точно осталось неизменным (поскольку злоумышленники не смогли бы заново подписать сообщение секретным ключом Тима).

5 В свою очередь, Дженни подписывает ответ Тиму с помощью своего секретного ключа, а Тим использует открытый ключ Дженни для проверки полученного ответа.

Устройство NXC использует сертификаты, основанные на криптографии с открытым ключом, для аутентификации пользователей, пытающихся установить соединение (а не для шифрования данных, отправляемых после установки соединения). Метод шифрования данных, отправляемых по установленному соединению, зависит от типа соединения.

Центр сертификации подписывает сертификаты с помощью собственного секретного ключа. После этого любой может использовать открытый ключ центра сертификации для проверки сертификатов.

Путь сертификации – это иерархия сертификатов центра сертификации, которая делает сертификат действующим. Устройство NXC не доверяет сертификату, если хотя бы один из сертификатов на его пути сертификации имеет истекший срок действия или был отозван.

Центры сертификации располагают серверами каталогов с базами данных, хранящими информацию о действующих и отозванных сертификатах. Каталог сертификатов, которые были отозваны до запланированного окончания срока действия, называют CRL (Certificate Revocation List, список отозванных сертификатов). Устройство NXC может проверить наличие сертификата, предоставленного партнером по соединению, в списке отозванных сертификатов сервера каталогов. Инфраструктура, включающая в себя серверы, программные средства, процедуры и политики для работы с ключами, называется инфраструктурой PKI (public-key infrastructure, инфраструктурой шифрования с открытым ключом).

Преимущества сертификатов

Сертификаты обладают следующими преимуществами.

- Устройство NXC должно хранить только сертификаты доверенных центров сертификации, независимо от того, сколько устройств приходится аутентифицировать.
- Механизм распространения ключей прост и исключительно безопасен, поскольку имеется возможность свободно распространять открытые ключи, и при этом никогда не приходится передавать кому-либо секретные ключи.

Самоподписанные сертификаты

Устройство NXC может выступать в качестве центра сертификации и подписывать собственные сертификаты.

Заводской сертификат по умолчанию

При первом включении устройство NXC генерирует собственный уникальный самоподписанный сертификат. В графическом интерфейсе пользователя (GUI) этот сертификат упоминается как заводской сертификат по умолчанию.

Форматы файлов сертификатов

Система поддерживает импорт сертификатов, предоставленных исключительно в файлах следующих форматов:

- Двоичный X.509: Это рекомендация ITU-T, которая описывает форматы сертификатов X.509.
- X.509 с кодировкой PEM (Base-64): Этот формат почты с повышенной конфиденциальностью (Privacy Enhanced Mail) использует буквы в нижнем и верхнем регистрах и цифры для преобразования двоичного сертификата X.509 в печатную форму.
- Двоичный PKCS#7: Это стандарт, который определяет общий синтаксис данных (включая цифровые подписи), которые могут быть зашифрованы. Файл в формате PKCS #7 используют для передачи сертификата с открытым ключом. Секретный ключ в этот файл не включается. В настоящее время устройство NXC разрешает импорт файла PKS#7, который содержит один сертификат.
- PKCS#7 с шифрованием PEM (Base-64): Этот формат почты с повышенной конфиденциальностью (Privacy Enhanced Mail) использует буквы в нижнем и верхнем регистрах и цифры для преобразования двоичного сертификата PKCS#7 в печатную форму.
- Двоичный PKCS#12: Это формат для передачи сертификатов с открытым и секретным ключами. Секретный ключ в файле PKCS #12 содержится в конверте, защищенном паролем. Пароль к файлу не связан с открытым или секретным паролем к сертификату. Пароль создается при экспорте файла PKCS #12, и его необходимо будет указать для дешифровки содержимого при импорте файла на устройство NXC.

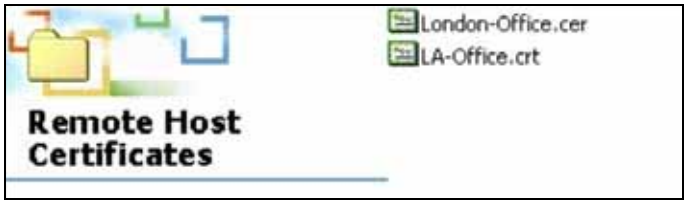
Примечание: Будьте внимательны, не преобразуйте случайно двоичный файл в текстовый в процессе передачи. Это легко может произойти, потому что многие программы по умолчанию используют текстовый формат файлов для передачи.

26.1.3 Проверка сертификата

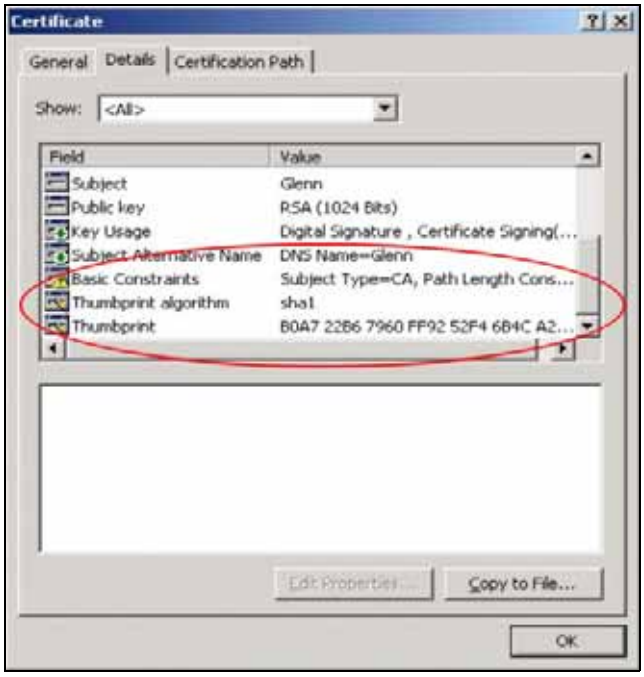
Перед тем, как импортировать доверенный сертификат на устройство NXC, необходимо убедиться, что этот сертификат – именно тот, что требуется. Это можно сделать с помощью отпечатка (fingerprint) сертификата. Отпечаток сертификата – это дайджест сообщения, рассчитанный с использованием алгоритма MD5 или SHA1. Приведенная ниже процедура описывает процесс проверки отпечатка сертификата для того, чтобы убедиться, что это действительно требуемый сертификат.

1 Откройте папку на компьютере, в которой хранится сертификат.

2 Убедитесь, что файл сертификата имеет расширение «.cer» или «.crt».



3 Дважды щелкните мышью на пиктограмме сертификата, чтобы открыть окно **Certificate**. Перейдите на вкладку **Details** и прокрутите содержимое окна вниз, до полей **Thumbprint Algorithm** и **Thumbprint**.

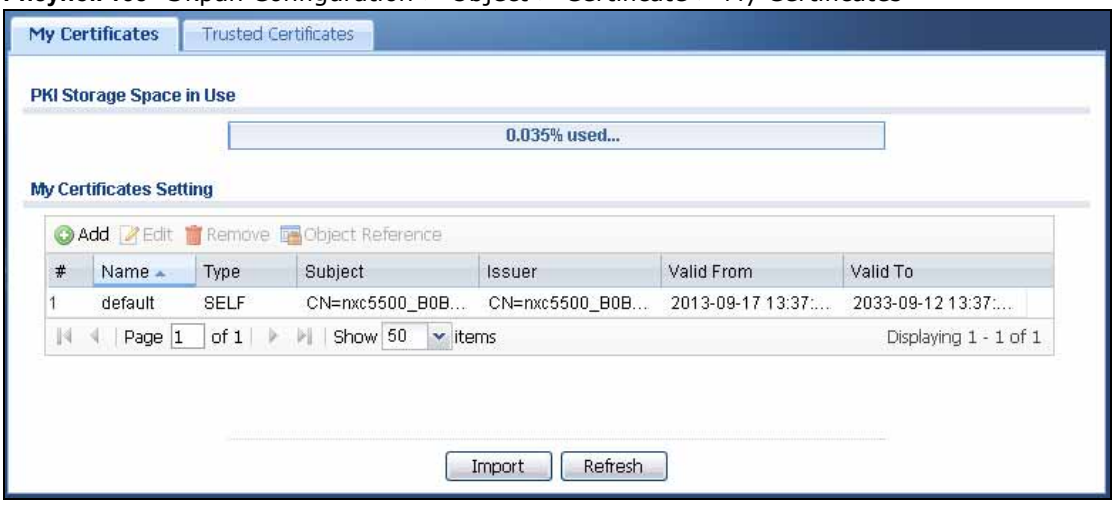


4 Используя защищенный метод, удостоверьтесь, что у владельца сертификата в полях **Thumbprint Algorithm** и **Thumbprint** содержится та же самая информация. Выбор защищенного метода может в значительной мере зависеть от ситуации. Очевидно, что безопасный метод проверки будет различаться, например, в случае телефонного разговора и соединения по протоколу HTTPS.

26.2 Экран My Certificates

Выберите в меню **Configuration > Object > Certificate > My Certificates**, чтобы открыть этот экран. На этом экране приведен сводный список сертификатов и запросов на сертификаты устройства NXC.

Рисунок 158 Экран Configuration > Object > Certificate > My Certificates



Поля экрана описаны в следующей таблице.

Таблица 142 Экран Configuration > Object > Certificate > My Certificates

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use	Эта полоса отображает задействованную на текущий момент долю (в процентах) пространства, отведенного устройством NXC для инфраструктуры PKI. Если отведенное пространство практически заполнено, то, возможно, следует удалить сертификаты с истекшим сроком действия или необязательные сертификаты перед добавлением новых сертификатов.
Add	Нажмите эту кнопку, чтобы перейти на экран генерации устройством NXC сертификата или запроса на сертификат.
Edit	Дважды щелкните по нужной записи мышью или выберите ее и нажмите кнопку **Edit**, чтобы открыть экран, содержащий подробную информацию о сертификате.
Remove	Устройство NXC хранит все сертификаты до тех пор, пока они не будут явным образом удалены. Выгрузка новой версии встроенного программного обеспечения или файла конфигурации по умолчанию не приводит к удалению сертификатов. Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. При выполнении этого действия все последующие сертификаты передвигаются в списке вверх на одну позицию.
Object Reference	Удалить сертификат невозможно, если он используется хотя бы одной из функций устройства NXC. Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	Это поле показывает порядковый номер сертификата в списке. Сертификаты в списке перечислены в алфавитном порядке.
Name	Это поле показывает имя, используемое для идентификации данного сертификата. Рекомендуется использовать для сертификатов уникальные имена.
Type	Это поле указывает на тип сертификата. **REQ** означает, что это запрос на сертификат, то есть данная сущность еще не является действующим сертификатом. Запрос на сертификат отправляют в центр сертификации, который затем выпускает сертификат. Для импорта сертификата и замены запроса настоящим сертификатом можно использовать экран **My Certificate Import**. **SELF** означает, что это самоподписанный сертификат. **CERT** означает, что это сертификат, выпущенный центром сертификации.

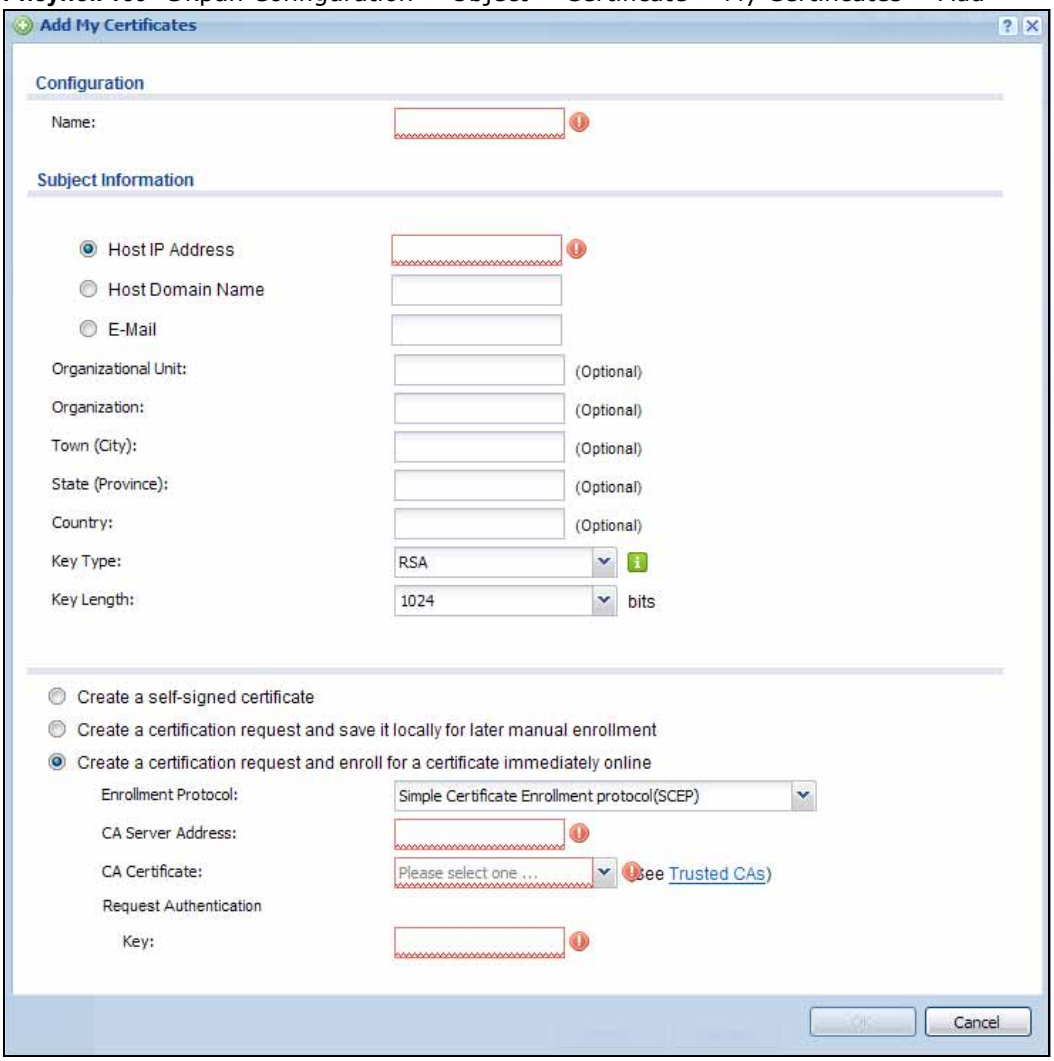
Таблица 142 Экран Configuration > Object > Certificate > My Certificates (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subject	Это поле показывает идентификационную информацию о владельце сертификата, в частности, CN (Common Name, общее имя), OU (Organizational Unit or department, структурное подразделение или отдел), O (Organization or company, организация или компания) и C (Country, страна). Рекомендуется использовать уникальное значение поля Subject для каждого сертификата.
Issuer	Это поле содержит идентификационную информацию о центре сертификации, выпустившем сертификат, в частности, сведения о его общем имени, структурном подразделении или отделе, организации или компании и стране. Для самоподписанных сертификатов эта информация совпадает с информацией в поле **Subject**.
Valid From	Это поле показывает дату, начиная с которой сертификат является действительным.
Valid To	Это поле показывает дату окончания срока действия сертификата. Текст в этом поле отображается в красном цвете и содержит сообщение Expired!, если срок действия сертификата уже истек.
Import	Нажмите кнопку **Import**, чтобы открыть экран, с помощью которого можно сохранить сертификат на устройстве NXC.
Refresh	Нажмите кнопку **Refresh**, чтобы отобразить текущее состояние действительности сертификатов.

26.2.1 Экран Add My Certificates

Выберите в меню **Configuration > Object > Certificate > My Certificates**, а затем нажмите на пиктограмму **Add**, чтобы открыть экран **My Certificates Add**. С помощью этого экрана можно создать на устройстве NXC самоподписанный сертификат, зарегистрировать сертификат, выпущенный центром сертификации, и сгенерировать запрос на сертификат.

Рисунок 159 Экран Configuration > Object > Certificate > My Certificates > Add



Поля экрана описаны в следующей таблице.

Таблица 143 Экран Configuration > Object > Certificate > My Certificates > Add

ПОЛЕ	ОПИСАНИЕ
Name	Укажите имя для идентификации этого сертификата. В имени можно использовать алфавитно-цифровые символы, а также символы ;`~!@#$%^&()_+[]{}',.=-. Длина имени не может составлять более 31 символа.
Subject Information	В эти поля заносится информация, которая идентифицирует владельца сертификата. Заполнять все поля необязательно, однако необходимо выбрать и заполнить одно из следующих полей: **Host IP Address**, **Host Domain Name** или **E-Mail**. Центр сертификации может добавлять поля (например, серийный номер) в раздел Subject Information при выпуске сертификата. Рекомендуется использовать уникальное значение поля Subject для каждого сертификата. Установите радиопереключатель, указывающий на способ идентификации владельца сертификата – по IP-адресу, доменному имени или адресу электронной почты. Укажите в соответствующем поле IP-адрес (в точечно-десятичной нотации), доменное имя или адрес электронной почты. Доменное имя или адрес электронной почты служат только для целей идентификации, поэтому значением этих полей может быть любая строка. Длина доменного имени не может превышать 255 символов. В имени можно использовать алфавитно-цифровые символы, символы дефиса и точки. Длина адреса электронной почты не может превышать 63 символов. В адресе можно использовать алфавитно-цифровые символы, символы дефиса, @, точки и подчеркивания.
Organizational Unit	Укажите структурное подразделение или отдел, к которому принадлежит владелец сертификата. Длина значения не может превышать 31 символ. В этом поле можно использовать алфавитно-цифровые символы, символы дефиса и подчеркивания.
Organization	Укажите компанию или группу, к которой принадлежит владелец сертификата. Длина значения не может превышать 31 символ. В этом поле можно использовать алфавитно-цифровые символы, символы дефиса и подчеркивания.
Town (City)	Укажите город или населенный пункт, в котором находится владелец сертификата. Длина значения не может превышать 31 символ. В этом поле можно использовать алфавитно-цифровые символы, символы дефиса и подчеркивания.
State (Province)	Укажите регион, в котором находится владелец сертификата. Длина значения не может превышать 31 символ. В этом поле можно использовать алфавитно-цифровые символы, символы дефиса и подчеркивания.
Country	Укажите страну, в которой находится владелец сертификата. Длина значения не может превышать 31 символ. В этом поле можно использовать алфавитно-цифровые символы, символы дефиса и подчеркивания.
Key Type	Выберите опцию **RSA**, если необходимо использовать алгоритм Ривеста-Шамира-Эдльмана (Rivest, Shamir, Adleman) на основе открытого ключа. Выберите опцию **DSA**, если необходимо использовать алгоритм цифровой подписи (Digital Signature Algorithm) на основе открытого ключа.
Key Length	Выберите из выпадающего списка разрядность ключа. Чем длиннее ключ, тем более безопасным он является. Более длинный ключ занимает больше места в хранилище PKI.
	Эти радиопереключатели определяют, каким образом и когда происходит генерация сертификата.
Create a self-signed certificate	Выберите эту опцию, чтобы устройство NXC сгенерировало сертификат и само выступило в качестве центра сертификации (ЦС). В этом случае не нужно будет подавать запросы на получение сертификата в другие центры сертификации.

Таблица 143 Экран Configuration > Object > Certificate > My Certificates > Add (продолжение)

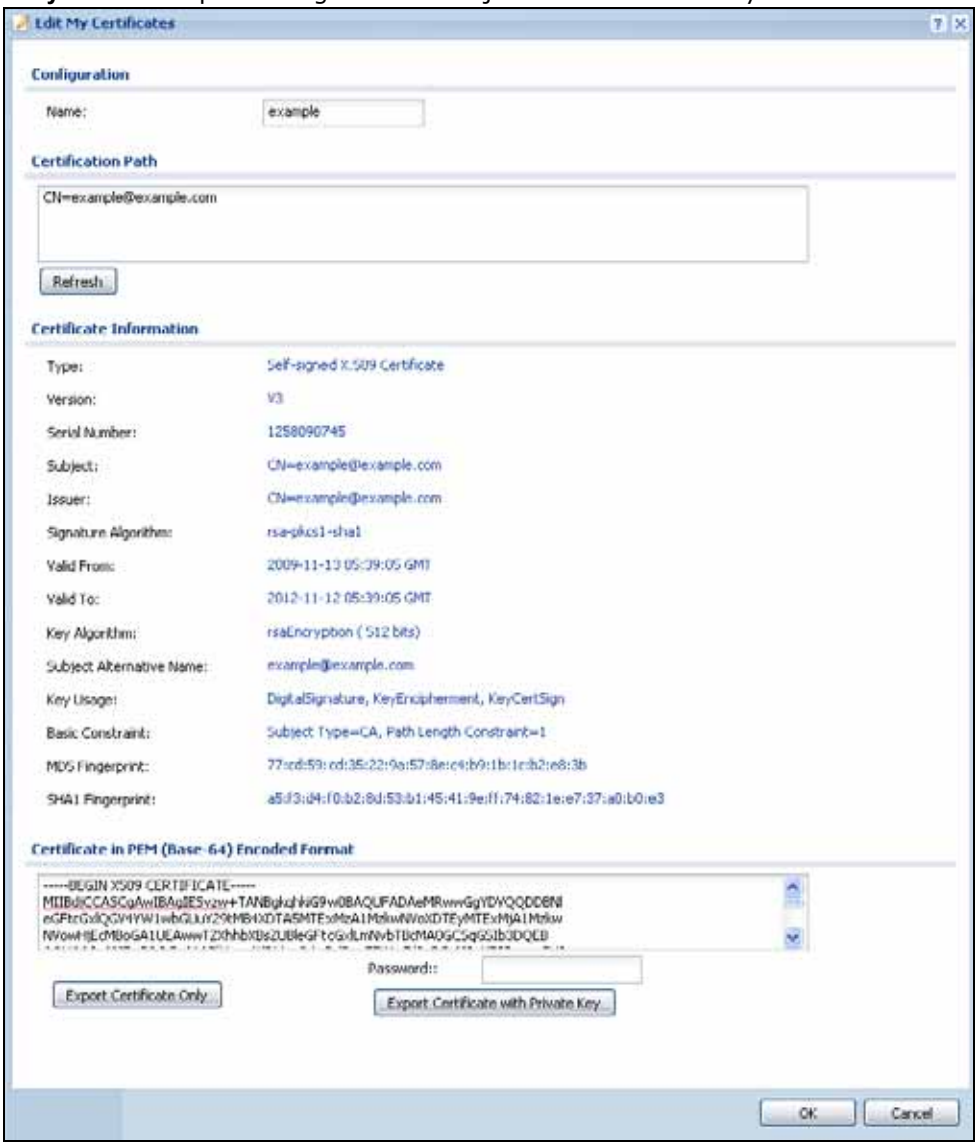
ПОЛЕ	ОПИСАНИЕ
Create a certification request and save it locally for later manual enrollment	Выберите эту опцию, чтобы устройство NXC сгенерировало и сохранило запрос на локальном уровне для последующей регистрации сертификата вручную. Для просмотра сертификационного запроса и его копирования для отправки в центр сертификации можно воспользоваться экраном **My Certificate Details**. Скопируйте сертификационный запрос на экране **My Certificate Details** и отправьте его в центр сертификации.
Create a certification request and enroll for a certificate immediately online	Выберите эту опцию, чтобы устройство NXC сгенерировало запрос на сертификат и сразу же отправило этот запрос в центр сертификации. К этому моменту сертификат этого центра сертификации должен быть уже импортирован в систему с помощью экрана **Trusted Certificates**. При выборе этой опции потребуется также выбрать протокол регистрации сертификата и сертификат центра сертификации из выпадающих списков и ввести адрес сервера центра сертификации. Если центр сертификации этого требует, вам, возможно, понадобится заполнить поля **Reference Number** и **Key**.
Enrollment Protocol	Это поле используется, если выбрана опция **Create a certification request and enroll for a certificate immediately online**. Выберите протокол регистрации центра сертификации из выпадающего списка. **Simple Certificate Enrollment Protocol (SCEP)** – это протокол регистрации на основе протокола TCP, который был разработан компаниями VeriSign и Cisco. **Certificate Management Protocol (CMP)** – это протокол регистрации на основе протокола TCP, который был разработан рабочей группой по развитию инфраструктуры шифрования с открытым ключом X.509 группы по проблемам проектирования Интернета (Internet Engineering Task Force, IETF) и описан в документе RFC 2510.
CA Server Address	Это поле используется, если выбрана опция **Create a certification request and enroll for a certificate immediately online**. Укажите IP-адрес (или адрес) сервера центра сертификации. Длина адреса не может превышать 511 символов; при написании адреса можно использовать следующие символы: a-zA-Z0-9'()+,/:.=?;!*#@$_%-
CA Certificate	Это поле используется, если выбрана опция **Create a certification request and enroll for a certificate immediately online**. Выберите сертификат центра сертификации из выпадающего списка **CA Certificate**. К этому моменту сертификат этого центра сертификации должен быть уже импортирован в систему с помощью экрана **Trusted Certificates**. Нажмите кнопку **Trusted CAs**, чтобы перейти на экран **Trusted Certificates**, где можно просмотреть список сертификатов, полученных устройством NXC от доверенных центров сертификации, и проделать с ними различные манипуляции.
Request Authentication	При выборе опции **Create a certification request and enroll for a certificate immediately online** центр сертификации, возможно, потребует указать ссылочный номер и ключ, чтобы идентифицировать отправителя сертификационного запроса. Заполните оба поля – **Reference Number** и **Key** – если центр сертификации использует протокол регистрации CMP. Если центр сертификации использует протокол регистрации SCEP, на экране будет видно только поле **Key**. В качестве ссылочного номера выбирается число в диапазоне от 0 до 99999999. Длина ключа не может превышать 31 символ; при заполнении этого поля можно использовать следующие символы: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
OK	Нажмите кнопку **OK**, чтобы начать генерацию сертификата или сертификационного запроса.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран и вернуться на экран **My Certificates**.

Если на экране **My Certificate Create** выбрана опция, в соответствии с которой устройство NXC должно зарегистрировать сертификат, и выполнить регистрацию не удалось, появится экран с кнопкой **Return**, нажатие которой позволяет вернуться на экран **My Certificate Create**. Нажмите кнопку **Return** и еще раз проверьте информацию на экране **My Certificate Create**. Убедитесь, что сведения о центре сертификации введены правильно, и что Интернет-соединение работает нормально, чтобы устройство NXC выполнило регистрацию сертификата в режиме онлайн.

26.2.2 Экран Edit My Certificates

Выберите в меню **Configuration > Object > Certificate > My Certificates**, а затем нажмите на пиктограмму **Edit**, чтобы открыть экран **My Certificate Edit**. На этом экране можно просмотреть подробную информацию о сертификатах и изменить имена сертификатов.

Рисунок 160 Экран Configuration > Object > Certificate > My Certificates > Edit



Поля экрана описаны в следующей таблице.

Таблица 144 Экран Configuration > Object > Certificate > My Certificates > Edit

ПОЛЕ	ОПИСАНИЕ
Name	Это поле отображает имя, идентифицирующее данный сертификат. В имени можно использовать алфавитно-цифровые символы, а также символы ;'~!@#$%^&()_+[]{}',.=-. Длина имени не может составлять более 31 символа.
Certification Path	Это поле отображается только для сертификата (для запроса на сертификат оно не видно). Нажмите кнопку **Refresh**, если необходимо отобразить в этом поле, доступном только для чтения, иерархию центров сертификации, которые делают этот сертификат действующим (включая и сам сертификат). Если выпускающий центр сертификации был импортирован как доверенный, то он может быть единственным центром сертификации в списке (вместе с самим сертификатом). Если сертификат является самоподписанным, то единственным элементом в списке является сам сертификат. Устройство NXC не доверяет сертификату и отображает в этом поле сообщение «Not trusted», если хотя бы один из сертификатов на его пути сертификации имеет истекший срок действия или был отозван.
Refresh	Нажмите кнопку **Refresh**, чтобы отобразить путь сертификации.
Certificate Information	Эти поля, доступные только для чтения, отображают подробную информацию о данном сертификате.
Type	Это поле отображает общую информацию о сертификате. CA-signed означает, что данный сертификат подписан центром сертификации. Self-signed означает, что данный сертификат подписан не центром сертификации, а владельцем сертификата. «X.509» означает, что это сертификат был создан и подписан в соответствии с рекомендацией ITU-T X.509, которая описывает форматы сертификатов на основе открытого ключа.
Version	Это поле показывает номер версии X.509 version number. "
Serial Number	Это поле показывает идентификационный номер сертификата, присвоенный сертификату центром сертификации или сгенерированный устройством NXC.
Subject	Это поле показывает информацию, которая идентифицирует владельца сертификата, в частности, такие сведения, как CN (Common Name, общее имя), OU (Organizational Unit or department, структурное подразделение или отдел), O (Organization or company, организация или компания), ST (State, регион) и C (Country, страна).
Issuer	Это поле содержит идентификационную информацию о центре сертификации, выпустившем сертификат, в частности, сведения о его общем имени, структурном подразделении, организации и стране. Для самоподписанных сертификатов эта информация совпадает с информацией в поле **Subject Name**. для сертификационного запроса отображается значение «none».
Signature Algorithm	Это поле отображает тип алгоритма, с помощью которого был подписан сертификат. Устройство NXC использует алгоритм rsa-pkcs1-sha1 (алгоритм шифрования RSA на основе открытого-секретного ключа и алгоритм хэширования SHA1). Некоторые центры сертификации могут использовать алгоритм rsa-pkcs1-md5 (алгоритм шифрования RSA на основе открытого-секретного ключа и алгоритм хэширования MD5).
Valid From	Это поле показывает дату, начиная с которой сертификат является действительным. для сертификационного запроса отображается значение «none».
Valid To	Это поле показывает дату окончания срока действия сертификата. Текст в этом поле отображается в красном цвете и содержит сообщение Expired!, если срок действия сертификата уже истек. для сертификационного запроса отображается значение «none».

Таблица 144 Экран Configuration > Object > Certificate > My Certificates > Edit

ПОЛЕ	ОПИСАНИЕ
Key Algorithm	Это поле отображает тип алгоритма, с помощью которого была сгенерирована пара ключей сертификата (устройство NXC использует шифрование по алгоритму RSA), а также длину набора ключей в битах (например, 1024 бита).
Subject Alternative Name	Это поле показывает IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.
Key Usage	Это поле показывает, для каких задач можно использовать ключ этого сертификата. Например, «DigitalSignature» означает, что ключ можно использовать для подписи сертификатов, а «KeyEncipherment» – для шифрования текста.
Basic Constraint	Это поле отображает общую информацию о сертификате. Например, «Subject Type=CA» означает, что это сертификат, выпущенный центром сертификации, а «Path Length Constraint=1» означает, что в пути сертификации для данного сертификата может быть только один центр сертификации. Для запроса на сертификат это поле не отображается на экране.
MD5 Fingerprint	Это дайджест сообщения сертификата, рассчитанный устройством NXC с использованием алгоритма MD5.
SHA1 Fingerprint	Это дайджест сообщения сертификата, рассчитанный устройством NXC с использованием алгоритма SHA1.
Certificate in PEM (Base-64) Encoded Format	Это поле, доступное только для чтения, отображает сертификат или запрос на сертификат в формате Privacy Enhanced Mail (PEM). Формат PEM использует буквы в нижнем и верхнем регистрах и цифры для преобразования двоичного сертификата в печатную форму.. Можно скопировать сертификационный запрос и вставить его в соответствующее поле на веб-странице центра сертификации, отправить его в центр сертификации по электронной почте или вставить его в текстовый редактор и сохранить в виде файла на компьютере администратора для последующей регистрации вручную. Можно скопировать сертификат, вставить его в тело сообщения и отправить по электронной почте друзьям или коллегам или вставить его в текстовый редактор и сохранить в виде файла на компьютере администратора для последующего распространения (например, на гибком диске).
Export	Эта кнопка отображается на экране в случае сертификационного запроса. С помощью этой кнопки можно сохранить копию запроса без секретного ключа. Нажмите эту кнопку и выберите опцию **Save** на экране **File Download**. Откроется экран **Save As**; выберите нужную папку и нажмите кнопку **Save**.
Export Certificate Only	С помощью этой кнопки можно сохранить копию сертификата без секретного ключа. Нажмите эту кнопку и выберите опцию **Save** на экране **File Download**. Откроется экран **Save As**; выберите нужную папку и нажмите кнопку **Save**.
Password	Если необходимо экспортировать сертификат с секретным ключом, придумайте пароль и введите его в этом поле. Позаботьтесь о том, чтобы сохранить пароль в надежном месте. Он понадобится при импорте сертификата на другое устройство.
Export Certificate with Private Key	Нажмите эту кнопку, чтобы сохранить копию сертификата вместе с секретным ключом. Введите пароль для сертификата и нажмите эту кнопку. Нажмите кнопку **Save** на экране **File Download**. Откроется экран **Save As**; выберите нужную папку и нажмите кнопку **Save**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации NXC. Допускается только изменение имени.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран и вернуться на экран **My Certificates**.

26.2.3 Импорт сертификатов

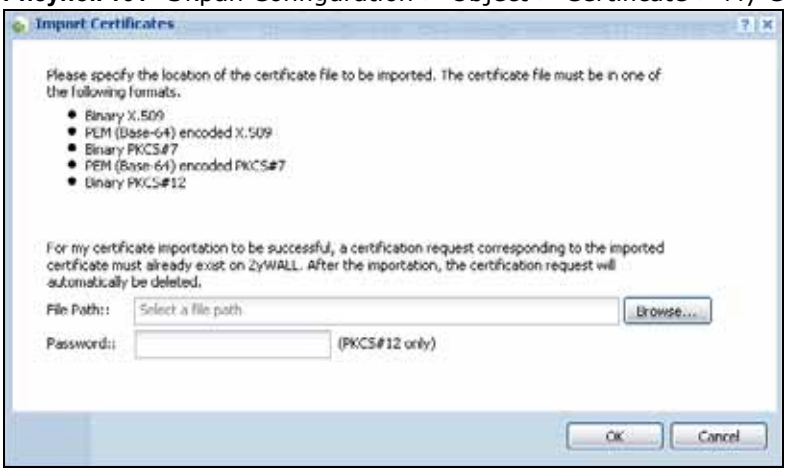
Выберите в меню **Configuration > Object > Certificate > My Certificates > Import**, чтобы открыть экран **My Certificate Import**. Следуя инструкциям на этом экране, сохраните существующий сертификат на устройстве NXC.

Примечание: Можно импортировать сертификат, который совпадает с соответствующим сертификационным запросом, сгенерированным устройством NXC. Можно также импортировать сертификат в формате PKCS#12, включающий в себя открытый и секретный ключи.

Импортируемый сертификат заменит соответствующий запрос на экране **My Certificates**.

Перед импортом необходимо удалить все пробелы в имени файла сертификата.

Рисунок 161 Экран Configuration > Object > Certificate > My Certificates > Import



Поля экрана описаны в следующей таблице.

Таблица 145 Экран Configuration > Object > Certificate > My Certificates > Import

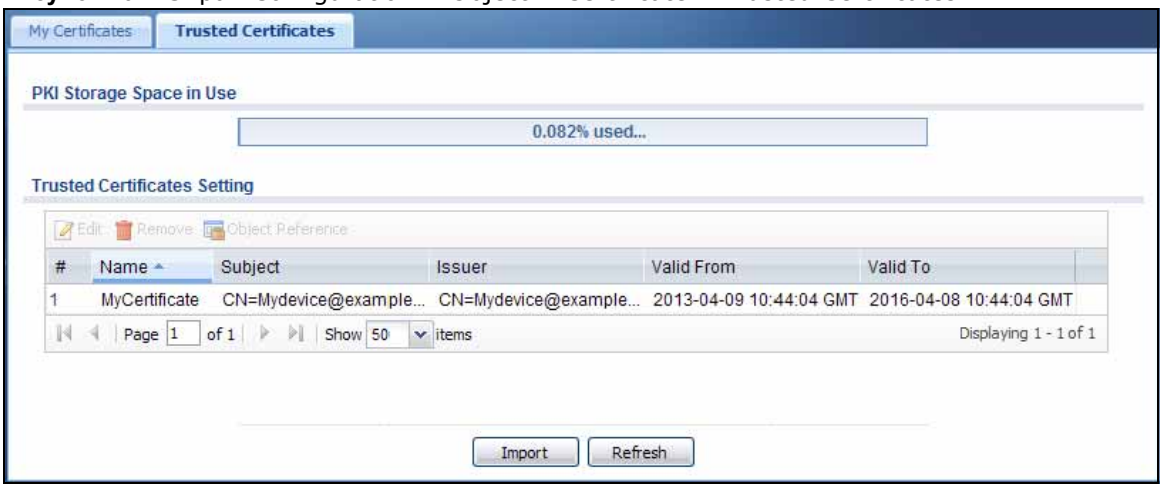
ПОЛЕ	ОПИСАНИЕ
File Path	Укажите в этом поле путь к файлу, который необходимо выгрузить, или нажмите кнопку **Browse**, чтобы найти его. Импортировать сертификат, чье имя совпадает с именем сертификата, уже имеющегося на устройстве NXC, нельзя.
Browse	Нажмите кнопку **Browse**, чтобы найти файл сертификата, который необходимо выгрузить.
Password	Это поле используется только при импорте файла в двоичном формате PKCS#12. Введите пароль к файлу, который был создан при экспорте файла PKCS #12.
OK	Нажмите кнопку **OK**, чтобы сохранить сертификат на устройстве NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран и вернуться на экран **My Certificates**.

26.3 Экран Trusted Certificates

Выберите в меню **Configuration > Object > Certificate > Trusted Certificates**, чтобы открыть экран **Trusted Certificates**. Этот экран содержит список сертификатов, которые были указаны на устройстве NXC как доверенные. Устройство NXC принимает любой действующий

сертификат, подписанный сертификатом из данного списка, как заслуживающий доверия; то есть не нужно импортировать сертификат, если он подписан одним из сертификатов, присутствующих в этом списке.

Рисунок 162 Экран Configuration > Object > Certificate > Trusted Certificates



Поля экрана описаны в следующей таблице.

Таблица 146 Экран Configuration > Object > Certificate > Trusted Certificates

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use	Эта полоса отображает задействованную на текущий момент долю (в процентах) пространства, отведенного устройством NXC для инфраструктуры PKI. Если отведенное пространство практически заполнено, то, возможно, следует удалить сертификаты с истекшим сроком действия или необязательные сертификаты перед добавлением новых сертификатов.
Edit	Дважды щелкните по нужной записи мышью или выберите ее и нажмите кнопку **Edit**, чтобы открыть экран, содержащий подробную информацию о сертификате.
Remove	Устройство NXC хранит все сертификаты до тех пор, пока они не будут явным образом удалены. Выгрузка новой версии встроенного программного обеспечения или файла конфигурации по умолчанию не приводит к удалению сертификатов. Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. При выполнении этого действия все последующие сертификаты передвигаются в списке вверх на одну позицию.
Object Reference	Удалить сертификат невозможно, если он используется хотя бы одной из функций устройства NXC. Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	Это поле показывает порядковый номер сертификата в списке. Сертификаты в списке перечислены в алфавитном порядке.
Name	Это поле показывает имя, используемое для идентификации данного сертификата.
Subject	Это поле показывает идентификационную информацию о владельце сертификата, в частности, CN (Common Name, общее имя), OU (Organizational Unit or department, структурное подразделение или отдел), O (Organization or company, организация или компания) и C (Country, страна). Рекомендуется использовать уникальное значение поля Subject для каждого сертификата.
Issuer	Это поле содержит идентификационную информацию о центре сертификации, выпустившем сертификат, в частности, сведения о его общем имени, структурном подразделении или отделе, организации или компании и стране. Для самоподписанных сертификатов эта информация совпадает с информацией в поле **Subject**.

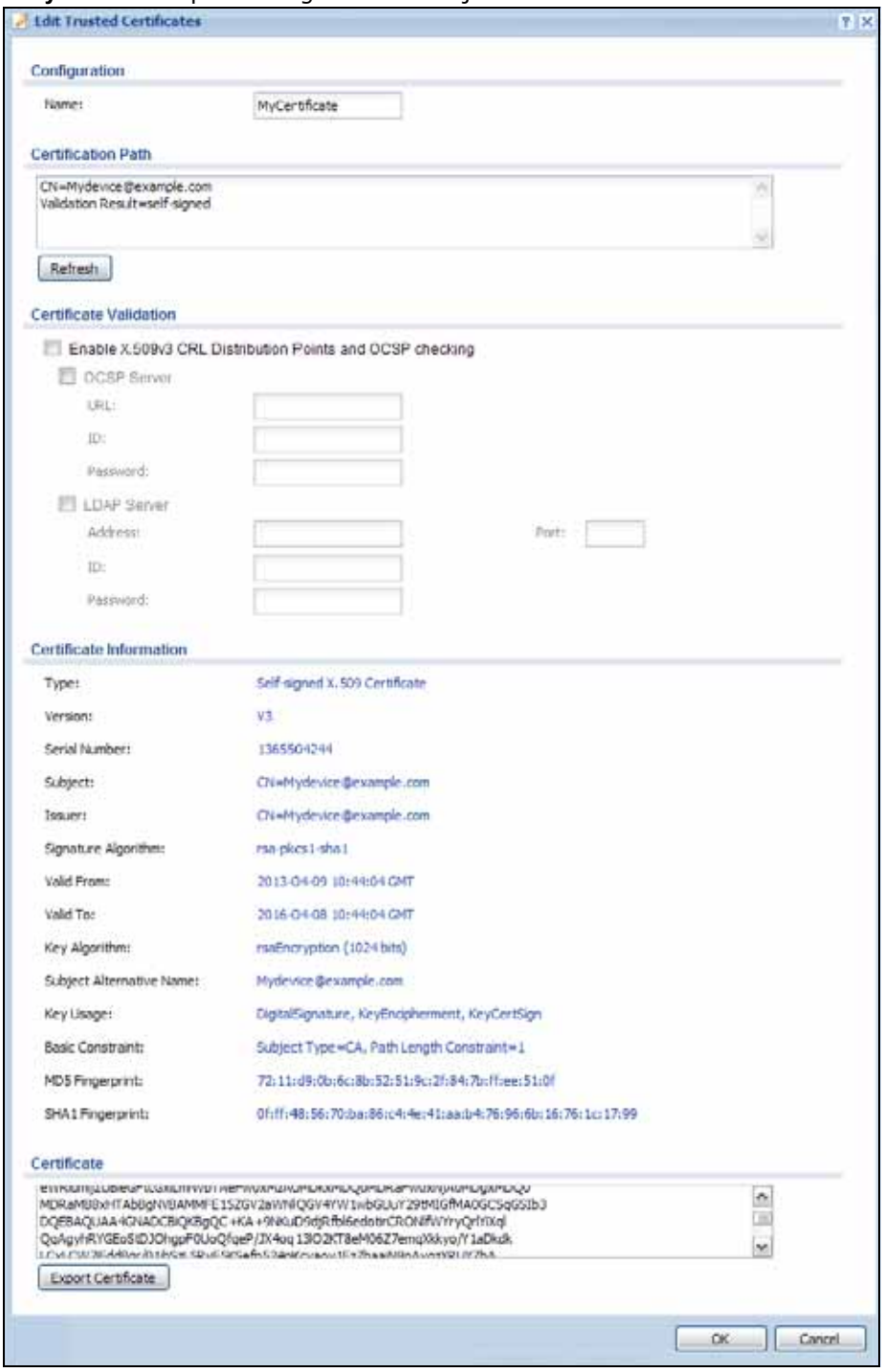
Таблица 146 Экран Configuration > Object > Certificate > Trusted Certificates (продолжение)

ПОЛЕ	ОПИСАНИЕ
Valid From	Это поле показывает дату, начиная с которой сертификат является действительным.
Valid To	Это поле показывает дату окончания срока действия сертификата. Текст в этом поле отображается в красном цвете и содержит сообщение Expired!, если срок действия сертификата уже истек.
Import	Нажмите кнопку **Import**, чтобы открыть экран, с помощью которого можно будет сохранить сертификат, выпущенный доверенным центром сертификации, со своего компьютера на устройство NXC.
Refresh	Нажмите эту кнопку, чтобы отобразить текущее состояние действительности сертификатов.

26.3.1 Экран Edit Trusted Certificates

Выберите в меню **Configuration > Object > Certificate > Trusted Certificates**, а затем нажмите на пиктограмму **Edit, чтобы открыть экран Trusted Certificates Edit**. С помощью этого экрана можно просмотреть подробную информацию о сертификате, изменить имя сертификата и указать, должно ли устройство NXC проверять список отозванных сертификатов данного центра сертификации прежде, чем доверять выпущенному им сертификату.

Рисунок 163 Экран Configuration > Object > Certificate > Trusted Certificates > Edit



Поля экрана описаны в следующей таблице.

Таблица 147 Экран Configuration > Object > Certificate > Trusted Certificates > Edit

ПОЛЕ	ОПИСАНИЕ
Name	Это поле отображает имя, идентифицирующее данный сертификат. Имя можно изменить. В имени можно использовать алфавитно-цифровые символы, а также символы ;`~!@#$%^&()_+[]{}',.=-. Длина имени не может составлять более 31 символа.
Certification Path	Нажмите кнопку **Refresh**, чтобы отобразить в этом поле, доступном только для чтения, сертификат конечной сущности и список сертификатов центров сертификации, показывающий всю иерархию центров сертификации, удостоверяющих сертификат конечной сущности. Если выпускающий центр сертификации был импортирован как доверенный, то он может быть единственным центром сертификации в списке (вместе с сертификатом конечной сущности). Устройство NXC не доверяет сертификату конечной сущности и отображает в этом поле сообщение «Not trusted», если хотя бы один из сертификатов на его пути сертификации имеет истекший срок действия или был отозван.
Refresh	Нажмите кнопку **Refresh**, чтобы отобразить путь сертификации.
Enable X.509v3 CRL Distribution Points and OCSP checking	Установите этот переключатель, чтобы устройство NXC проверяло наличие сертификатов, подписанных данным сертификатом, в списке отозванных сертификатов (Certificate Revocation List, CRL) или на сервере OCSP. Необходимо будет указать параметры сервера OSCP или LDAP.
OCSP Server	Установите этот переключатель, если соответствующий сервер каталогов использует протокол OCSP (Online Certificate Status Protocol, протокол определения состояния сертификата в режиме онлайн).
URL	Укажите протокол, IP-адрес и ссылку на сервер OCSP.
ID	Возможно, устройству NXC потребуется аутентифицировать себя для доступа к серверу OCSP. Введите имя пользователя (не более 31 ASCII-символа), предоставленное организацией, управляющей данным сервером (как правило, центром сертификации).
Password	Введите пароль (не более 31 ASCII-символа), предоставленный организацией, управляющей сервером OCSP (как правило, центром сертификации).
LDAP Server	Установите этот переключатель, если соответствующий сервер каталогов использует протокол LDAP (Lightweight Directory Access Protocol, облегченный протокол службы каталогов). LDAP – это протокол, который действует поверх протокола TCP и описывает процедуру доступа клиентов к каталогам сертификатов и спискам отозванных сертификатов.
Address	Укажите IP-адрес (в точечно-десятичной нотации) сервера каталогов.
Port	Укажите в этом поле номер порта сервера LDAP. Необходимо использовать тот же серверный порт, который использует сервер каталогов. 389 – это порт сервера по умолчанию для LDAP.
ID	Возможно, устройству NXC потребуется аутентифицировать себя для доступа к серверу каталогов CRL. Введите имя пользователя (не более 31 ASCII-символа), предоставленное организацией, управляющей данным сервером (как правило, центром сертификации).
Password	Введите пароль (не более 31 ASCII-символа), предоставленный организацией, управляющей сервером каталогов CRL (как правило, центром сертификации).
Certificate Information	Эти поля, доступные только для чтения, отображают подробную информацию о данном сертификате.
Type	Это поле отображает общую информацию о сертификате. CA-signed означает, что данный сертификат подписан центром сертификации. Self-signed означает, что данный сертификат подписан не центром сертификации, а владельцем сертификата. X.509 означает, что это сертификат был создан и подписан в соответствии с рекомендацией ITU-T X.509, которая описывает форматы сертификатов на основе открытого ключа.
Version	Это поле показывает номер версии X.509 version number.

Таблица 147 Экран Configuration > Object > Certificate > Trusted Certificates > Edit

ПОЛЕ	ОПИСАНИЕ
Serial Number	Это поле показывает идентификационный номер сертификата, присвоенный сертификату центром сертификации.
Subject	Это поле показывает информацию, которая идентифицирует владельца сертификата, в частности, такие сведения, как CN (Common Name, общее имя), OU (Organizational Unit or department, структурное подразделение или отдел), O (Organization or company, организация или компания) и C (Country, страна).
Issuer	Это поле содержит идентификационную информацию о центре сертификации, выпустившем сертификат, в частности, сведения о его общем имени, структурном подразделении, организации и стране. Для самоподписанных сертификатов эта информация совпадает с информацией в поле **Subject Name**.
Signature Algorithm	Это поле отображает тип алгоритма, с помощью которого был подписан сертификат. Некоторые центры сертификации используют алгоритм rsa-pkcs1-sha1 (алгоритм шифрования RSA на основе открытого-секретного ключа и алгоритм хэширования SHA1). Другие центры сертификации могут использовать алгоритм rsa-pkcs1-md5 (алгоритм шифрования RSA на основе открытого-секретного ключа и алгоритм хэширования MD5).
Valid From	Это поле показывает дату, начиная с которой сертификат является действительным. Текст в этом поле отображается в красном цвете и содержит сообщение Not Yet Valid!, если этот сертификат еще не стал действительным.
Valid To	Это поле показывает дату окончания срока действия сертификата. Текст в этом поле отображается в красном цвете и содержит сообщение Expiring! или Expired!, если срок действия этого сертификата близится к концу или уже истек.
Key Algorithm	Это поле отображает тип алгоритма, с помощью которого была сгенерирована пара ключей сертификата (устройство NXC использует шифрование по алгоритму RSA), а также длину набора ключей в битах (например, 1024 бита).
Subject Alternative Name	Это поле показывает IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.
Key Usage	Это поле показывает, для каких задач можно использовать ключ этого сертификата. Например, «DigitalSignature» означает, что ключ можно использовать для подписи сертификатов, а «KeyEncipherment» – для шифрования текста.
Basic Constraint	Это поле отображает общую информацию о сертификате. Например, «Subject Type=CA» означает, что это сертификат, выпущенный центром сертификации, а «Path Length Constraint=1» означает, что в пути сертификации для данного сертификата может быть только один центр сертификации.
MD5 Fingerprint	Это дайджест сообщения сертификата, рассчитанный устройством NXC с использованием алгоритма MD5. Его можно использовать для проверки, действительно ли данный сертификат выпущен этим центром сертификации (например, можно позвонить в центр сертификации и продиктовать им этот дайджест).
SHA1 Fingerprint	Это дайджест сообщения сертификата, рассчитанный устройством NXC с использованием алгоритма SHA1. Его можно использовать для проверки, действительно ли данный сертификат выпущен этим центром сертификации (например, можно позвонить в центр сертификации и продиктовать им этот дайджест).
Certificate in PEM (Base-64) Encoded Format	Это поле, доступное только для чтения, отображает сертификат или запрос на сертификат в формате Privacy Enhanced Mail (PEM). Формат PEM использует буквы в нижнем и верхнем регистрах и цифры для преобразования двоичного сертификата в печатную форму.. Можно скопировать сертификат, вставить его в тело сообщения и отправить по электронной почте друзьям или коллегам или вставить его в текстовый редактор и сохранить в виде файла на компьютере администратора для последующего распространения (например, на гибком диске).

Таблица 147 Экран Configuration > Object > Certificate > Trusted Certificates > Edit

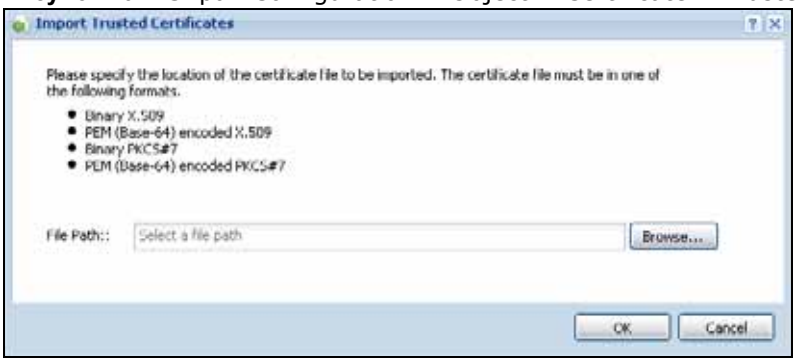
ПОЛЕ	ОПИСАНИЕ
Export Certificate	Нажмите эту кнопку и выберите опцию **Save** на экране **File Download**. Откроется экран **Save As**; выберите нужную папку и нажмите кнопку **Save**.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации NXC. Допускается только изменение имени.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран и вернуться на экран **Trusted Certificates**.

26.3.2 Экран Import Trusted Certificates

Выберите в меню **Configuration > Object > Certificate > Trusted Certificates > Import**, чтобы открыть экран **Trusted Certificates Import**. Следуя инструкциям на этом экране, сохраните доверенный сертификат на устройстве NXC.

Примечание: Перед импортом необходимо удалить все пробелы в имени файла сертификата.

Рисунок 164 Экран Configuration > Object > Certificate > Trusted Certificates > Import



Поля экрана описаны в следующей таблице.

Таблица 148 Экран Configuration > Object > Certificate > Trusted Certificates > Import

ПОЛЕ	ОПИСАНИЕ
File Path	Укажите в этом поле путь к файлу, который необходимо выгрузить, или нажмите кнопку **Browse**, чтобы найти его. Импортировать сертификат, чье имя совпадает с именем сертификата, уже имеющегося на устройстве NXC, нельзя.
Browse	Нажмите кнопку **Browse**, чтобы найти файл сертификата, который необходимо выгрузить.
OK	Нажмите кнопку **OK**, чтобы сохранить сертификат на устройстве NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран и вернуться к предыдущему.

26.4 Справочная техническая информация

В этом разделе содержится дополнительная техническая информация, относящаяся к функциям, описанным в этой главе.

OCSP

OCSP (Online Certificate Status Protocol, протокол проверки состояния сертификата в режиме онлайн) позволяет приложениям или устройствам проверять, является ли данный сертификат действительным. Используя протокол OCSP, устройство NXC проверяет состояние конкретного сертификата вместо загрузки всего списка отозванных сертификатов (Certificate Revocation List, CRL). OCSP имеет два важных преимущества по сравнению с CRL. Первое – это возможность проверить состояние сертификата в режиме онлайн. Второе – это снижение объемов сетевого трафика, поскольку устройство NXC получает информацию только о тех сертификатах, которые ему необходимо проверить, а не загружает весь огромный список. В ответ на запрос о состоянии сертификата, поступивший от устройства NXC, сервер OCSP присылает одно из трех значений – «expired» (срок действия истек), «current» (действует) или «unknown» (неизвестно).

27

DHCPv6

27.1 Обзор

Эта глава описывает процесс настройки объектов запросов DHCPv6.

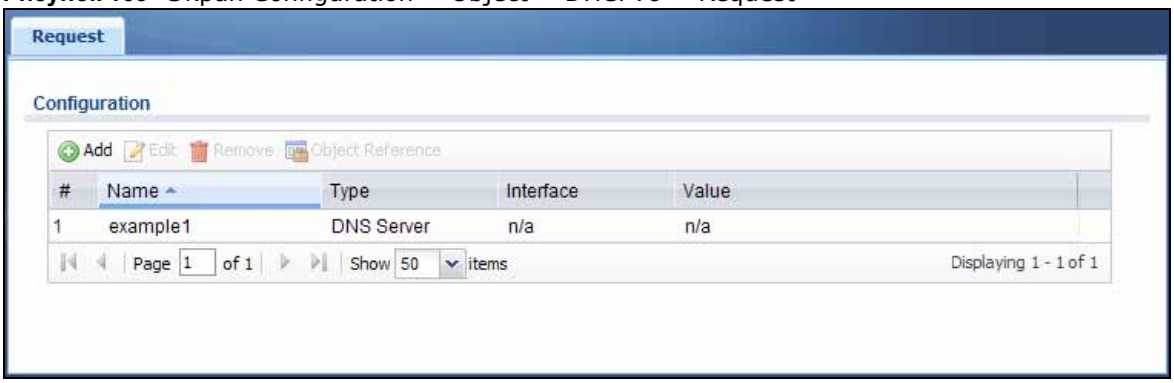
27.1.1 О чем рассказывается в этой главе

Экран **Request** (разд. 27.2 на стр. 310) служит для настройки объектов запросов DHCPv6.

27.2 Экран DHCPv6 Request

С помощью экрана **Request** можно добавлять, редактировать и удалять объекты запросов DHCPv6. Чтобы перейти к этому экрану, выберите в меню **Configuration > Object > DHCPv6 > Request**.

Рисунок 165 Экран Configuration > Object > DHCPv6 > Request



Поля экрана описаны в следующей таблице.

Таблица 149 Экран Configuration > Object > DHCPv6 > Request

ПОЛЕ	ОПИСАНИЕ
Configuration	
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Примечание: Удалить используемую в настоящий момент запись нельзя.

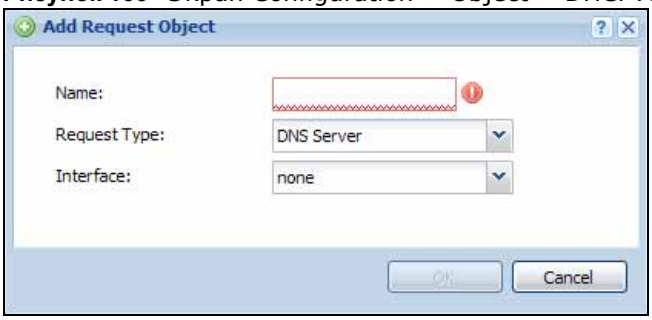
Таблица 149 Экран Configuration > Object > DHCPv6 > Request (продолжение)

ПОЛЕ	ОПИСАНИЕ
Object Reference	Выберите запись и нажмите **Object Reference**, чтобы открыть экран, на котором показано, какие параметры используют эту запись.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным объектом.
Name	Это поле показывает имя каждого объекта запроса.
Type	Это поле показывает тип каждого объекта запроса.
Interface	Это поле показывает интерфейс, используемый для каждого объекта запроса.
Value	Это поле показывает значение для каждого объекта запроса.

27.2.1 Экран Add/Edit DHCPv6 Request Object

С помощью экрана **Request Add/Edit** можно создавать новые или редактировать существующие объекты запросов. Чтобы открыть этот экран, перейдите к экрану **Request** и нажмите на пиктограмму **Add** или на пиктограмму **Edit**.

Рисунок 166 Экран Configuration > Object > DHCPv6 > Request > Add



Поля экрана описаны в следующей таблице.

Таблица 150 Экран Configuration > Object > DHCPv6 > Request > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя для этого объекта запроса. В имени можно использовать алфавитно-цифровые символы, символы подчеркивания (_) и дефиса (-) (не более 31 символа). В качестве первого символа нельзя использовать цифру. Имя чувствительно к регистру.
Request Type	Выберите тип для данного объекта запроса. Можно выбрать один из вариантов: **DNS Server** или **NTP Server**.
Interface	Выберите интерфейс для данного объекта запроса.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

28

Система

28.1 Обзор

Системные экраны позволяют настроить общие параметры устройства NXC.

28.1.1 О чем рассказывается в этой главе

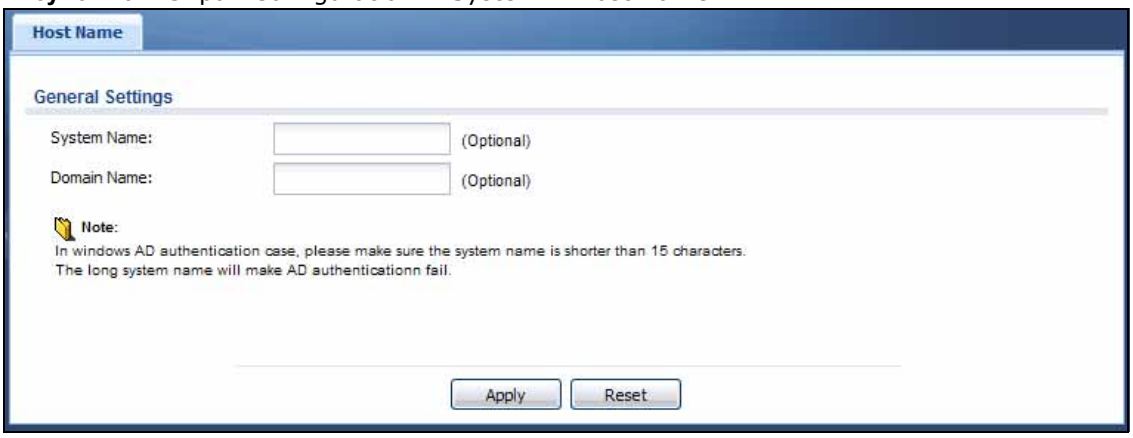
- Экран **Host Name** (разд. 28.2 на стр. 313) позволяет задать уникальное имя устройства NXC в сети.
- Экран **USB Storage** (разд. 28.3 на стр. 313) позволяет настроить параметры подключенных USB-устройств.
- Экран **Date/Time** (разд. 28.4 на стр. 314) позволяет настроить дату и время для устройства NXC.
- Экран **Console Speed** (разд. 28.5 на стр. 319) позволяет настроить скорость порта консоли при подключении к устройству NXC через порт консоли с использованием программы эмуляции терминала.
- Экран **DNS** (разд. 28.6 на стр. 319) позволяет настроить параметры сервера DNS (Domain Name System, сервер доменных имен), используемого для привязки доменных имен к соответствующим IP-адресам и наоборот.
- Экраны **WWW** (разд. 28.7 на стр. 326) позволяют настроить параметры доступа к устройству NXC по протоколам HTTP и HTTPS, а также изменить внешний вид страниц входа в систему и доступа.
- Экран **SSH** (разд. 28.8 на стр. 339) позволяет настроить параметры протокола SSH (Secure SHell) для защищенного доступа к интерфейсу командной строки устройства NXC. Можно указать, для каких зон и с каких IP-адресов разрешен доступ по протоколу SSH.
- Экран **Telnet** (разд. 28.9 на стр. 344) позволяет настроить параметры протокола Telnet для доступа к устройству NXC через интерфейс командной строки. Здесь можно указать, для каких зон и с каких IP-адресов разрешен доступ по протоколу Telnet.
- Экран **FTP** (разд. 28.10 на стр. 345) позволяет указать список зон, для которых разрешен доступ к устройству NXC по протоколу FTP. Можно также указать, с каких IP-адресов разрешен доступ по этому протоколу. Протокол FTP можно использовать для выгрузки и загрузки встроенного программного обеспечения и файлов конфигурации для устройства NXC. Более подробную информацию о встроенном программном обеспечении и файлах конфигурации можно найти в гл. 30 на стр. 373.
- Экран **SNMP** (разд. 28.11 на стр. 348) позволяет настроить параметры SNMP для устройства, в том числе список зон, с которых разрешен доступ к устройству NXC по протоколу SNMP. Можно также указать, с каких IP-адресов разрешен доступ по этому протоколу.
- Экран **Auth. Server** (разд. 28.12 на стр. 353) позволяет перевести устройство в режим работы в качестве сервера RADIUS.
- Экран **Language** (разд. 28.13 на стр. 355) позволяет выбрать язык интерфейса пользователя для экранов Web-конфигуратора устройства NXC.

- Экран **IPv6** (разд. 28.14 на стр. 356) позволяет включить или отключить поддержку протокола IPv6 устройства NXC.

28.2 Экран Host Name

Имя хоста – это уникальное имя, по которому устройство находят в сети. Чтобы открыть этот экран, выберите в меню **Configuration > System > Host Name**.

Рисунок 167 Экран Configuration > System > Host Name



Поля экрана описаны в следующей таблице.

Таблица 151 Экран Configuration > System > Host Name

ПОЛЕ	ОПИСАНИЕ
System Name	Выберите имя-описание, которое будет идентифицировать устройство NXC. Имя может содержать алфавитно-цифровые символы, его длина не может превышать 64 символа. Пробелы в имени запрещены, использование символов дефиса (-), подчеркивания (_) и точки (.) допускается.
Domain Name	Укажите здесь доменное имя (если оно известно). Это имя приходит DHCP-клиентам, подключенным к интерфейсам, на которых включена функция DHCP-сервера. Имя может содержать алфавитно-цифровые символы, его длина не может превышать 254 символа. Пробелы запрещены, использование символа дефиса («-») допускается.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

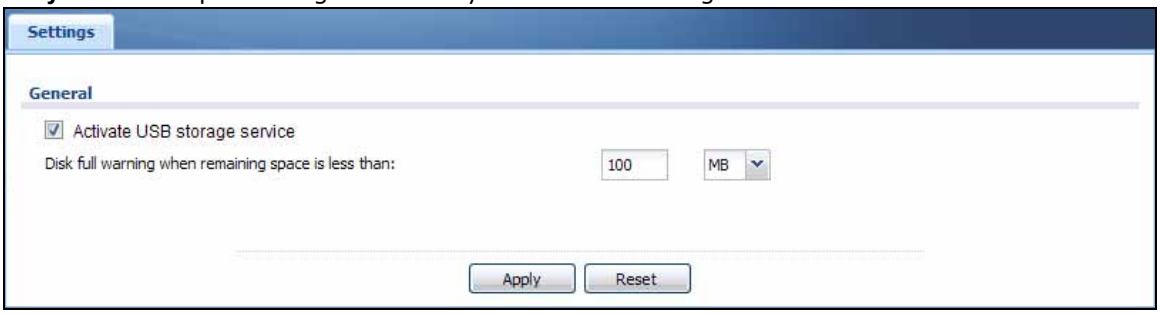
28.3 Экран USB Storage

Устройство NXC может использовать подключенный USB-накопитель для хранения системных журналов и другой диагностической информации. С помощью этого экрана можно включить эту функцию и установить порог предупреждения о переполнении диска.

Примечание: Для этой цели можно использовать только один USB-накопитель. Он должен разрешать запись (то есть он не может работать в режиме «только для чтения») и использовать файловую систему FAT16, FAT32, EXT2 или EXT3.

Выберите в меню **Configuration > System > USB Storage**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 168 Экран Configuration > System > USB Storage



Поля экрана описаны в следующей таблице.

Таблица 152 Экран Configuration > System > USB Storage

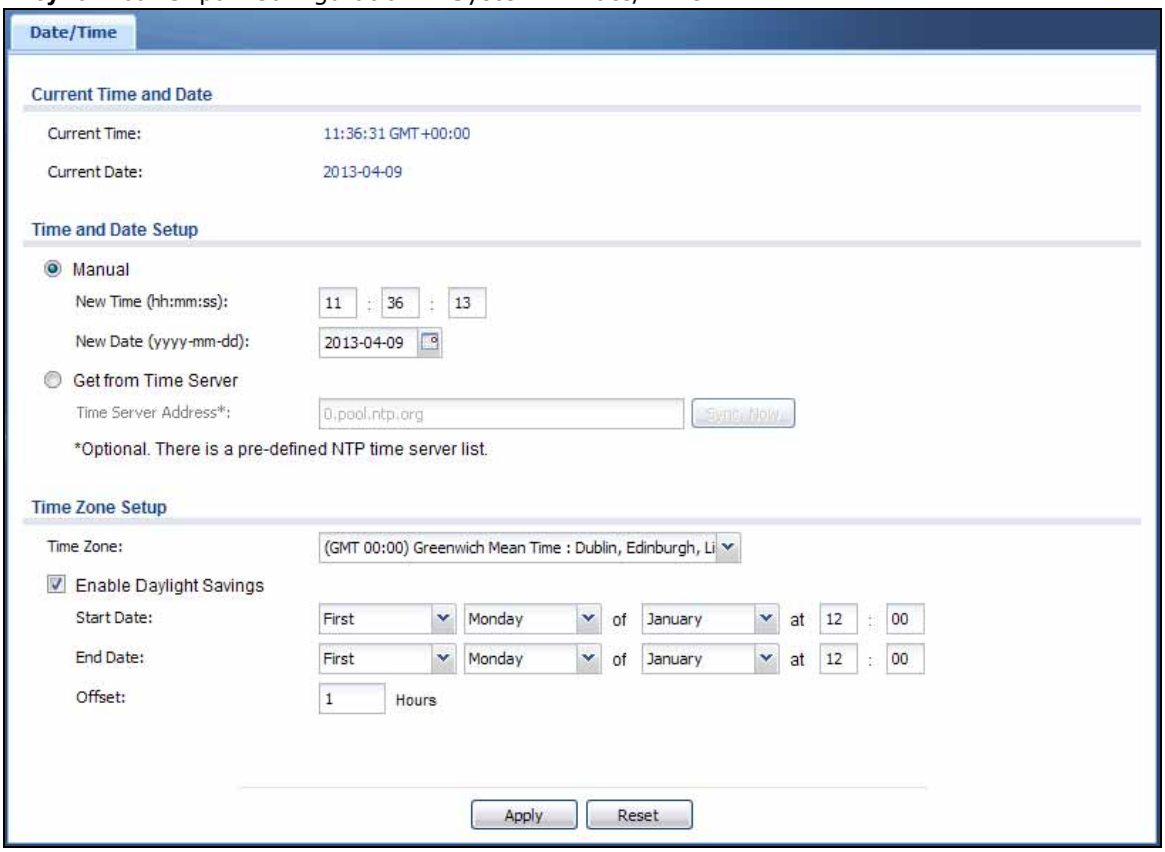
ПОЛЕ	ОПИСАНИЕ
Activate USB storage service	Выберите эту опцию, если необходимо использовать подключенный USB-накопитель.
Disk full warning when remaining space is less than	Укажите пороговое значение и выберите для него единицу измерения (Мбайт **MB** или **%**). Устройство NXC будет отправлять сообщение с предупреждением, если объем свободного дискового пространства на USB-накопителе уменьшится до указанного значения.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.4 Экран Date and Time

Для эффективной работы с расписаниями и журналами системное время на устройстве NXC должно быть точным. Чип реального времени (Real Time Chip, RTC), которым оснащено устройство NXC, отслеживает дату и время. Существует также программный механизм, который позволяет задавать время вручную или получать сведения о текущих дате и времени с внешнего сервера.

Чтобы изменить время на устройстве NXC в соответствии с местным часовым поясом и датой, выберите в меню **Configuration > System > Date/Time**. Откроется экран, изображенный на рисунке ниже. Время и дату на устройстве NXC можно установить вручную или включить механизм получения устройством NXC даты и времени с сервера времени.

Рисунок 169 Экран Configuration > System > Date/Time



Поля экрана описаны в следующей таблице.

Таблица 153 Экран Configuration > System > Date/Time

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	Это поле показывает текущее время устройства NXC.
Current Date	Это поле показывает текущую дату устройства NXC.
Time and Date Setup	
Manual	Этот переключатель следует установить в том случае, если необходимо ввести время и дату вручную. Если одновременно поменять время, дату, часовой пояс и настройки перехода на летнее время, то часовой пояс и параметры перехода на летнее время повлияют на только что введенные дату и время. При вводе настроек времени вручную устройство NXC применит новые параметры времени после того, как будет нажата кнопка **Apply**.
New Time (hh:mm:ss)	В этом поле отображается последнее время, полученное с сервера времени, или последнее время, введенное вручную. Если параметр **Time and Date Setup** установлен равным **Manual**, следует ввести в этом поле новое время и нажать кнопку **Apply**.

Таблица 153 Экран Configuration > System > Date/Time (продолжение)

ПОЛЕ	ОПИСАНИЕ
New Date (yyyy-mm-dd)	В этом поле отображается последняя дата, полученная с сервера времени, или последняя дата, введенная вручную. Если параметр **Time and Date Setup** установлен равным **Manual**, следует ввести в этом поле новую дату и нажать кнопку **Apply**.
Get from Time Server	Установите этот радиопереключатель, чтобы устройство NXC получало дату и время с сервера времени, указанного ниже. Устройство NXC запрашивает настройки времени и даты с сервера времени при следующих обстоятельствах. • При загрузке устройства NXC. • При нажатии кнопки **Apply** или кнопки **Synchronize Now** на этом экране. • Через каждые 24 часа после загрузки устройства.
Time Server Address	Введите IP-адрес или ссылку на сервер времени. В случае сомнений в выборе значения проконсультируйтесь с представителем провайдера Интернета/сетевым администратором.
Sync. Now	Нажмите эту кнопку, чтобы инициировать получение устройством NXC даты и времени с сервера времени (см. поле **Time Server Address**). Нажатие этой кнопки, кроме того, приведет к сохранению сделанных изменений (за исключением настроек перехода на летнее время).
Time Zone Setup	
Time Zone	Выберите часовой пояс для своей местности. Он определяет разницу во времени между вашим часовым поясом и Гринвичем (Greenwich Mean Time, GMT).
Enable Daylight Saving	Период летнего времени – период с поздней весны до начала осени, когда во многих странах принято переводить часы на один час вперед в целях более рационального использования светлого времени суток по вечерам. При использовании летнего времени необходимо установить данный переключатель.
Start Date	Укажите день и час, когда начинается действие летнего времени (в случае выбора переключателя **Enable Daylight Saving**). Поле **at** использует 24-часовой формат. Ниже приводится несколько примеров: Действие летнего времени на большей части Соединенных Штатов начинается со второго воскресенья марта. В каждом из часовых поясов Соединенных Штатов летнее время вступает в силу в 2:00 по местному времени. Поэтому в поле **at** для Соединенных Штатов следует выбрать Second, Sunday, March и тип 2. В странах Европейского Союза действие летнего времени начинается в последнее воскресенье марта. Во всех часовых поясах Европейского Союза летнее время вступает в силу одномоментно (1 A.M. GMT или UTC). Соответственно, для стран Европейского Союза в этом поле следует выбрать **Last**, **Sunday**, **March**. Время, которое необходимо указать в поле **at**, зависит от часового пояса. Например, для Германии, необходимо выбрать значение 2, так как часовой пояс Германии соответствует +1 часу относительно Гринвича или всеобщего скоординированного времени (GMT+1).

Таблица 153 Экран Configuration > System > Date/Time (продолжение)

ПОЛЕ	ОПИСАНИЕ
End Date	Укажите день и час, когда заканчивается действие летнего времени (в случае выбора переключателя **Enable Daylight Saving**). Поле **at** использует 24-часовой формат. Ниже приводится несколько примеров: Действие летнего времени в большинстве Соединенных Штатов прекращается с первого воскресенья ноября. В каждом из часовых поясов Соединенных Штатов летнее время отменяется в 2:00 по местному времени. Поэтому в поле **at** для Соединенных Штатов следует выбрать First, Sunday, November и тип 2. В странах Европейского Союза действие летнего времени прекращается в последнее воскресенье октября. Во всех часовых поясах Европейского Союза летнее время прекращает действовать одномоментно (1 A.M. GMT или UTC). Таким образом, для Европейского Союза необходимо выбрать **Last**, **Sunday**, **October**. Время, которое необходимо указать в поле **at**, зависит от часового пояса. Например, для Германии, необходимо выбрать значение 2, так как часовой пояс Германии соответствует +1 часу относительно Гринвича или всеобщего скоординированного времени (GMT+1).
Offset	Укажите, на сколько часов осуществляется сдвиг в момент начала и окончания действия летнего времени. Введите число от 1 до 5,5 (с шагом 0,5). Например, если в этом поле указано значение 3,5, то событие, произошедшее в 18-00 по официальному местному времени, будет зафиксировано в журнале с временем 22:30.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.4.1 Готовый список серверов времени NTP

При первом включении на устройстве NXC будут установлены следующие время и дата: 2003-01-01 00:00:00. После включения устройство NXC попытается синхронизировать время/дату с одним из серверов времени, присутствующих в заранее подготовленном списке, по протоколу NTP (Network Time Protocol, протокол сетевого времени).

Устройство NXC продолжит обращаться к следующему предопределенному списку серверов времени, работающих по протоколу NTP, если сервер времени не указан, либо устройству не удастся выполнить синхронизацию с указанным сервером времени.

Таблица 154 Серверы времени по умолчанию

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

При обращении к готовому списку серверов времени, работающих по протоколу NTP, устройство NXC случайным образом выбирает один сервер и пытается выполнить синхронизацию с ним. Если синхронизацию провести не удается, устройство NXC переходит дальше по списку до тех пор, пока либо какая-то из попыток синхронизации не окажется успешной, либо список серверов не будет исчерпан.

28.4.2 Синхронизация с сервером времени

Нажмите кнопку **Synchronize Now**, чтобы получить дату и время с сервера времени, который был указан в поле **Time Server Address**.

После появления на экране сообщения **Loading** вам, возможно, придется подождать одну минуту.

Рисунок 170 Сообщение «Loading»

Если синхронизация завершится успешно, то в полях **Current Time** и **Current Date** отобразятся значения времени и даты, полученные с сервера.

Если синхронизацию выполнить не удастся, то на экране **View Log** появится журнал. Попробуйте изменить настройки на экране **Date/Time**.

Чтобы установить дату/время на устройстве NXC вручную:

1 Выберите в меню **System > Date/Time**.

2 Выберите опцию **Manual** в разделе **Time and Date Setup**.

3 Введите время для устройства NXC в поле **New Time**.

4 Введите дату для устройства NXC в поле **New Date**.

5 В разделе **Time Zone Setup** выберите часовой пояс из списка.

6 Дополнительно можно установить переключатель **Enable Daylight Saving**, если необходимо включить на устройстве NXC опцию перехода на летнее время.

7 Нажмите на кнопку **Apply**.

Чтобы получить для устройства NXC дату и время с сервера времени:

1 Выберите в меню **System > Date/Time**.

2 Выберите опцию **Get from Time Server** в разделе **Time and Date Setup**.

3 В разделе **Time Zone Setup** выберите часовой пояс из списка.

4 В разделе **Time and Date Setup** введите адрес сервера времени в поле **Time Server Address**.

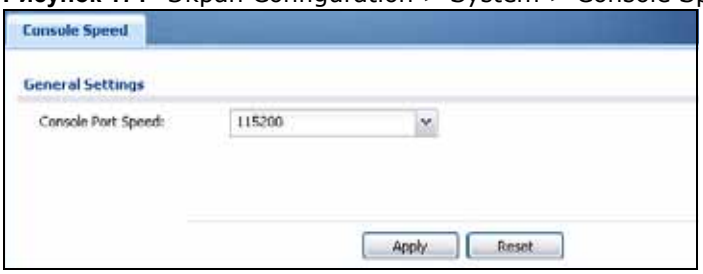
5 Нажмите на кнопку **Apply**.

28.5 Экран Console Speed

В этом разделе описана процедура настройки скорости порта консоли при подключении к устройству NXC через порт консоли с использованием программы эмуляции терминала. Настройки порта консоли по умолчанию приведены в табл. 4 на стр. 21.

Чтобы открыть этот экран, выберите в меню **Configuration > System > Console Speed**.

Рисунок 171 Экран Configuration > System > Console Speed



Поля экрана описаны в следующей таблице.

Таблица 155 Экран Configuration > System > Console Speed

ПОЛЕ	ОПИСАНИЕ
Console Port Speed	Выберите нужную скорость порта консоли в этом выпадающем списке. Устройство NXC поддерживает следующие скорости порта консоли: 9600, 19200, 38400, 57600 и 115200 бит/с (по умолчанию). Значение, выбранное в поле **Console Port Speed**, применяется к соединению через порт консоли с использованием программного обеспечения для эмуляции терминала и НЕ применяется к окну **Console** на экране Web Configurator Status устройства NXC.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.6 Обзор DNS

Сервер DNS (системы доменных имен) определяет соответствие между доменным именем и IP-адресом, и наоборот. Значение сервера DNS трудно переоценить, поскольку без него потребовалось бы знать IP-адрес каждой машины, к которой необходимо обратиться.

28.6.1 Назначение адресов серверов DNS

Устройство NXC может получить адреса серверов DNS следующими способами.

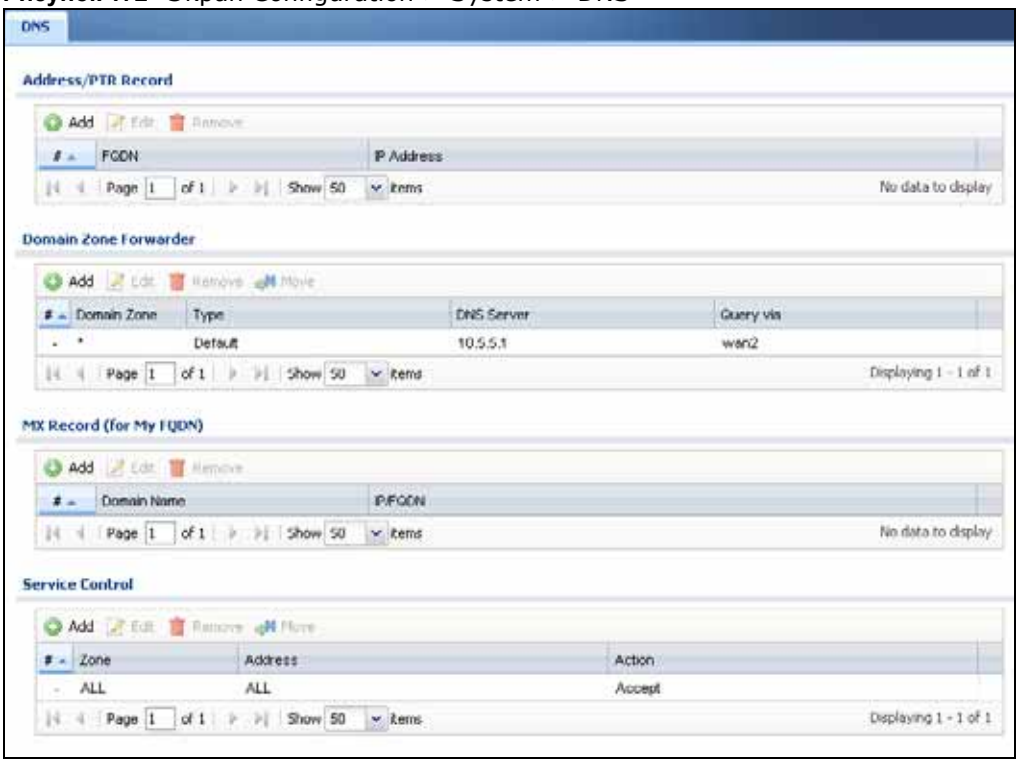
- Провайдер услуг Интернет сообщает адреса серверов DNS, обычно в виде памятки, при подписании договора о предоставлении услуг. Если провайдер услуг Интернет предоставил адреса серверов DNS, введите их вручную в полях настроек сервера DNS.
- Если провайдер услуг Интернет динамически назначает IP-адреса серверов DNS (как и IP-адрес устройства NXC в сети WAN), выберите в настройках сервера DNS опцию получения адреса сервера DNS от провайдера услуг Интернет.

- При этом сохраняется возможность указать IP-адреса других серверов DNS вручную.

28.6.2 Настройка параметров на экране DNS

Выберите в меню **Configuration > System > DNS**, чтобы изменить настройки DNS на устройстве NXC. С помощью экрана **DNS** можно выбрать для устройства NXC опцию использования сервера DNS для разрешения доменных имен, используемых системными функциями устройства NXC, например, функцией обращения к серверу времени. Можно также разрешить или запретить прием запросов DNS устройством NXC. Настройка параметров сервера DNS, которые устройство NXC рассылает указанным клиентским устройствам DHCP, выполняется на экранах **Network > Interface**.

Рисунок 172 Экран Configuration > System > DNS



Поля экрана описаны в следующей таблице.

Таблица 156 Экран Configuration > System > DNS

ПОЛЕ	ОПИСАНИЕ
Address/PTR Record	Эта запись описывает соответствие между полным доменным именем (Fully-Qualified Domain Name, FQDN) и IP-адресом. Имя в формате FQDN включает в себя имя хоста и имя домена. Например, www.zyxel.com.tw представляет собой полное доменное имя, где «www» – это хост, «zyxel» – домен третьего уровня, «com» – домен второго уровня и «tw» – домен верхнего уровня.
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
#	Это порядковый номер записи адреса/PTR record.

Таблица 156 Экран Configuration > System > DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
FQDN	Это полное доменное имя хоста.
IP Address	Это IP-адрес хоста.
Domain Zone Forwarder	Это поле указывает на IP-адрес сервера DNS. Устройство NXC может посылать на сервер DNS запросы о разрешении доменных зон для таких функций, как связь с сервером времени. Если устройству NXC требуется разрешить доменную зону, он ищет ее название в записях форвардера доменных зон в том порядке, в котором они указаны в списке.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер записи форвардера доменных зон. Порядок расположения правил имеет очень большое значение, поскольку применение правил происходит последовательно. Для форвардера доменных зон по умолчанию отображается символ дефиса (-). Параметры записи по умолчанию изменить нельзя. Устройство NXC использует эту запись по умолчанию, если доменная зона, которую надо разрешить, не совпадает ни с одной записью из числа остальных записей форвардера доменных зон.
Domain Zone	Доменная зона – это полное имя домена без хоста. Например, zyxel.com.tw – это доменная зона для полного доменного имени www.zyxel.com.tw. «*» означает все доменные зоны.
Type	Это поле указывает на то, получает ли устройство IP-адрес DNS-сервера от провайдера услуг Интернет в динамическом режиме через определенный интерфейс, либо этот IP-адрес задается вручную (**User-Defined**).
DNS Server	Это IP-адрес сервера DNS. В этом поле отображается значение **N/A**, если выбран режим получения устройством NXC IP-адреса сервера DNS в динамическом режиме от провайдера услуг Интернета, но указанный интерфейс при этом неактивен.
Query Via	Это интерфейс, через который устройство NXC отправляет запросы DNS на сервер DNS, указанный в данной записи.
MX Record (for My FQDN)	Запись типа MX (Mail eXchange, обмен почтой) идентифицирует почтовый сервер, который обрабатывает почту в определенном домене.
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
#	Это порядковый номер записи типа MX.
Domain Name	Это имя домена, в который адресована почта.
IP/FQDN	Это IP-адрес или полное доменное имя (Fully-Qualified Domain Name, FQDN) почтового сервера, который обрабатывает почту для домена, указанного в поле выше.

Таблица 156 Экран Configuration > System > DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service Control	Это поле определяет, с каких компьютеров и из каких зон разрешается посылать запросы DNS на устройство NXC.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами. Порядок расположения правил имеет очень большое значение, поскольку применение правил происходит последовательно. Запись с дефисом (-) вместо номера соответствует политике устройства NXC по умолчанию (чьи параметры менять нельзя). Устройство NXC применяет ее к трафику, который не соответствует ни одному из созданных правил. Данное правило не является редактируемым. Если необходимо применить другой алгоритм, создайте правило, критериям которого этот трафик будет соответствовать, и тогда устройство NXC не будет использовать для него политику по умолчанию.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается отправка запросов DNS.
Action	Это поле указывает на то, принимает ли устройство NXC запросы DNS, пришедшие от компьютера с указанным выше IP-адресом через указанную зону (**Accept**), или отбрасывает их (**Deny**).

28.6.3 Адресные записи

Адресная запись содержит соответствие между полным доменным именем (Fully-Qualified Domain Name, FQDN) и IP-адресом. Имя в формате FQDN включает в себя имя хоста и имя домена. Например, www.zyxel.com – это полное доменное имя, где «www» – это хост, «zyxel» – домен второго уровня и «com» – домен верхнего уровня. mail.myZyXEL.com.tw – это тоже полное доменное имя (FQDN), где «mail» – это хост, «myZyXEL» – домен третьего уровня, «com» – домен второго уровня и «tw» – домен верхнего уровня.

Устройство NXC позволяет создавать адресные записи как для устройства NXC, так и для других устройств. Таким образом можно хранить информацию об именах DNS и адресах, к которым часто обращаются пользователи в сети. При поступлении на устройство NXC запроса DNS, ссылающегося на полное доменное имя (FQDN), для которого на устройстве NXC имеется адресная запись, то устройство NXC может само отправить нужный IP-адрес в ответном сообщении DNS, не обращаясь к другому серверу DNS.

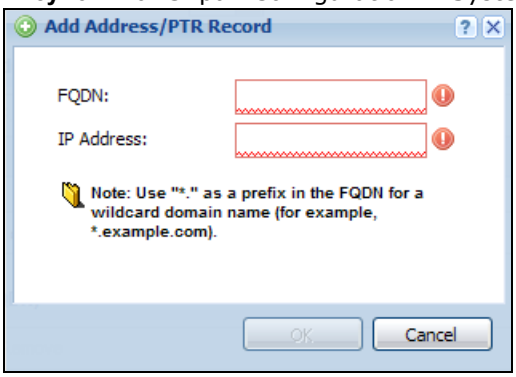
28.6.4 Запись типа PTR

Запись типа PTR (pointer, указатель) называют также обратной записью или записью обратного поиска. Она определяет соответствие между IP-адресом и доменным именем.

28.6.5 Создание адресной записи/записи PTR

Нажмите на пиктограмме **Add** в таблице **Address/PTR Record**, чтобы добавить новую адресную запись/запись PTR.

Рисунок 173 Экран Configuration > System > DNS > Add Address/PTR Record



Поля экрана описаны в следующей таблице.

Таблица 157 Экран Configuration > System > DNS > Add Address/PTR Record

ПОЛЕ	ОПИСАНИЕ
FQDN	Введите полное доменное имя (Fully-Qualified Domain Name, FQDN) сервера. Имя FQDN начинается с имени хоста и продолжается вплоть до доменного имени верхнего уровня. Например, www.zyxel.com.tw представляет собой полное доменное имя, где «www» – это хост, «zyxel» – домен третьего уровня, «com» – домен второго уровня и «tw» – домен верхнего уровня. Использование подчеркиваний в имени не допускается. Используйте префикс «*.» в имени FQDN для обозначения множества любых имен данного уровня (например, *.example.com).
IP Address	Введите IP-адрес хоста в точечно-десятичной нотации.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений

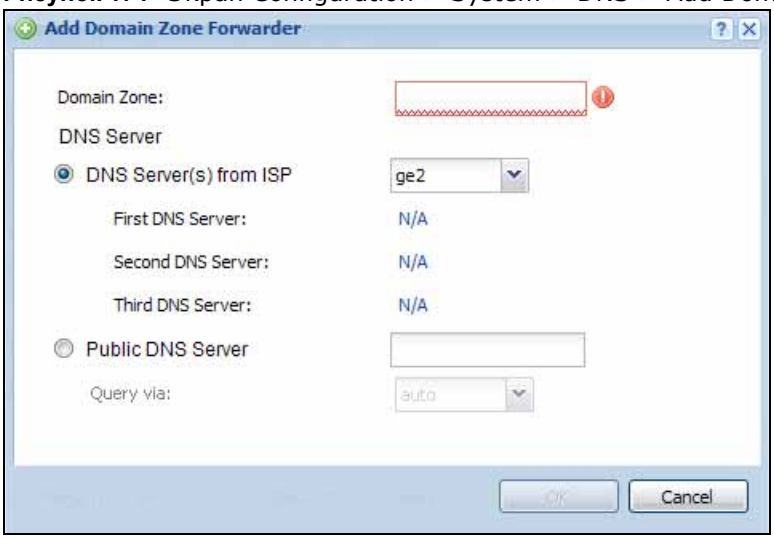
28.6.6 Форвардер доменных зон

Форвардер доменных зон содержит IP-адрес сервера DNS. Устройство NXC может посылать на сервер DNS запросы о разрешении доменных зон для таких функций, как связь с сервером времени. Доменная зона – это полное имя домена без хоста. Например, zyxel.com – это доменная зона для полного доменного имени www.zyxel.com.

28.6.7 Создание записи форвардера доменных зон

Нажмите на пиктограмму **Add** в таблице **Domain Zone Forwarder**, чтобы добавить новую запись форвардера доменных зон.

Рисунок 174 Экран Configuration > System > DNS > Add Domain Zone Forwarder



Поля экрана описаны в следующей таблице.

Таблица 158 Экран Configuration > System > DNS > Add Domain Zone Forwarder

ПОЛЕ	ОПИСАНИЕ
Domain Zone	Доменная зона – это полное имя домена без хоста. Например, zyxel.com.tw – это доменная зона для полного доменного имени www.zyxel.com.tw. Например, если устройство NXC получает запрос на разрешение доменного имени zyxel.com.tw, оно может направить запрос по IP-адресу сервера имен, указанного в данной записи. Введите *, если обслуживание всех доменных зон осуществляет указанный сервер (или серверы) DNS.
DNS Server	Выберите опцию **DNS Server(s) from ISP**, если провайдер услуг Интернет предоставляет информацию о серверах DNS в динамическом режиме. Необходимо также выбрать интерфейс, через который провайдер услуг Интернет предоставляет сведения об IP-адресе (или адресах) сервера DNS. Этот интерфейс нужно активировать и настроить для работы в качестве DHCP-клиента. Поля, приведенные ниже, отображают (показывают в режиме «только для чтения») IP-адрес (или адреса) сервера DNS, назначенного провайдером услуг Интернет. **Значение N/A** отображается во всех полях для IP-адресов серверов DNS, для которых провайдер услуг Интернет не назначил адрес. Примечание: Если все интерфейсы являются статическими, то это поле будет скрыто. Выберите опцию **Public DNS Server**, если известен IP-адрес сервера DNS. Введите IP-адрес сервера DNS в поле справа. Сервер DNS должен быть в пределах досягаемости для устройства NXC. Сервер DNS может находиться в Интернете или в одной из локальных сетей устройства NXC. Значение 0.0.0.0 использовать не разрешается. Выберите в поле **Query via** интерфейс, через который устройство NXC отправляет запросы DNS серверу DNS.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений.

28.6.8 Запись типа MX

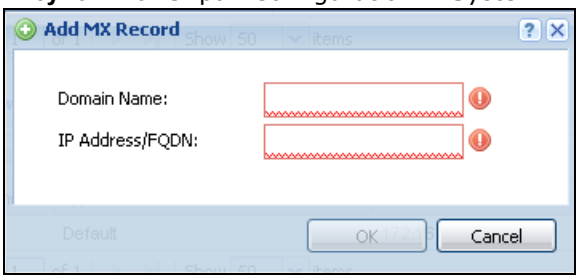
Запись типа MX (Mail eXchange) указывает на хост, который отвечает за обработку почты в определенном домене, то есть определяет, куда следует отправлять почту в этом домене. Если не указать соответствующие записи типа MX для своего или для других доменов, то другие

почтовые серверы не смогут доставить внешнюю почту на ваш почтовый сервер, и наоборот. Для каждого хоста или домена может существовать только одна запись типа MX, то есть одному домену соответствует один хост.

28.6.9 Создание записи типа MX

Нажмите на пиктограмму **Add** в таблице **MX Record**, чтобы создать новую запись типа MX.

Рисунок 175 Экран Configuration > System > DNS > Add MX Record



Поля экрана описаны в следующей таблице.

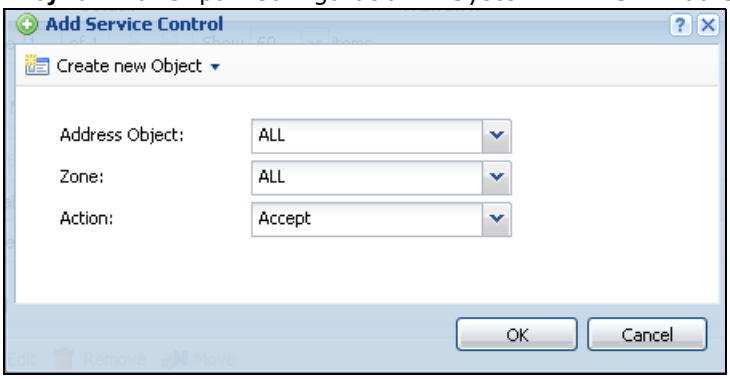
Таблица 159 Экран Configuration > System > DNS > Add MX Record

ПОЛЕ	ОПИСАНИЕ
Domain Name	Введите имя домена, для которого предназначается почта.
IP Address/FQDN	Введите IP-адрес или полное доменное имя (Fully-Qualified Domain Name, FQDN) почтового сервера, который обрабатывает почту для домена, указанного в поле выше.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений

28.6.10 Добавление правил управления службами

Нажмите на пиктограмму **Add** в таблице **Service Control**, чтобы создать новое правило управления службами.

Рисунок 176 Экран Configuration > System > DNS > Add Service Control Rule



Поля экрана описаны в следующей таблице.

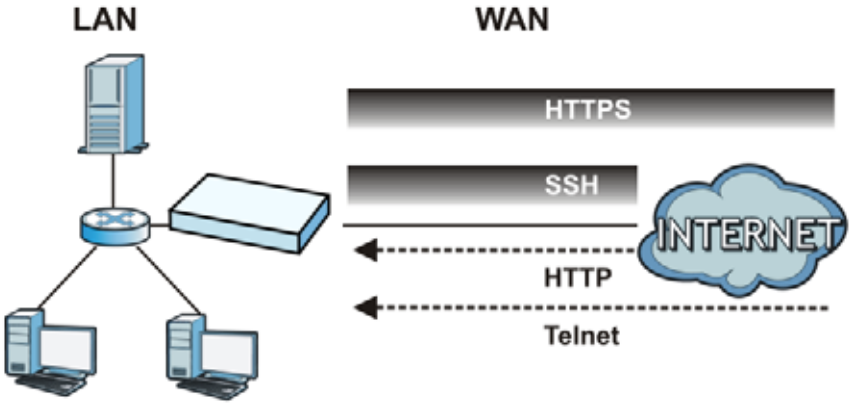
Таблица 160 Экран Configuration > System > DNS > Add Service Control Rule

ПОЛЕ	ОПИСАНИЕ
Create new Object	С помощью этой кнопки можно создать любые новые объекты настроек, которые понадобятся на этом экране.
Address Object	Выберите опцию **ALL**, если необходимо разрешить или запретить любому компьютеру отправку запросов DNS на устройство NXC. Выберите заранее созданный адресный объект, чтобы разрешить или запретить компьютеру с указанным IP-адресов отправлять запросы DNS на устройство NXC.
Zone	Выберите опцию **ALL**, чтобы разрешить или запретить отправку запросов DNS через любые зоны. Выберите заранее созданную зону, в которой разрешена или запрещена отправка запросов DNS на устройство NXC.
Action	Выберите **Accept**, чтобы устройство NXC разрешало запросы DNS от указанного компьютера. Выберите **Deny**, чтобы устройство NXC блокировало запросы DNS от указанного компьютера.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений

28.7 Обзор службы WWW

На рисунке ниже показаны варианты безопасного и небезопасного управления устройством NXC из сети WAN. Доступ по протоколам HTTPS и SSH является защищенным. Доступ по протоколам HTTP и Telnet является незащищенным.

Рисунок 177 Защищенные и незащищенные варианты доступа из сети WAN с использованием различных служб



28.7.1 Ограничения доступа к службам

Данную службу нельзя использовать для доступа к устройству NXC, если:

1 Эта служба была отключена на соответствующем экране.

2 Разрешенный IP-адрес (адресный объект) в таблице **Service Control** не соответствует IP-адресу данного клиента (устройство NXC запрещает эту сессию).

3 IP-адрес (адресный объект) в таблице **Service Control** не принадлежит к разрешенной зоне, или для него установлено действие **Deny**.

28.7.2 Системный тайм-аут

Для администраторов существует срок действия аренды. Устройство NXC автоматически прерывает управляющую сессию, если время отсутствия активности для нее превышает период тайм-аута. Тайм-аут управляющей сессии не происходит, если выполняется сбор сведений на экране статистики.

По истечении интервала повторной аутентификации устройство NXC предлагает каждому пользователю пройти аутентификацию еще раз.

Изменить параметры тайм-аута можно на экранах **User/Group**.

28.7.3 HTTPS

Можно настроить на устройстве NXC использование протокола HTTP или HTTPS (HTTPS является более безопасным) для работы с Web-конфигуратором. Укажите, для каких зон и с каких IP-адресов разрешен доступ к Web-конфигуратору.

Протокол HTTPS (протокол передачи гипертекста через протокол защищенных сокетов, или HTTP через SSL) – это Web-протокол, обеспечивающий шифрование и дешифрование Web-страниц. Протокол защищенных сокетов Secure Socket Layer (SSL) представляет собой протокол уровня приложений, реализующий безопасную передачу данных посредством обеспечения конфиденциальности (посторонние не смогут прочесть передаваемые данные), аутентификации (одна сторона может идентифицировать другую) и целостности данных (изменение данных будет заметно).

Этот протокол работает на основе сертификатов, открытых и секретных ключей (более подробную информацию можно найти в гл. 26 на стр. 290).

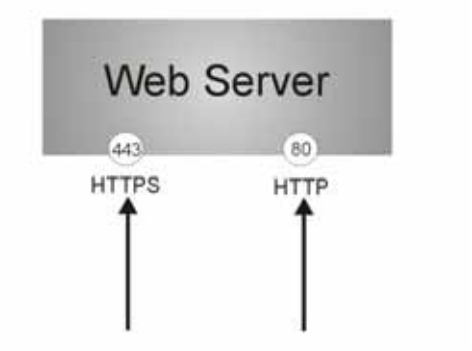
Протокол HTTPS на устройстве NXC используется для предоставления доступа к устройству NXC через Web-конфигуратор. В соответствии с протоколом SSL сервер HTTPS (устройство NXC) должен всегда предоставлять свою аутентификационную информацию клиенту HTTPS (компьютеру, который запрашивает соединение HTTPS с устройством NXC), тогда как клиент HTTPS должен проходить аутентификацию только по требованию сервера HTTPS (выберите опцию **Authenticate Client Certificates** на экране **WWW**). Опция **Authenticate Client Certificates** является необязательной. В случае ее выбора клиент HTTPS должен обязательно отправлять устройству NXC сертификат. За сертификатом для браузера следует обращаться к поставщику сертификатов, являющемуся доверенным поставщиком сертификатов для устройства NXC.

См. следующий рисунок.

1 Запросы на соединение HTTPS от веб-браузера с поддержкой SSL по умолчанию поступают на порт 443 веб-сервера устройства NXC.

2 Запросы на соединение HTTP от веб-браузера по умолчанию поступают на порт 80 веб-сервера устройства NXC.

Рисунок 178 Реализация HTTP/HTTPS



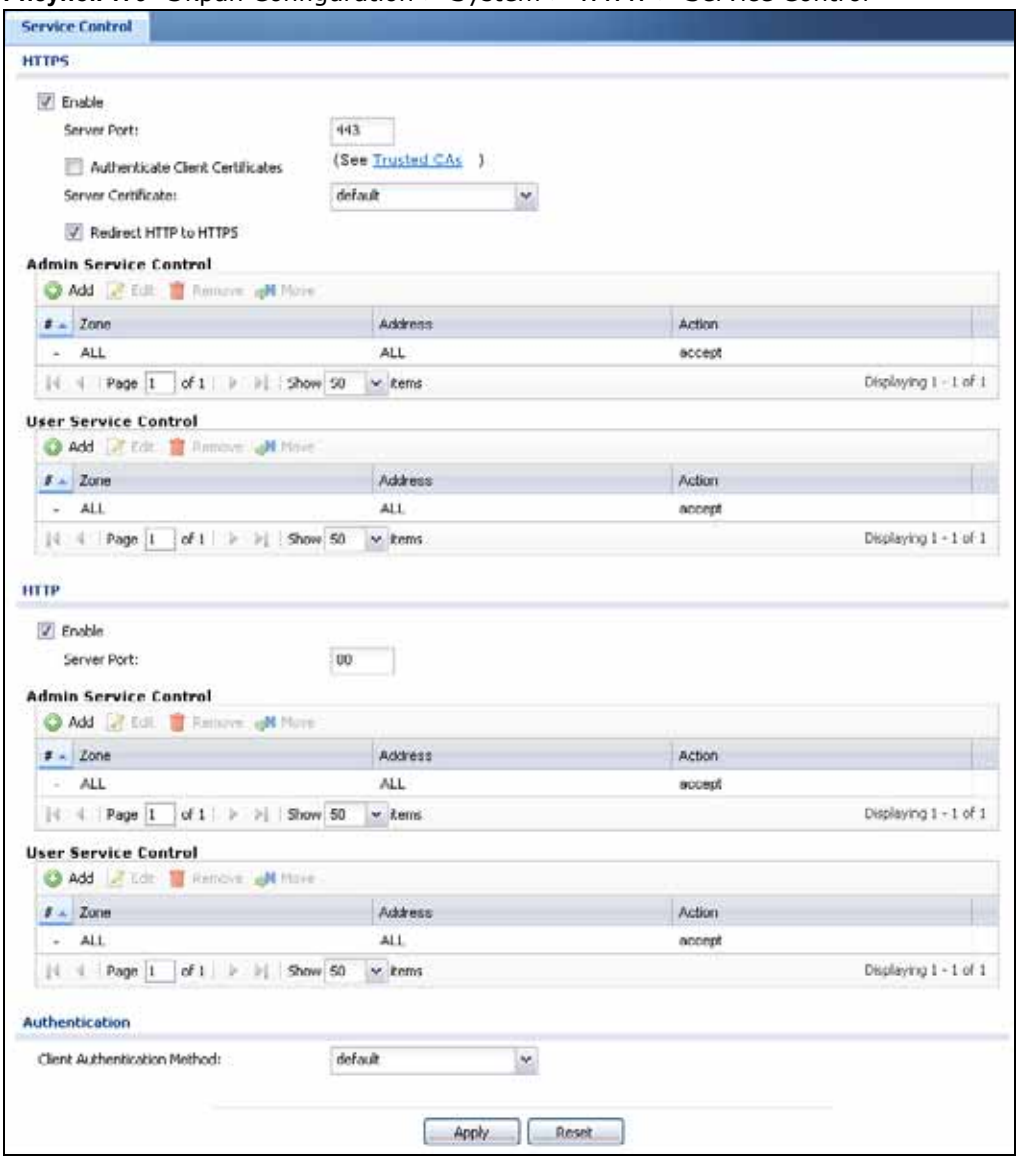
Примечание: Если отключить опцию **HTTP** на экране **WWW**, то устройство NXC будет блокировать все попытки соединений HTTP.

28.7.4 Настройка управления службами WWW

Выберите в меню **Configuration > System > WWW**. чтобы открыть экран **WWW**. С помощью этого экрана можно указать, из каких зон разрешен доступ к устройству NXC по протоколам HTTP или HTTPS. Можно также указать, с каких IP-адресов разрешен доступ по указанным протоколам.

Примечание: Раздел **Admin Service Control** описывает параметры управляющего доступа (через Web-конфигуратор).
Раздел **User Service Control** описывает параметры доступа пользователей к устройству NXC.

Рисунок 179 Экран Configuration > System > WWW > Service Control



Поля экрана описаны в следующей таблице.

Таблица 161 Экран Configuration > System > WWW > Service Control

ПОЛЕ	ОПИСАНИЕ
HTTPS	
Enable	Установите этот переключатель, чтобы разрешить или запретить компьютеру с IP-адресом, совпадающим с IP-адресом в таблице **Service Control**, доступ к Web-конфигуратору устройства NXC с использованием соединения HTTPS.
Server Port	По умолчанию сервер HTTPS прослушивает порт 443. Если номер порта для сервера HTTPS на устройстве NXC был изменен, например, установлен равным 8443, необходимо будет уведомить пользователей, которые захотят подключиться к устройству NXC через Web-конфигуратор, что им следует использовать в качестве адреса строку вида «https://IP-адрес-NXC:**8443**».

Таблица 161 Экран Configuration > System > WWW > Service Control (продолжение)

ПОЛЕ	ОПИСАНИЕ
Authenticate Client Certificates	Выберите опцию **Authenticate Client Certificates** (она не является обязательной), если необходимо потребовать от SSL-клиента обязательной аутентификации на устройстве NXC посредством отправки сертификата на устройство NXC. Для этого SSL-клиент должен иметь сертификат, подписанный центром сертификации, который был импортирован в качестве доверенного центра сертификации на устройство NXC.
Server Certificate	Выберите сертификат, который сервер HTTPS (устройство NXC) будет использовать при отправке собственных аутентификационных данных клиенту HTTPS. Соответствующие сертификаты должны быть уже занесены в систему на экране **My Certificates**.
Redirect HTTP to HTTPS	Выберите опцию, если необходимо обеспечить переадресацию всех запросов на HTTP соединение на сервер HTTPS. В этом случае будет исключена возможность незащищенного доступа к Web-конфигуратору.
Admin/User Service Control	Раздел **Admin Service Control** описывает, из каких зон администратор может управлять устройством NXC (через Web-конфигуратор) с использованием соединения HTTPS. Можно также указать, с каких IP-адресов администраторы могут управлять устройством NXC. Раздел **User Service Control** описывает, из каких зон пользователи могут подключаться к устройству NXC с использованием соединения HTTPS. Можно также указать, с каких IP-адресов пользователи могут подключаться к устройству NXC.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами. Запись с дефисом (-) вместо номера соответствует политике устройства NXC по умолчанию (чьи параметры менять нельзя). Устройство NXC применяет ее к трафику, который не соответствует ни одному из созданных правил. Данное правило не является редактируемым. Если необходимо применить другой алгоритм, создайте правило, критериям которого этот трафик будет соответствовать, и тогда устройство NXC не будет использовать для него политику по умолчанию.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается доступ.
Action	Это поле указывает на то, разрешен ли (значение **Accept**) компьютеру с IP-адресом, указанным выше, доступ к зоне устройства NXC, указанной в поле **Zone**, или нет (значение **Deny**).
HTTP	
Enable	Установите этот переключатель, чтобы разрешить или запретить компьютеру с IP-адресом, совпадающим с IP-адресом в таблице **Service Control**, доступ к Web-конфигуратору устройства NXC с использованием соединения HTTP.

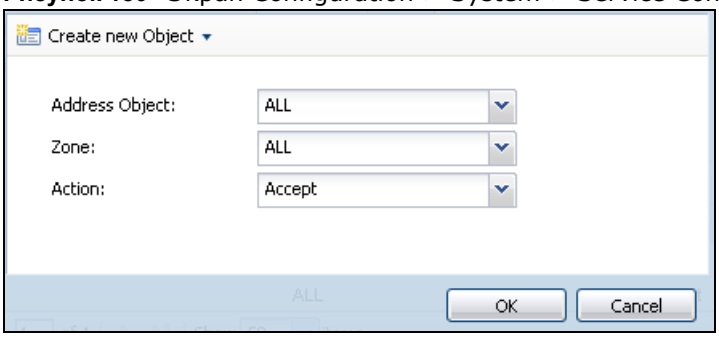
Таблица 161 Экран Configuration > System > WWW > Service Control (продолжение)

ПОЛЕ	ОПИСАНИЕ
Server Port	При необходимости можно изменить номер порта сервера для данной службы, но в этом случае придется использовать тот же номер порта для доступа к устройству NXC посредством этой службы.
Admin/User Service Control	Раздел **Admin Service Control** описывает, из каких зон администратор может управлять устройством NXC (через Web-конфигуратор) с использованием протокола HTTP. Можно также указать, с каких IP-адресов администраторы могут управлять устройством NXC. Раздел **User Service Control** описывает, из каких зон пользователи могут подключаться к устройству NXC с использованием соединения HTTP. Можно также указать, с каких IP-адресов пользователи могут подключаться к устройству NXC.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами. Запись с дефисом (-) вместо номера соответствует политике устройства NXC по умолчанию (чьи параметры менять нельзя). Устройство NXC применяет ее к трафику, который не соответствует ни одному из созданных правил. Данное правило не является редактируемым. Если необходимо применить другой алгоритм, создайте правило, критериям которого этот трафик будет соответствовать, и тогда устройство NXC не будет использовать для него политику по умолчанию.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается доступ.
Action	Это поле указывает на то, разрешен ли (значение **Accept**) компьютеру с IP-адресом, указанным выше, доступ к зоне устройства NXC, указанной в поле **Zone**, или нет (значение **Deny**).
Authentication	
Client Authentication Method	Выберите метод, который сервер HTTPS или HTTP будет использовать для аутентификации клиентов. Соответствующие методы аутентификации уже должны быть настроены с помощью экрана **Auth. method**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.7.5 Правила управления службами

Воспользуйтесь кнопками **Add** или **Edit** в таблице **Service Control** на экранах **WWW**, **SSH**, **TELNET**, **FTP** или **SNMP**, чтобы добавить или изменить правило управления службами.

Рисунок 180 Экран Configuration > System > Service Control Rule > Add/Edit



Поля экрана описаны в следующей таблице.

Таблица 162 Экран Configuration > System > Service Control Rule > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Create new Object	С помощью этой кнопки можно создать любые новые объекты настроек, которые понадобятся на этом экране.
Address Object	Выберите опцию **ALL**, если необходимо разрешить или запретить любому компьютеру доступ к устройству NXC с использованием этой службы. Выберите заранее созданный адресный объект, чтобы разрешить или запретить компьютеру с указанным IP-адресом доступ к устройству NXC с использованием данной службы.
Zone	Выберите опцию **ALL**, чтобы разрешить или запретить доступ к любым зонам устройства NXC с использованием данной службы. Выберите заранее созданную зону устройства NXC, в которой разрешена или запрещена входящая служба.
Action	Выберите опцию **Accept**, если необходимо разрешить пользователю доступ к устройству NXC с указанных компьютеров. Выберите опцию **Deny**, если необходимо запретить пользователю доступ к устройству NXC с указанных компьютеров.
OK	Нажмите кнопку **OK**, чтобы сохранить измененные параметры и закрыть этот экран.
Cancel	Нажмите кнопку **Cancel**, чтобы покинуть этот экран без сохранения изменений

28.7.6 Пример подключения по протоколу HTTPS

Если порт HTTPS по умолчанию для устройства NXC не менялся, введите в адресной строке браузера «https://IP-адрес устройства NXC», где «IP-адрес устройства NXC» – это IP-адрес или доменное имя устройства NXC, к которому необходимо получить доступ.

28.7.6.1 Предупредительные сообщения Internet Explorer

При попытке получить доступ к устройству NXC через HTTPS-сервер появится диалоговое окно Windows с вопросом о доверии к сертификату сервера. Нажмите кнопку **View Certificate**, чтобы проверить, принадлежит ли сертификат устройству NXC.

В Internet Explorer появляется следующее сообщение **Security Alert**. Нажмите кнопку **Yes**, чтобы перейти к экрану входа в Web-конфигуратор; если нажать кнопку **No**, доступ к Web-конфигуратору будет заблокирован.

Рисунок 181 Диалоговое окно Security Alert (Internet Explorer)

28.7.6.2 Как избежать появления предупредительных сообщений в браузере

Ниже перечислены основные причины появления предупредительных сообщений, касающихся сертификатов сервера HTTPS, развернутого на устройстве NXC, а также методы, позволяющие избежать появления этих сообщений:

- Центр сертификации, выпустивший сертификат для сервера HTTPS устройства NXC, не принадлежит к числу доверенных центров сертификации данного браузера. Центром сертификации заводского сертификата по умолчанию устройства NXC является само устройство NXC, поскольку сертификат является самоподписанным.
- Для того, чтобы браузер доверял самоподписанному сертификату, импортируйте его в хранилище сертификатов операционной системы в качестве доверенного сертификата.
- Для того, чтобы браузер доверял сертификатам, выпущенным каким-либо центром сертификации, импортируйте сертификат данного центра сертификации в хранилище сертификатов операционной системы в качестве доверенного сертификата. Более подробную информацию можно найти в прил. C на стр. 450.

28.7.6.3 Экран входа в систему

После принятия сертификата откроется экран входа на устройство NXC. Значок замка в нижней части экрана браузера свидетельствует об установлении защищенного соединения.

Рисунок 182 Экран входа в систему (Internet Explorer)

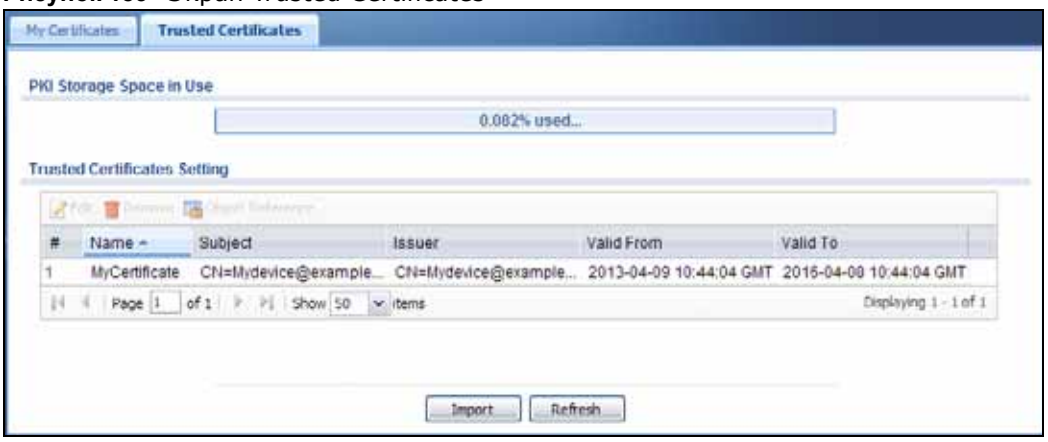
28.7.6.4 Регистрация и импорт сертификатов SSL-клиентов

SSL-клиенту требуется сертификат в том случае, если в настройках устройства NXC выбрана опция Authenticate Client Certificates.

Необходимо импортировать хотя бы один доверенный центр сертификации на устройство NXC, чтобы опция **Authenticate Client Certificates** стала активной (более подробную информацию можно найти в главе «Сертификаты»).

Запросите сертификат у центра сертификации, который устройство NXC считает доверенным (см. экран Web-конфигуратора Trusted Certificates для устройства NXC).

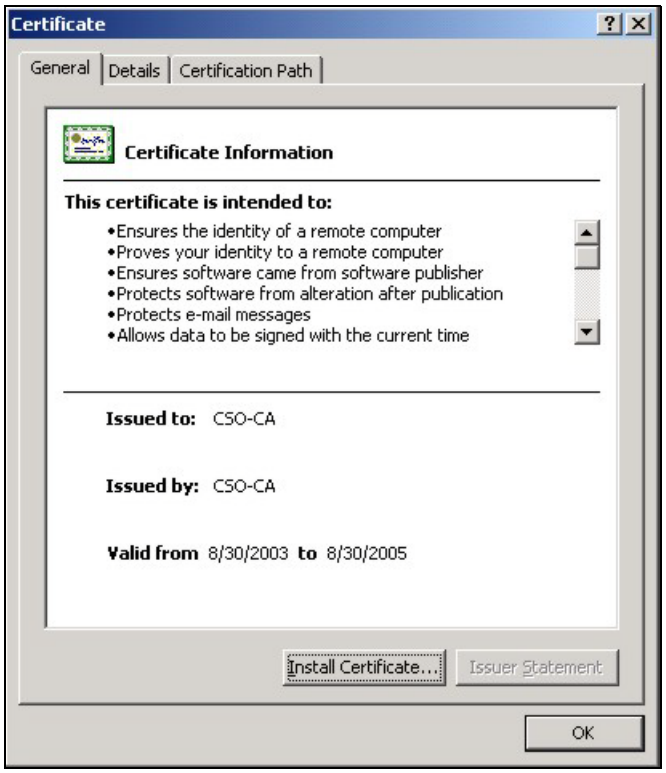
Рисунок 183 Экран Trusted Certificates



Центр сертификации направляет пакет, содержащий доверенный сертификат (или сертификаты) центра сертификации, персональный сертификат (или сертификаты) и пароль для установки персонального сертификата (или сертификатов).

28.7.6.5 Установка сертификата, полученного от центра сертификации

1 Дважды щелкните мышью по доверенному сертификату, полученному от центра сертификации. Откроется экран, похожий на тот, что изображен ниже.



2 Нажмите кнопку **Install Certificate** и следуйте указаниям мастера пошаговой настройки, как показано ранее в этом приложении.

28.7.6.6 Установка персонального сертификата

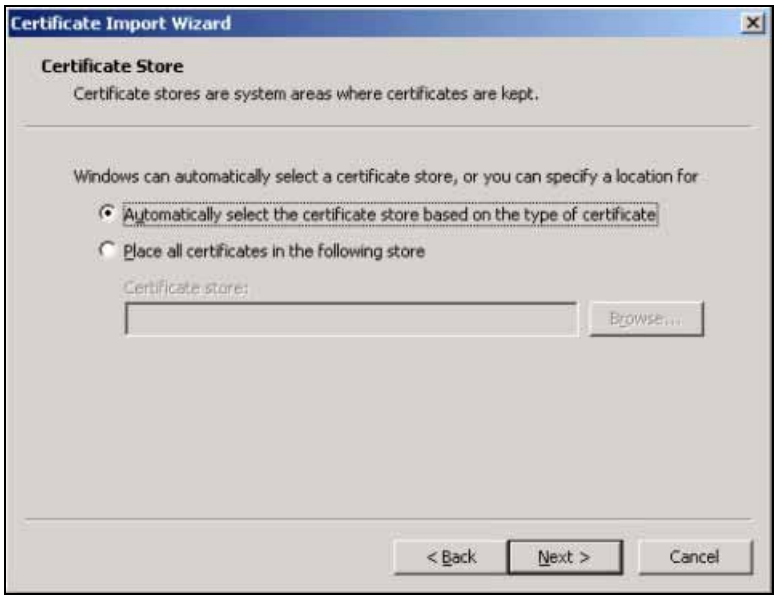
До начала установки необходимо получить пароль. Пароль может быть выпущен центром сертификации, либо вам, возможно, потребуется указать его самостоятельно при регистрации сертификата. Дважды щелкните мышью по персональному сертификату, предоставленному центром сертификации. Откроется экран, похожий на тот, что изображен ниже

1 Нажмите кнопку **Next, чтобы запустить мастер пошаговой настройки**.

2 Имя и путь к файлу сертификата после двойного щелчка мышью должны автоматически появиться в текстовом поле **File name**. Нажмите кнопку **Browse**, если необходимо импортировать другой сертификат.

3 Введите пароль, предоставленный центром сертификации.

4 Позвольте мастеру пошаговой настройки самостоятельно определить, где именно следует сохранить данный сертификат на компьютере, или выберите опцию **Place all certificates in the following store** и укажите нужный каталог сами.



5 Нажмите кнопку **Finish**, чтобы завершить работу мастера пошаговой настройки и начать процесс импорта.

6 Если сертификат установлен правильно, появится следующий экран.

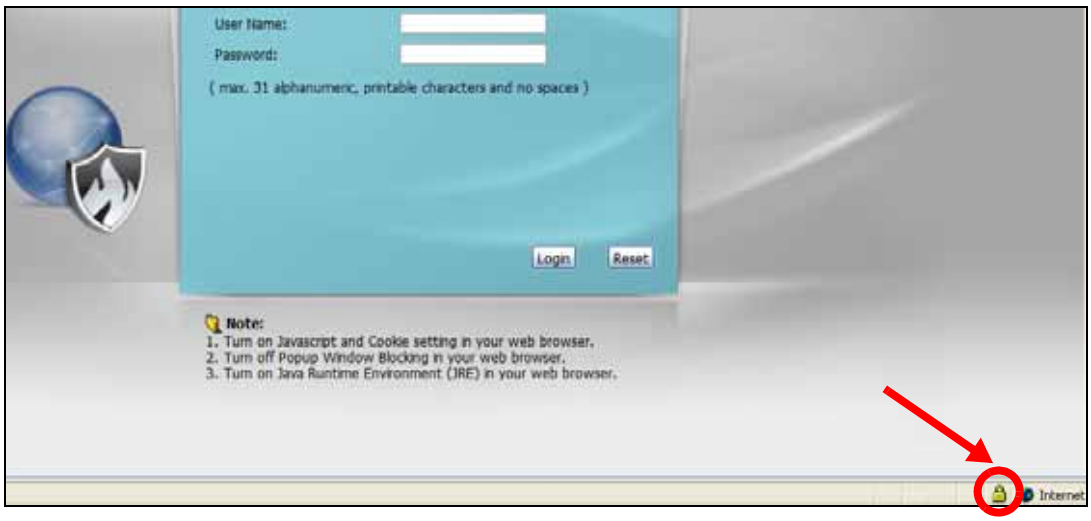
28.7.6.7 Использование сертификата при доступе к устройству NXC

Чтобы обратиться к устройству NXC по протоколу HTTPS:

1 Введите строку вида «https://IP-адрес устройства NXC/» в строке адреса браузера.

2 Если в настройках устройства NXC выбрана опция Authenticate Client Certificates, то на следующем экране будет предложено выбрать персональный сертификат для отправки на устройство NXC. Следующий экран откроется, даже если имеется только один сертификат, как в примере.

3 Затем откроется экран вход в Web-конфигуратор.



28.8 Протокол SSH

Протокол SSH (Secure SHell) используют для защищенного доступа к интерфейсу командной строки устройства NXC. Укажите. для каких зон и с каких IP-адресов разрешен доступ по протоколу SSH.

SSH – это защищенный коммуникационный протокол, который совмещает возможности аутентификации и шифрования для обеспечения безопасной передачи данных между двумя хостами по небезопасной сети. На следующем рисунке компьютер A, который находится в сети

Интернет, использует протокол SSH для защищенного подключения к порту WAN устройства NXC с целью управления.

Рисунок 184 Пример подключения с использованием протокола SSH по сети WAN

28.8.1 Как работает протокол SSH

Следующий рисунок иллюстрирует процесс установки защищенного соединения между двумя удаленными хостами с использованием протокола SSH v1.

Рисунок 185 Пример работы протокола SSH v1

1 Идентификация хоста

SSH-клиент отправляет запрос на соединение SSH-серверу. Сервер идентифицирует себя с помощью ключа хоста. Клиент шифрует случайно сгенерированный ключ сессии с помощью ключа хоста и ключа сервера, затем отправляет результат обратно на сервер.

Клиент автоматически сохраняет все новые открытые ключи сервера. При последующих подключениях открытый ключ сервера сверяется с сохраненной версией на клиентском компьютере.

2 Метод шифрования

После проверки идентификационной информации клиент и сервер должны согласовать используемый метод шифрования.

3 Аутентификация и передача данных

После проверки идентификационных данных и активации шифрования образуется защищенный туннель между клиентом и сервером. Для подключения к серверу клиент отправляет ему аутентификационную информацию (имя пользователя и пароль).

28.8.2 Реализация протокола SSH на устройстве NXC

Устройство NXC поддерживает протокол SSH версии 1 и 2 с использованием аутентификации RSA и четырех методов шифрования (AES, 3DES, Archfour и Blowfish). На устройстве NXC развернут сервер SSH для удаленного управления по порту 22 (по умолчанию).

28.8.3 Требования к использованию протокола SSH

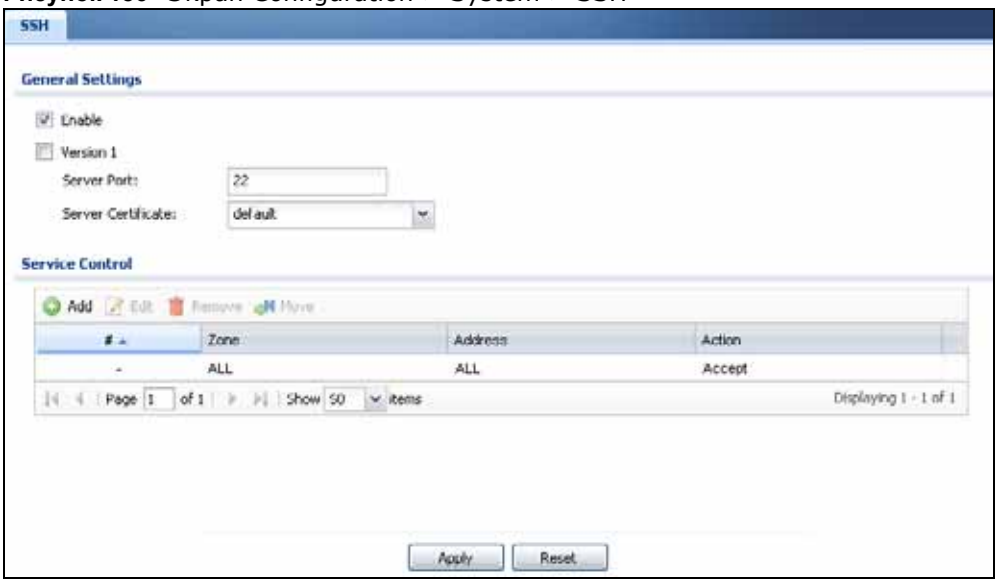
Для подключения к устройству NXC по протоколу SSH необходимо установить программу-клиент SSH на клиентском компьютере (с установленной операционной системой Windows или Linux).

28.8.4 Настройка SSH

Выберите в меню **Configuration > System > SSH**, чтобы изменить параметры службы Secure Shell устройства NXC. С помощью этого экрана можно указать, из каких зон разрешено управление устройством NXC по протоколу SSH. Можно также указать, с каких IP-адресов разрешен доступ по этому протоколу.

Примечание: Если необходимо использовать для защищенных соединений протокол SSH, рекомендуется отключить протоколы Telnet и FTP.

Рисунок 186 Экран Configuration > System > SSH



Поля экрана описаны в следующей таблице.

Таблица 163 Экран Configuration > System > SSH

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы разрешить или запретить компьютеру с IP-адресом, совпадающим с IP-адресом в таблице **Service Control**, доступ к интерфейсу командной строки устройства NXC с использованием данной службы.
Version 1	Установите этот переключатель, если необходимо включить на устройстве NXC поддержку обеих версий SSH – 1 и 2. Если снять выделение с этого переключателя, устройство NXC будет использовать только протокол SSH версии 2.
Server Port	При необходимости можно изменить номер порта сервера для данной службы, но в этом случае придется использовать тот же номер порта для удаленного управления с использованием этой службы.
Server Certificate	Выберите сертификат, чей секретный ключ будет использоваться для идентификации устройства NXC при установке соединений SSH. Соответствующие сертификаты должны быть уже занесены в систему на экране **My Certificates**.
Service Control	Это поле указывает на то, с каких компьютеров и какие зоны устройства NXC будут доступны пользователям.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается доступ.
Action	Это поле указывает на то, разрешен ли (значение **Accept**) компьютеру с IP-адресом, указанным выше, доступ к зоне устройства NXC, указанной в поле **Zone**, или нет (значение **Deny**).
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.8.5 Пример защищенного подключения по Telnet с использованием SSH

В данном разделе описаны два примера использования интерфейса командной строки и клиентской программы SSH с графическим интерфейсом для получения удаленного доступа к устройству NXC. Этапы настройки и подключения аналогичны для большинства клиентских программ SSH. Более подробную информацию можно найти в руководстве пользователя к клиентской программе SSH.

28.8.5.1 Пример 1: Microsoft Windows

В данном разделе описано получение доступа к устройству NXC при помощи клиентской программы Secure Shell.

1 Запустите клиента SSH и введите данные для подключения (IP-адрес, номер порта) к устройству NXC.

2 Настройте на клиенте SSH прием соединений по протоколу SSH версии 1.

3 Появится окно с запросом на сохранение ключа хоста на компьютере. Нажмите на **Yes** для продолжения.

Рисунок 187 Пример 1, SSH: Сохраните ключ хоста

Введите пароль для входа на устройство NXC. После этого должен появиться экран интерфейса командной строки.

28.8.5.2 Пример 2: Linux

В данном разделе описано получение доступа к устройству NXC при помощи клиентской программы OpenSSH, которая поставляется в составе большинства дистрибутивов Linux.

1 Проверьте, запущена ли на устройстве NXC служба SSH.

Введите в приглашении терминала «`telnet 192.168.1.1 22`» и нажмите на [ENTER]. Компьютер попытается установить соединение с устройством NXC на порту 22 (с использованием IP-адреса по умолчанию 192.168.1.1).

Появится сообщение с указанием версии протокола SSH, поддерживаемой устройством NXC.

Рисунок 188 Пример 2, SSH: Проверка

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Введите «`ssh -1 192.168.1.1`». Данная команда заставляет компьютер установить соединение с устройством NXC с использованием протокола SSH версии 1. При первой попытке установить соединение с устройством NXC при помощи SSH появится сообщение с запросом на сохранение информации о хосте для устройства NXC. Введите «`yes`» и нажмите [ENTER].

Затем введите пароль для входа на устройство NXC.

Рисунок 189 Пример 2, SSH: Выполните вход в систему

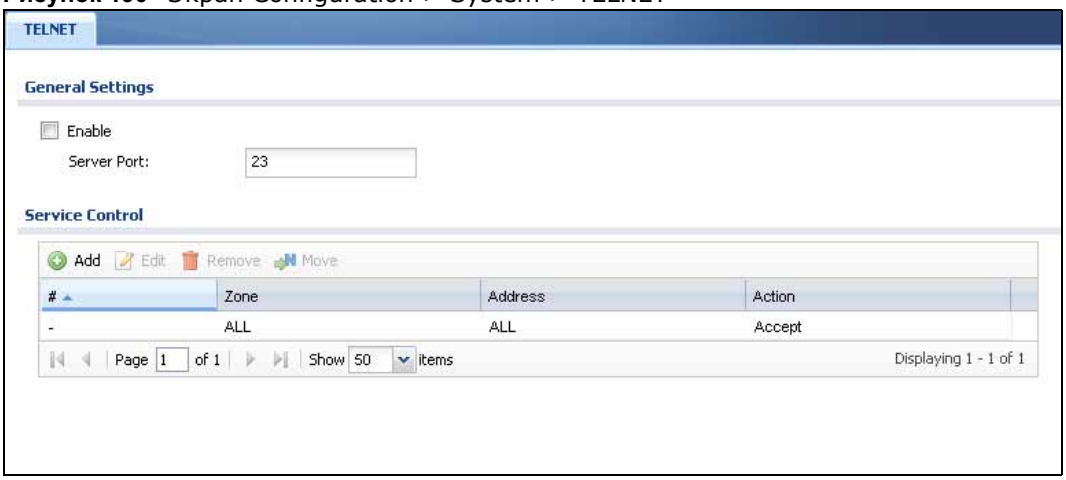
```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 После этого должен появиться экран интерфейса командной строки.

28.9 Протокол Telnet

С помощью протокола Telnet можно получить доступ к интерфейсу командной строки устройства NXC. Здесь можно указать, для каких зон и с каких IP-адресов разрешен доступ по протоколу Telnet. Выберите в меню **Configuration > System > TELNET**, чтобы открыть экран настройки удаленного доступа к устройству NXC по протоколу Telnet. С помощью этого экрана можно указать, из каких зон разрешен доступ по протоколу Telnet для управления устройством NXC. Можно также указать, с каких IP-адресов разрешен доступ по этому протоколу.

Рисунок 190 Экран Configuration > System > TELNET



Поля экрана описаны в следующей таблице.

Таблица 164 Экран Configuration > System > TELNET

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы разрешить или запретить компьютеру с IP-адресом, совпадающим с IP-адресом в таблице **Service Control**, доступ к интерфейсу командной строки устройства NXC с использованием данной службы.
Server Port	При необходимости можно изменить номер порта сервера для данной службы, но в этом случае придется использовать тот же номер порта для удаленного управления с использованием этой службы.
Service Control	Это поле указывает на то, с каких компьютеров и какие зоны устройства NXC будут доступны пользователям.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.

Таблица 164 Экран Configuration > System > TELNET (продолжение)

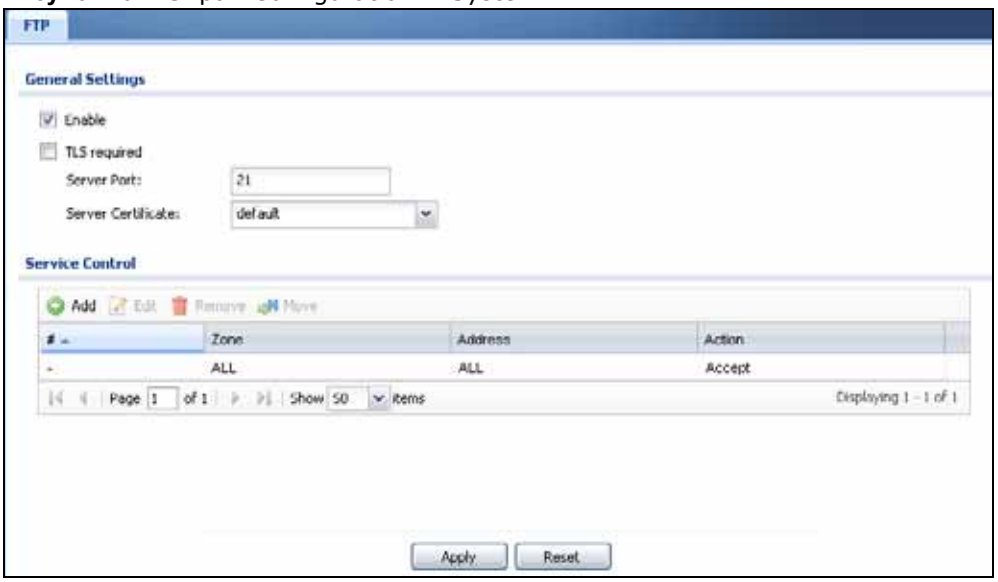
ПОЛЕ	ОПИСАНИЕ
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами. Запись с дефисом (-) вместо номера соответствует политике устройства NXC по умолчанию (чьи параметры менять нельзя). Устройство NXC применяет ее к трафику, который не соответствует ни одному из созданных правил. Данное правило не является редактируемым. Если необходимо применить другой алгоритм, создайте правило, критериям которого этот трафик будет соответствовать, и тогда устройство NXC не будет использовать для него политику по умолчанию.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается доступ.
Action	Это поле указывает на то, разрешен ли (значение **Accept**) компьютеру с IP-адресом, указанным выше, доступ к зоне устройства NXC, указанной в поле **Zone**, или нет (значение **Deny**).
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.10 Протокол FTP

С помощью протокола FTP можно выгружать и загружать встроенное программное обеспечение и файлы конфигурации на устройства NXC и с этих устройств. Чтобы использовать этот протокол, на компьютере должен быть установлен клиент FTP. Более подробную информацию о встроенном программном обеспечении и файлах конфигурации можно найти в гл. 30 на стр. 373.

Чтобы изменить настройки FTP на устройстве NXC, перейдите на вкладку **Configuration > System > FTP**. Откроется экран, изображенный на рисунке ниже. С помощью этого экрана можно указать, из каких зон разрешен доступ по протоколу FTP к устройству NXC. Можно также указать, с каких IP-адресов разрешен доступ по этому протоколу.

Рисунок 191 Экран Configuration > System > FTP



Поля экрана описаны в следующей таблице.

Таблица 165 Экран Configuration > System > FTP

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы разрешить или запретить компьютеру с IP-адресом, совпадающим с IP-адресом в таблице **Service Control**, доступ к устройству NXC с использованием данной службы.
TLS required	Установите этот переключатель, если необходимо использовать FTP поверх TLS (Transport Layer Security, протокол безопасности транспортного уровня) для шифрования данных в соединении. Эта опция включает TLS в качестве механизма безопасности для защиты клиентов и/или серверов FTP.
Server Port	При необходимости можно изменить номер порта сервера для данной службы, но в этом случае придется использовать тот же номер порта для удаленного управления с использованием этой службы.
Server Certificate	Выберите сертификат, чей секретный ключ будет использоваться для идентификации устройства NXC при установке соединений FTP. Соответствующие сертификаты должны быть уже занесены в систему на экране **My Certificates**.
Service Control	Это поле указывает на то, с каких компьютеров и какие зоны устройства NXC будут доступны пользователям.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.

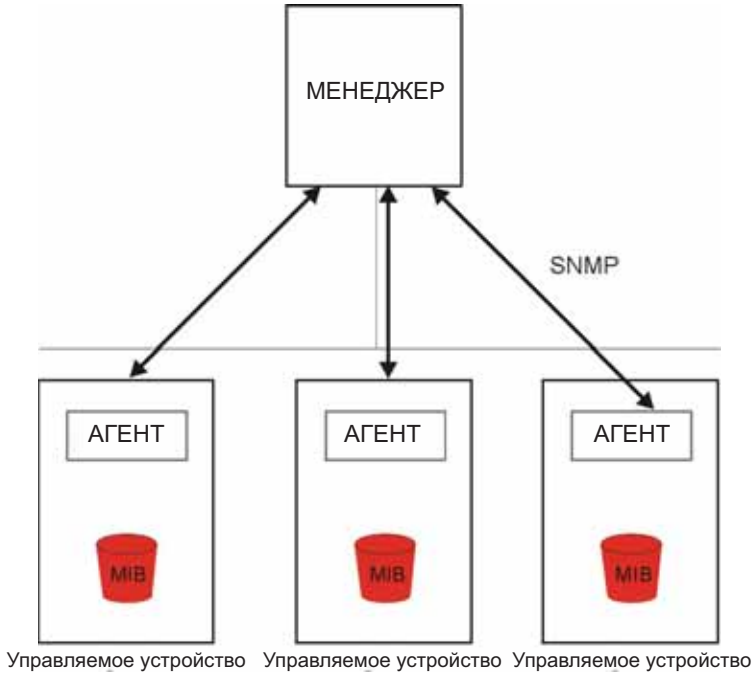
Таблица 165 Экран Configuration > System > FTP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами. Запись с дефисом (-) вместо номера соответствует политике устройства NXC по умолчанию (чьи параметры менять нельзя). Устройство NXC применяет ее к трафику, который не соответствует ни одному из созданных правил. Данное правило не является редактируемым. Если необходимо применить другой алгоритм, создайте правило, критериям которого этот трафик будет соответствовать, и тогда устройство NXC не будет использовать для него политику по умолчанию.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается доступ.
Action	Это поле указывает на то, разрешен ли (значение **Accept**) компьютеру с IP-адресом, указанным выше, доступ к зоне устройства NXC, указанной в поле **Zone**, или нет (значение **Deny**).
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.11 Протокол SNMP

SNMP (Simple Network Management Protocol, простой протокол управления сетью) – это протокол, который служит для обмена управляющей информацией между сетевыми устройствами. Устройство NXC может работать в качестве агента SNMP, что позволяет организовать управление и мониторинг работы устройства NXC по сети с управляющей станции. Устройство NXC поддерживает SNMP версии один (SNMPv1), версии два (SNMPv2c) и версии три (SNMPv3).Пример управления с помощью протокола SNMP показан на следующем рисунке.

Рисунок 192 Модель управления по протоколу SNMP



Сеть, управляемая посредством SNMP, включает в себя компоненты двух основных типов: агентов и менеджера.

Агент – это программный управляющий модуль, установленный на управляемом устройстве (устройстве NXC). Агент преобразует локальную управляющую информацию от управляемого устройства в форму, совместимую с протоколом SNMP. Менеджер – это консоль, с помощью которой администраторы сети выполняют функции управления сетью. На ней запускаются приложения, осуществляющие контроль и мониторинг управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют, какую информацию об устройстве необходимо собрать. Примеры переменных включают в себя количество полученных пакетов, состояние узлового порта и т.д. Хранилище управляемых объектов называется базой управляющей информации (MIB). Протокол SNMP позволяет менеджеру и агентам общаться между собой для получения доступа к этим объектам.

Сам по себе SNMP – это простой протокол типа «запрос/ответ» на основе модели «менеджер/агент». Менеджер отправляет запрос, а агент отвечает на него посредством следующих операций протокола:

- Get – Позволяет менеджеру получать объектные переменные от агента.
- GetNext – Позволяет менеджеру получить следующую объектную переменную из таблицы или списка, хранящегося у агента. В протоколе SNMPv1, когда менеджер хочет получить от агента все элементы таблицы, он инициирует операцию Get и сразу за ней серию операций GetNext.
- Set – Позволяет менеджеру устанавливать значения объектных переменных, хранящихся у агента.
- Trap – Используется агентом для оповещения менеджера о каких-либо событиях.

28.11.1 Поддерживаемые базы MIB

Устройство NXC поддерживает базы MIB II, формат которых описан в документах RFC-1213 и RFC-1215. Кроме того, устройство NXC поддерживает частные базы MIB (zywall.mib и zyxel-zywall-ZLD-Common.mib) для сбора информации об использовании процессорных ресурсов и оперативной памяти. Базы управляющей информации MIB позволяют администраторам собирать статистические сведения и отслеживать состояние и производительность сетевых устройств. Загрузить базы MIB для устройства NXC можно с сайта www.zyxel.com.

28.11.2 Команды Trap протокола SNMP

Устройство NXC будет отправлять «ловушки» менеджеру SNMP при наступлении одного из перечисленных ниже событий.

Таблица 166 Команды Trap протокола SNMP

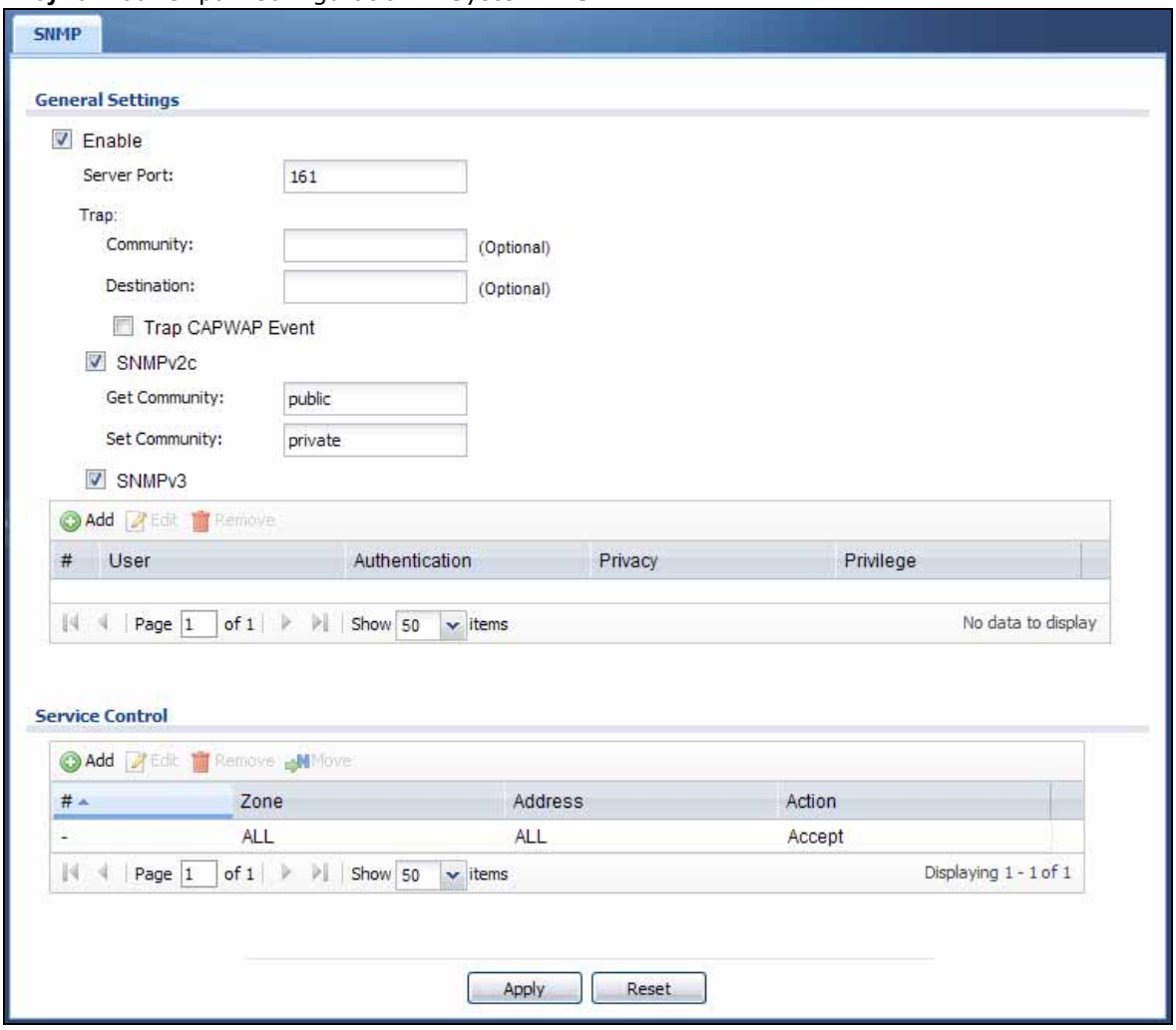
МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
Cold Start	1.3.6.1.6.3.1.1.5.1	Эта «ловушка» отправляется при реинициализации агентом собственных таблиц конфигурации.
linkDown	1.3.6.1.6.3.1.1.5.3	Эта команда Trap отправляется при разрыве Ethernet-соединения.
linkUp	1.3.6.1.6.3.1.1.5.4	Эта команда Trap отправляется при установлении Ethernet-соединения.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	Эта команда Trap отправляется при получении SNMP-запроса от хостов, не прошедших аутентификацию.

28.11.3 Настройка SNMP

Устройство NXC может работать в качестве агента SNMP, что позволяет организовать управление и мониторинг работы устройства NXC по сети с управляющей станции.

Чтобы изменить настройки SNMP на устройстве NXC, перейдите на вкладку **Configuration > System > SNMP**. Откроется экран, изображенный на рисунке ниже. Этот экран позволяет настроить параметры SNMP для устройства, в том числе список зон, с которых разрешен доступ к устройству NXC по протоколу SNMP. Кроме того, можно указать, с каких IP-адресов разрешен доступ к устройству, а также настроить профили пользователей, которые определяют разрешенный доступ по протоколу SNMPv3.

Рисунок 193 Экран Configuration > System > SNMP



Поля экрана описаны в следующей таблице.

Таблица 167 Экран Configuration > System > SNMP

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы разрешить или запретить компьютеру с IP-адресом, совпадающим с IP-адресом в таблице **Service Control**, доступ к устройству NXC с использованием данной службы.
Server Port	При необходимости можно изменить номер порта сервера для данной службы, но в этом случае придется использовать тот же номер порта для удаленного управления с использованием этой службы.
Trap	
Community	Введите значение для команды trap community – это пароль, отправляемый менеджеру SNMP с каждой «ловушкой». Значение по умолчанию public разрешает все запросы.
Destination	Введите IP-адрес менеджера SNMP, на который будут отправляться «ловушки» SNMP.
Trap CAPWAP Event	Выберите эту опцию, чтобы устройство NXC отправляло «ловушку» менеджеру SNMP при подключении и отключении управляемой точки доступа от устройства NXC.
SNMPv2c	Выберите эту опцию, если необходимо разрешить менеджерам SNMP, использующим протокол SNMPv2c, доступ к устройству NXC.
Get Community	Введите значение для команды get community – это пароль для входящих запросов Get и GetNext от станции управления. Значение по умолчанию public разрешает все запросы.
Set Community	Введите значение Set Community – это пароль для входящих запросов Set от станции управления. Значение по умолчанию private разрешает все запросы.
SNMPv3	Выберите эту опцию, если необходимо разрешить менеджерам SNMP, использующим протокол SNMPv3, доступ к устройству NXC.
Add	Нажатие на этот значок позволяет создать новую запись.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
#	Это порядковый номер профиля пользователя SNMPv3.
User	Имя пользователя, для которого создан данный пользовательский профиль SNMPv3.
Authentication	Это поле указывает на тип аутентификации, который должен использовать пользователь SNMPv3 для доступа к устройству NXC с использованием профиля пользователя SNMPv3.
Privacy	Это поле указывает на тип шифрования, который должен использовать пользователь SNMPv3 для доступа к устройству NXC с использованием профиля пользователя SNMPv3.
Privilege	Это поле указывает на то, какой тип доступа – только на чтение или на чтение и запись – имеет пользователь SNMPv3 к устройству NXC с использованием профиля пользователя SNMPv3.
Service Control	Это поле указывает на то, с каких компьютеров и какие зоны устройства NXC будут доступны пользователям.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.

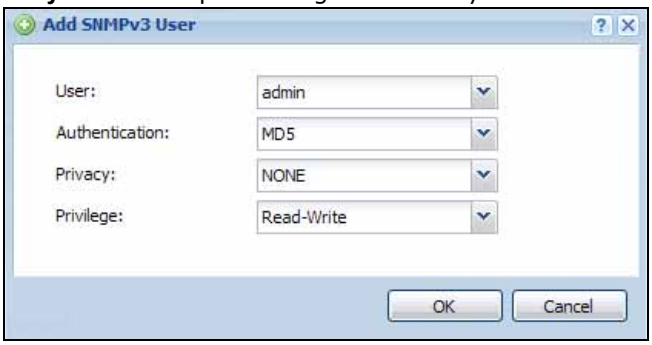
Таблица 167 Экран Configuration > System > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Move	Чтобы изменить позицию записи в нумерованном списке, выберите нужное правило и нажмите кнопку **Move**. На экране появится поле для ввода позиции, в которую можно перенести эту запись. Введите нужное значение и нажмите клавишу [ENTER], чтобы перенести правило на указанную позицию.
#	Это порядковый номер правила управления службами. Запись с дефисом (-) вместо номера соответствует политике устройства NXC по умолчанию (чьи параметры менять нельзя). Устройство NXC применяет ее к трафику, который не соответствует ни одному из созданных правил. Данное правило не является редактируемым. Если необходимо применить другой алгоритм, создайте правило, критериям которого этот трафик будет соответствовать, и тогда устройство NXC не будет использовать для него политику по умолчанию.
Zone	Это зона на устройстве NXC, к которой пользователю разрешен или запрещен доступ.
Address	Это имя объекта IP-адреса (или IP-адресов), с которого разрешается или запрещается доступ.
Action	Это поле указывает на то, разрешен ли (значение **Accept**) компьютеру с IP-адресом, указанным выше, доступ к зоне устройства NXC, указанной в поле **Zone**, или нет (значение **Deny**).
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.11.4 Создание или редактирование профиля пользователя SNMPv3

С помощью этого экрана можно создать новый профиль пользователя SNMPv3 или отредактировать существующий. Чтобы перейти к этому экрану, выберите в меню **Configuration > System > SNMP** и нажмите на открывшемся экране кнопку **Add** или выберите имеющийся профиль пользователя SNMPv3 из списка и нажмите кнопку **Edit**.

Рисунок 194 Экран Configuration > System > SNMP > Add



Поля экрана описаны в следующей таблице.

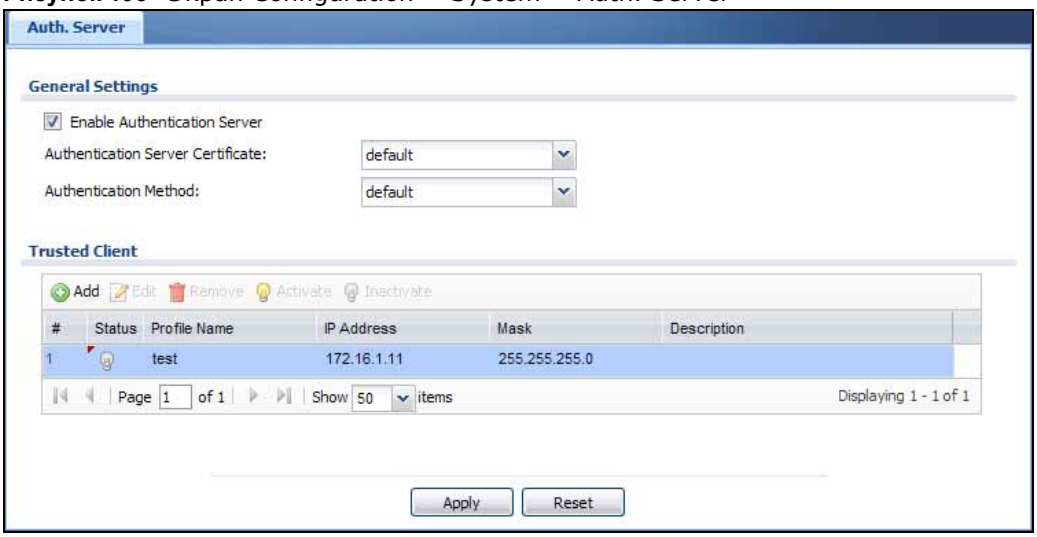
Таблица 168 Экран Configuration > System > SNMP

ПОЛЕ	ОПИСАНИЕ
User Name	Выберите имя пользователя, для учетной записи которого создан данный пользовательский профиль SNMPv3.
Authentication	Выберите тип аутентификации, который должен использовать пользователь SNMPv3 для подключения к устройству NXC с использованием данного профиля пользователя SNMPv3. Выберите **MD5**, если необходимо выполнять шифрование пароля пользователя SNMPv3 с помощью алгоритма MD5 для аутентификации. Выберите **SHA**, если необходимо выполнять шифрование пароля пользователя SNMPv3 с помощью алгоритма SHA для аутентификации.
Privacy	Выберите тип шифрования, который должен использовать пользователь SNMPv3 для подключения к устройству NXC с использованием данного профиля пользователя SNMPv3. Выберите **NONE**, чтобы не шифровать соединения SNMPv3. Выберите **DES**, чтобы шифровать соединения SNMPv3 с использованием шифра DES. Выберите **AES**, чтобы шифровать соединения SNMPv3 с использованием шифра AES.
Privilege	Укажите, какой тип доступа будет иметь данный пользователь SNMPv3 к устройству NXC с использованием данного профиля пользователя SNMPv3 – только на чтение (read-only) или на чтение – запись (read and write).
OK	Нажмите кнопку **OK**, чтобы сохранить изменения в конфигурации устройства NXC.
Cancel	Нажмите кнопку **Cancel**, чтобы закрыть текущий экран без сохранения изменений.

28.12 Сервер аутентификации

Устройство NXC может выполнять функции сервера RADIUS, обменивающегося сообщениями с клиентом RADIUS, например, точкой доступа, для аутентификации и авторизации пользователей. Перейдите на вкладку **Configuration > System > Auth. Server**. Откроется экран, изображенный на рисунке ниже. На этом экране можно включить функцию сервера аутентификации для устройства NXC и указать IP-адрес клиента RADIUS.

Рисунок 195 Экран Configuration > System > Auth. Server



Поля экрана описаны в следующей таблице.

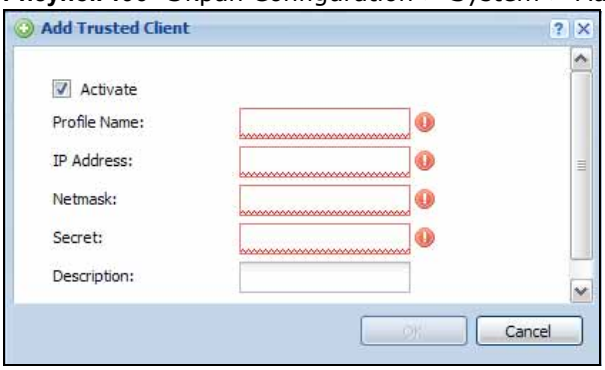
Таблица 169 Экран Configuration > System > Auth. Server

ПОЛЕ	ОПИСАНИЕ
Enable	Установите этот переключатель, чтобы включить функцию сервера RADIUS на устройстве NXC.
Authentication Server Certificate	Выберите сертификат, чей секретный ключ будет использоваться для идентификации устройства NXC перед клиентом RADIUS. Соответствующие сертификаты должны быть уже занесены в систему на экране **My Certificates**.
Authentication Method	Выберите метод аутентификации, если хотя бы один такой метод был создан на экране **Configuration > Object > Auth. Method**.
Service Control	Это поле указывает на то, с каких компьютеров и какие зоны устройства NXC будут доступны пользователям.
Add	Нажатие на этот значок позволяет создать новую запись. Выберите запись и нажмите кнопку **Add**, чтобы создать новую запись сразу после выбранной записи.
Edit	Дважды щелкните по записи или выберите ее и нажмите кнопку **Edit**, чтобы изменить настройки записи.
Remove	Для удаления записи необходимо выбрать ее и нажать на **Remove**. Перед удалением записи устройство NXC запрашивает подтверждение операции. Обратите внимание, что при выполнении этого действия все последующие записи смещаются вверх.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
#	Порядковый номер записи.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Profile Name	В этом поле отображается имя, которое присвоено данному профилю.
IP Address	Это IP-адрес клиента RADIUS, которому разрешено обмениваться сообщениями с устройством NXC.
Mask	Это маска подсети клиента RADIUS.
Description	Это описание клиента RADIUS.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.12.1 Создание/редактирование доверенного клиента RADIUS

Выберите в меню **Configuration > System > Auth. Server**, чтобы открыть экран **Auth. Server**. Нажмите на пиктограмму **Add** или пиктограмму **Edit**, чтобы открыть следующий экран. С помощью этого экрана можно создать новую запись или отредактировать существующую.

Рисунок 196 Экран Configuration > System > Auth. Server > Add/Edit



Поля экрана описаны в следующей таблице.

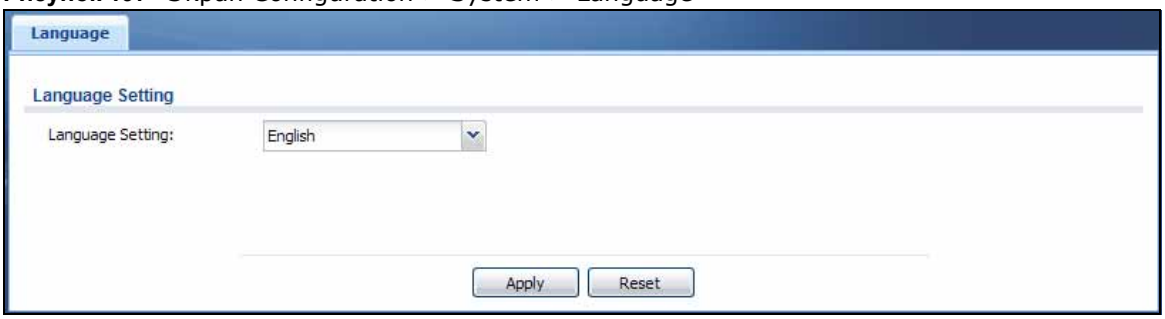
Таблица 170 Экран Configuration > System > Auth. Server > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Activate	Установите этот переключатель, чтобы активировать этот профиль.
Profile Name	Введите имя-описание (до 31 алфавитно-цифровых символов) для идентификации.
IP Address	Укажите IP-адрес клиента RADIUS, которому разрешен обмен сообщениями с устройством NXC.
Netmask	Введите маску подсети для клиента RADIUS.
Secret	Введите пароль (до 64 алфавитно-цифровых символов), который будет служить общим ключом для устройства NXC и клиентом RADIUS. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере аутентификации и устройстве NXC.
Description	Введите описание для каждого из серверов, если требуется. В поле можно ввести до 60 печатных символов ASCII.
OK	Нажмите кнопку **OK**, чтобы сохранить изменения.
Cancel	Нажмите кнопку **Cancel**, чтобы отменить изменения.

28.13 Язык интерфейса

Выберите в меню **Configuration > System > Language**, чтобы открыть этот экран. С помощью этого экрана можно выбрать язык интерфейса для экранов Web-конфигуратора устройства NXC.

Рисунок 197 Экран Configuration > System > Language



Поля экрана описаны в следующей таблице.

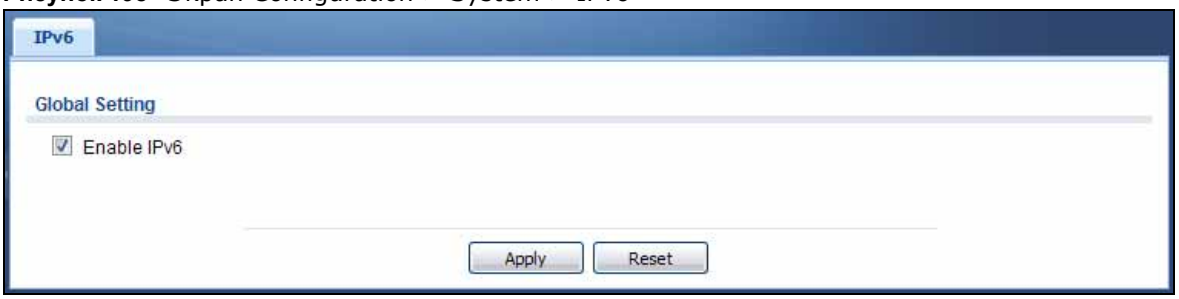
Таблица 171 Экран Configuration > System > Language

ПОЛЕ	ОПИСАНИЕ
Language Setting	Выберите язык интерфейса для экранов Web-конфигуратора устройства NXC. Для того, чтобы увидеть интерфейс экрана на новом языке, необходимо перезапустить браузер.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

28.14 Протокол IPv6

Выберите в меню **Configuration > System > IPv6**, чтобы открыть следующий экран. С помощью этого экрана можно включить поддержку протокола IPv6 на устройстве NXC.

Рисунок 198 Экран Configuration > System > IPv6



Поля экрана описаны в следующей таблице.

Таблица 172 Экран Configuration > System > IPv6

ПОЛЕ	ОПИСАНИЕ
Enable IPv6	Выберите эту опцию, чтобы включить поддержку протокола IPv6 на устройстве NXC и сделать настройки IPv6 доступными на экранах, поддерживаемых соответствующими функциями, таких, как **Configuration > Network > Interface > Ethernet** и **VLAN**. Если снять выделение с этого переключателя, устройство NXC будет отбрасывать все пакеты IPv6.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

29

Журналы и отчеты

29.1 Обзор

С помощью системных экранов можно настроить параметры ежедневных отчетов и журналов.

29.1.1 О чем рассказывается в этой главе

- Экран **Email Daily Report** (разд. 29.2 на стр. 357) позволяет указать, как и куда следует отправлять ежедневные отчеты, и какие именно отчеты нужно отправлять.
- Экраны **Log Settings** (разд. 29.3 на стр. 359) позволяет указать, какие журналы следует отправлять по электронной почте, куда и с какой периодичностью.

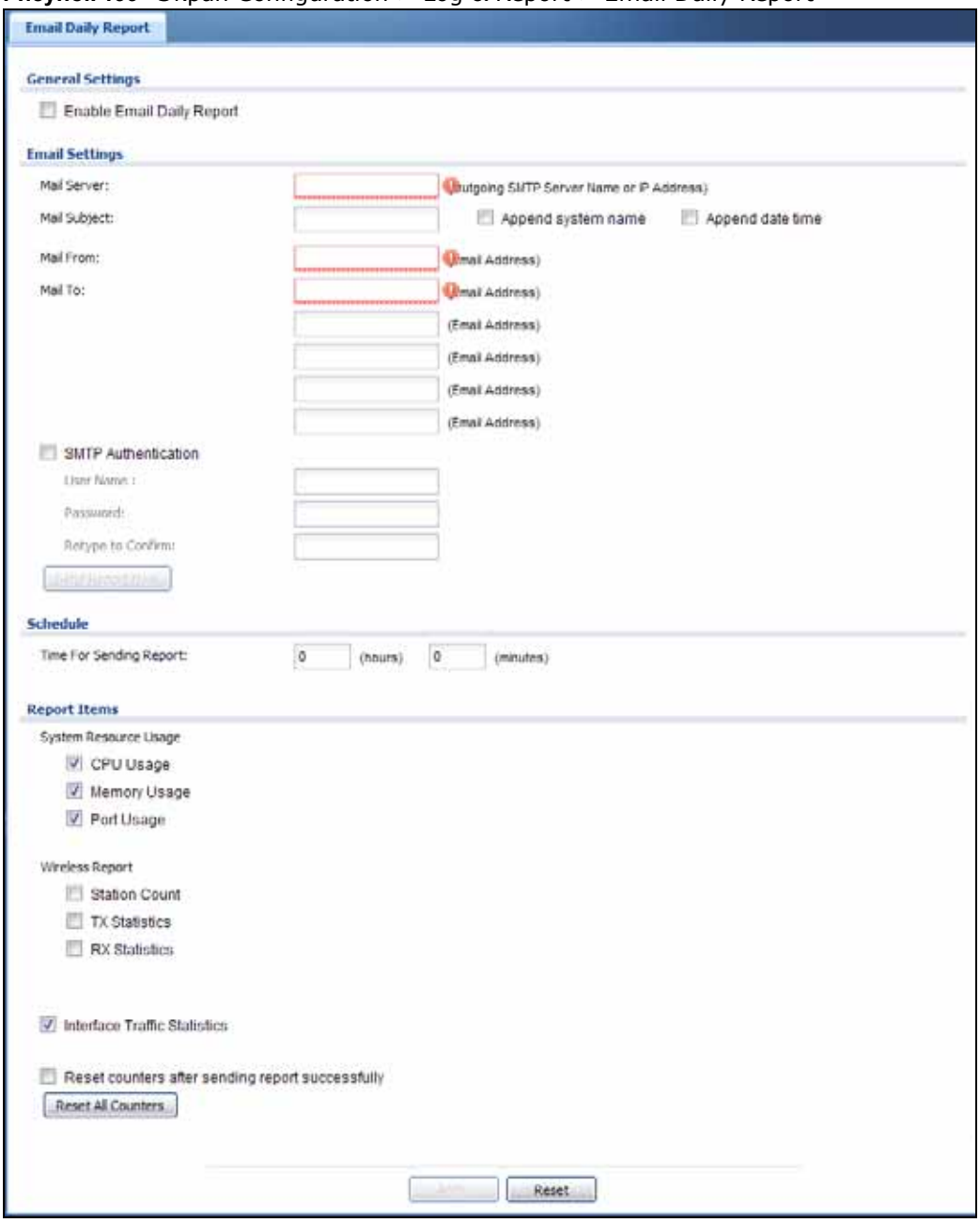
29.2 Экран Email Daily Report

С помощью этого экрана можно запустить или остановить сбор данных, а также ознакомиться с разнообразной статистикой по трафику, передаваемому через устройство NXC.

Примечание: Сбор данных может привести к уменьшению пропускной способности устройства NXC в плане передачи трафика.

Выберите в меню **Configuration > Log & Report > Email Daily Report**, чтобы открыть следующий экран. С помощью этого экрана можно настроить ежедневную отправку по электронной почте устройством NXC статистики о работе системы.

Рисунок 199 Экран Configuration > Log & Report > Email Daily Report



Поля экрана описаны в следующей таблице.

Таблица 173 Экран Configuration > Log & Report > Email Daily Report

ПОЛЕ	ОПИСАНИЕ
Enable Email Daily Report	Установите этот переключатель, чтобы включить ежедневную рассылку отчетов по электронной почте.
Mail Server	Введите имя или IP-адрес SMTP-сервера исходящей почты.
Mail Subject	Введите тему для исходящего почтового сообщения. Выберите опцию **Append system name**, если необходимо добавить к теме сообщения системное имя устройства NXC. Выберите опцию **Append date time**, если необходимо добавить к теме сообщения системные дату и время устройства NXC.

Таблица 173 Экран Configuration > Log & Report > Email Daily Report (продолжение)

ПОЛЕ	ОПИСАНИЕ
Mail From	Введите адрес электронной почты, с которого будет осуществляться рассылка. Этот адрес используется в ответах.
Mail To	Введите адрес (или адреса) электронной почты, на которые будет осуществляться рассылка.
SMTP Authentication	Установите этот переключатель, если SMTP-сервер требует обязательного указания имени пользователя и пароля.
User Name	Это поле действует при выборе опции **SMTP Authentication**. Введите имя пользователя, которое нужно передать SMTP-серверу при отправке журнала по электронной почте.
Password	Это поле действует при выборе опции **SMTP Authentication**. Введите пароль, которое нужно передать SMTP-серверу при отправке журнала по электронной почте.
Retype to Confirm	Введите еще раз новый пароль для подтверждения.
Send Report Now	Нажмите эту кнопку, чтобы устройство NXC отправило ежедневный отчет сейчас.
Time for sending report	Выберите время суток (часы и минуты) для отправки журнала по электронной почте. Используйте 24-часовую нотацию.
Report Items	Выберите информацию, которую нужно включить в отчет. Выберите опцию **Reset counters after sending report successfully**, если необходимо видеть статистику только за последние сутки.
Reset All Counters	Нажмите эту кнопку, чтобы убрать все накопленные данные для отчета и начать отсчет по всем счетчикам заново, с нуля.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в системе NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

29.3 Экран Log Settings

С помощью этих экранов настраивают параметры сообщений журнала и оповещений. Сообщение журнала хранит информацию для просмотра (например, на вкладке **View Log**) или отправки по электронной почте в рамках регулярной рассылки. Оповещение отправляется по почте немедленно. Как правило, оповещения используют для событий, которые требуют более пристального внимания, например, системных ошибок или попыток взлома.

Устройство NXC ведет системный журнал и поддерживает профили электронной почты и работу с удаленными серверами syslog. Системный журнал можно просмотреть на вкладке **View Log**, профили электронной почты используют для отправки сообщений журнала по электронной почте на указанные адреса, а четыре оставшихся журнала хранятся на указанных серверах syslog.

На вкладке **Log Settings** можно указать, какую информацию следует сохранять в каждом из журналов. Для системного журнала можно указать, какие сообщения журнала нужно отправлять по электронной почте, куда и с какой периодичностью.

На этой вкладке также можно указать, какие события должны генерировать оповещения, и куда следует отправлять эти оповещения.

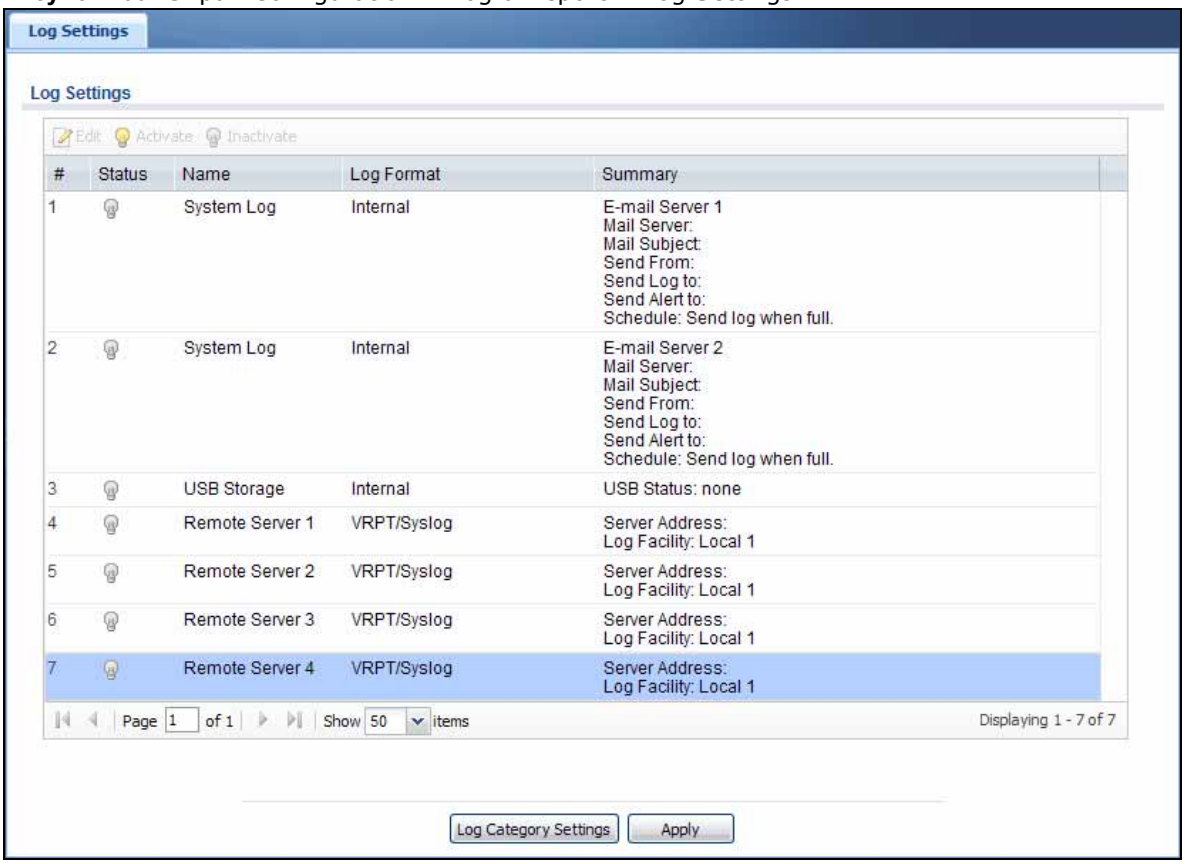
Экран **Log Settings Summary** содержит сводную информацию обо всех настройках. Для работы с детализированными настройками (такими, как категории журналов, адреса

электронной почты, имена серверов и т.п.) любых журналов можно использовать экран **Log Settings Edit**. Если необходимо изменить список событий, которые попадают в каждый из журналов, это можно сделать на экране **Log Category Settings** одновременно для всех журналов.

29.3.1 Сводный экран Log Settings

Чтобы перейти к этому экрану, выберите в меню **Configuration > Log & Report > Log Settings**.

Рисунок 200 Экран Configuration > Log & Report > Log Settings



Поля экрана описаны в следующей таблице.

Таблица 174 Экран Configuration > Log & Report > Log Settings

ПОЛЕ	ОПИСАНИЕ
Edit	Перейти к изменению параметров определенной записи можно двойным щелчком на ней, а также выбрав соответствующую запись и нажав на **Edit**.
Activate	Для включения записи необходимо выбрать ее и нажать на **Activate**.
Inactivate	Для отключения записи необходимо выбрать ее и нажать на **Inactivate**.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным журналом.
Status	Эта пиктограмма подсвечивается, если запись активна, и затемнена, если запись неактивна.
Name	Это поле отображает имя журнала (системного журнала или журнала на одном из удаленных серверов).

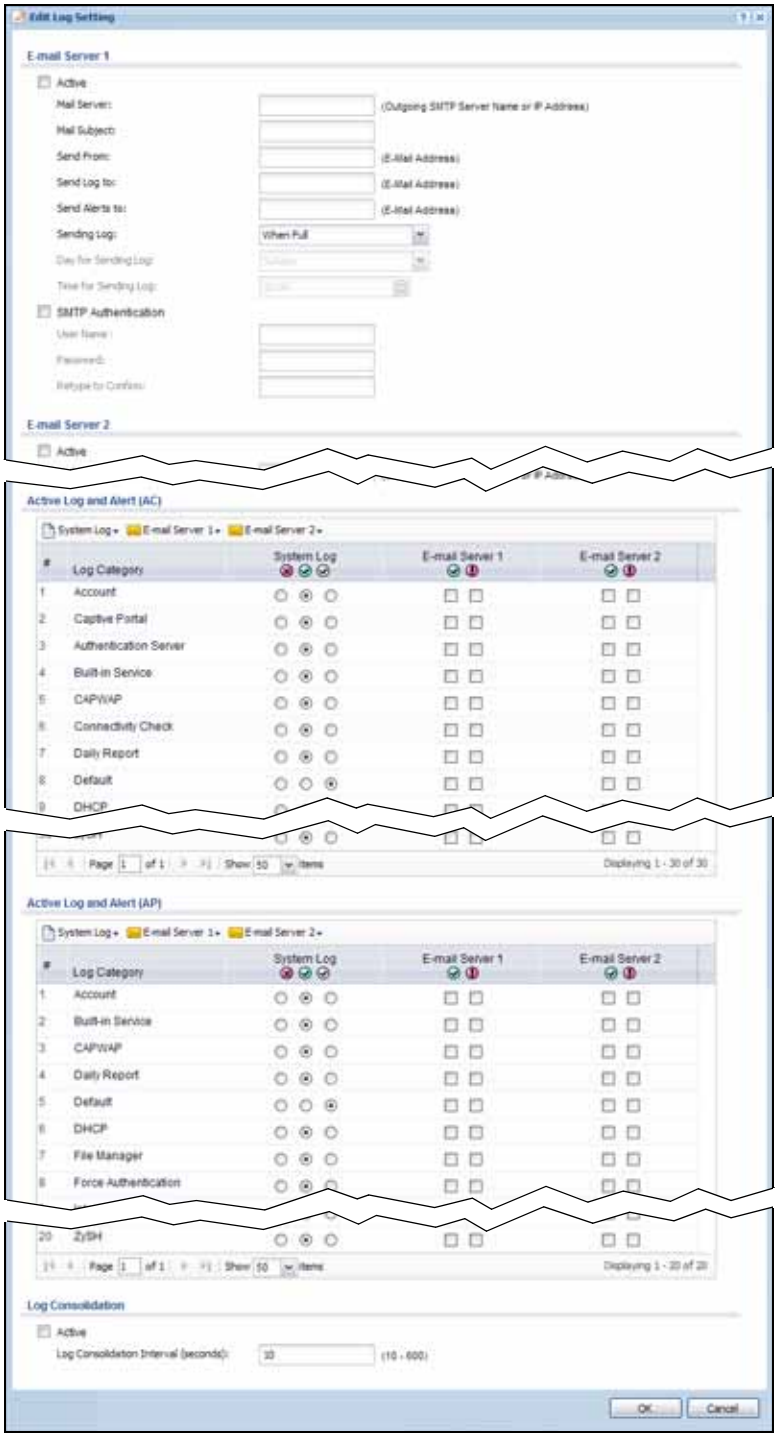
Таблица 174 Экран Configuration > Log & Report > Log Settings (продолжение)

ПОЛЕ	ОПИСАНИЕ
Log Format	Это поле указывает на формат журнала. **Internal** – системный журнал; этот журнал можно просмотреть на вкладке **View Log**. **VRPT/Syslog** – Vantage Report от ZyXEL, формат, совместимый с форматом syslog. **CEF/Syslog** – Common Event Format, формат, совместимый с форматом syslog.
Summary	Это поле содержит сводную информацию о настройках для каждого журнала.
Log Category Settings	Нажмите эту кнопку, чтобы открыть журнал **Log Category Settings**.
Apply	Нажмите эту кнопку, чтобы сохранить сделанные изменения (активировать и деактивировать журналы) и применить их.

29.3.2 Экран Edit System Log Settings

Этот экран позволяет управлять детальными настройками для каждой записи в системном журнале (в том числе – профилями электронной почты). Перейдите на экран **Log Settings Summary** и нажмите на пиктограмму **Edit** для системного журнала.

Рисунок 201 Экран Configuration > Log & Report > Log Settings > Edit (System Log)



Поля экрана описаны в следующей таблице.

Таблица 175 Экран Configuration > Log & Report > Log Settings > Edit (System Log)

ПОЛЕ	ОПИСАНИЕ
E-Mail Server 1/2	
Active	Установите этот переключатель, чтобы включить функцию отправки сообщений журнала и оповещений в соответствии с настройками, заданными в этом разделе. Укажите в разделе **Active Log and Alert**, какие виды сообщений должны попадать в журнал, а какие – в оповещения.
Mail Server	Введите имя или IP-адрес SMTP-сервера исходящей почты.
Mail Subject	Введите тему для исходящего почтового сообщения.
Send From	Введите адрес электронной почты, с которого будет осуществляться рассылка. Этот адрес используется в ответах.
Send Log To	Введите адрес электронной почты, на который будет осуществляться рассылка.
Send Alerts To	Введите адрес электронной почты, на который должны рассылаться оповещения.
Sending Log	Укажите, с какой периодичностью должна осуществляться рассылка журналов. Возможные варианты: **When Full** (При заполнении), **Hourly and When Full** (Ежечасно и при заполнении), **Daily and When Full** (Ежедневно и при заполнении) и **Weekly and When Full** (Еженедельно и при заполнении).
Day for Sending Log	Это поле становится доступным при выборе опции еженедельной рассылки журналов. Выберите день недели, в который необходимо выполнять рассылку журналов.
Time for Sending Log	Это поле становится доступным при выборе опции еженедельной или ежедневной рассылки журналов. Выберите время суток (часы и минуты) для отправки журнала по электронной почте. Используйте 24-часовую нотацию.
SMTP Authentication	Установите этот переключатель, если SMTP-сервер требует обязательного указания имени пользователя и пароля.
User Name	Это поле действует при выборе опции **SMTP Authentication**. Введите имя пользователя, которое нужно передать SMTP-серверу при отправке журнала по электронной почте.
Password	Это поле действует при выборе опции **SMTP Authentication**. Введите пароль, которое нужно передать SMTP-серверу при отправке журнала по электронной почте.
Retype to Confirm	Введите еще раз новый пароль для подтверждения.
Active Log and Alert	
System log	Воспользуйтесь выпадающим списком **System Log**, чтобы изменить настройки для всех категорий журналов. **disable all logs** (красный символ X) – не заносить никакую информацию для любых категорий системного журнала и не отправлять никакие сообщения из журналов по электронной почте на почтовые серверы 1 и 2. **enable normal logs** (зеленая «галочка») – создавать сообщения и оповещения для всех категорий системного журнала. Если на почтовых серверах 1 или 2 включены нормальные журналы, то устройство NXC будет отправлять им сообщения журналов по электронной почте. **enable normal logs and debug logs** (желтая «галочка») – создавать сообщения, оповещения и отладочную информацию для всех категорий. Устройство NXC не рассылает по электронной почте отладочную информацию, даже если эта опция включена.

Таблица 175 Экран Configuration > Log & Report > Log Settings > Edit (System Log)

ПОЛЕ	ОПИСАНИЕ
E-mail Server 1	Воспользуйтесь выпадающим списком **E-Mail Server 1**, чтобы изменить настройки почтовой рассылки журналов на почтовом сервера 1 для всех категорий журналов. Опция disable all logs, выбранная в выпадающем списке **System Log**, имеет больший приоритет по сравнению с настройками для почтового сервера 1. **enable normal logs** (зеленая «галочка») – отправлять сообщения журнала по электронной почте для всех категорий на почтовый сервер 1. **enable alert logs** (красный восклицательный знак) – отправлять оповещения для всех категорий на почтовый сервер 1.
E-mail Server 2	Воспользуйтесь выпадающим списком **E-Mail Server 2**, чтобы изменить настройки почтовой рассылки журналов на почтовом сервера 2 для всех категорий журналов. Опция disable all logs, выбранная в выпадающем списке **System Log**, имеет больший приоритет по сравнению с настройками для почтового сервера 2. **enable normal logs** (зеленый переключатель) – отправлять сообщения журнала по электронной почте для всех категорий на почтовый сервер 2. **enable alert logs** (красный восклицательный знак) – отправлять оповещения для всех категорий на почтовый сервер 2.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным адресом.
Log Category	Это поле показывает все категории сообщений. Здесь отображается то же значение, которое было указано в полях **Display** и **Category** на вкладке **View Log**. Категория **Default** включает в себя отладочные сообщения, генерируемые программным обеспечением с открытым исходным кодом.
System log	Выберите события, которые необходимо заносить в журнал, по категориям журналов (**Log Category**). Существует три варианта: **disable all logs** (красный символ X) – не заносить в журнал никакой информации из этой категории **enable normal logs** (зеленая «галочка») – создавать сообщения в журнале и оповещения для этой категории **enable normal logs and debug logs** (желтая «галочка») – создавать сообщения в журнале, оповещения и отладочную информацию для этой категории; устройство NXC не рассылает отладочную информацию по электронной почте, даже если эта опция включена.
E-mail Server 1	Укажите, должны ли события каждой категории попадать в сообщения журнала, если для этой категории предусмотрена рассылка по электронной почте (зеленая «галочка») и/или рассылка оповещений (красный восклицательный знак) в соответствии с настройками на почтовом сервере **E-Mail Server 1**. Устройство NXC не рассылает по электронной почте отладочную информацию, даже если она попадает в системный журнал **System log**.
E-mail Server 2	Укажите, должны ли события каждой категории попадать в сообщения журнала, если для этой категории предусмотрена рассылка по электронной почте (зеленая «галочка») и/или рассылка оповещений (красный восклицательный знак) в соответствии с настройками на почтовом сервере **E-Mail Server 2**. Устройство NXC не рассылает по электронной почте отладочную информацию, даже если она попадает в системный журнал **System log**.
Log Consolidation	

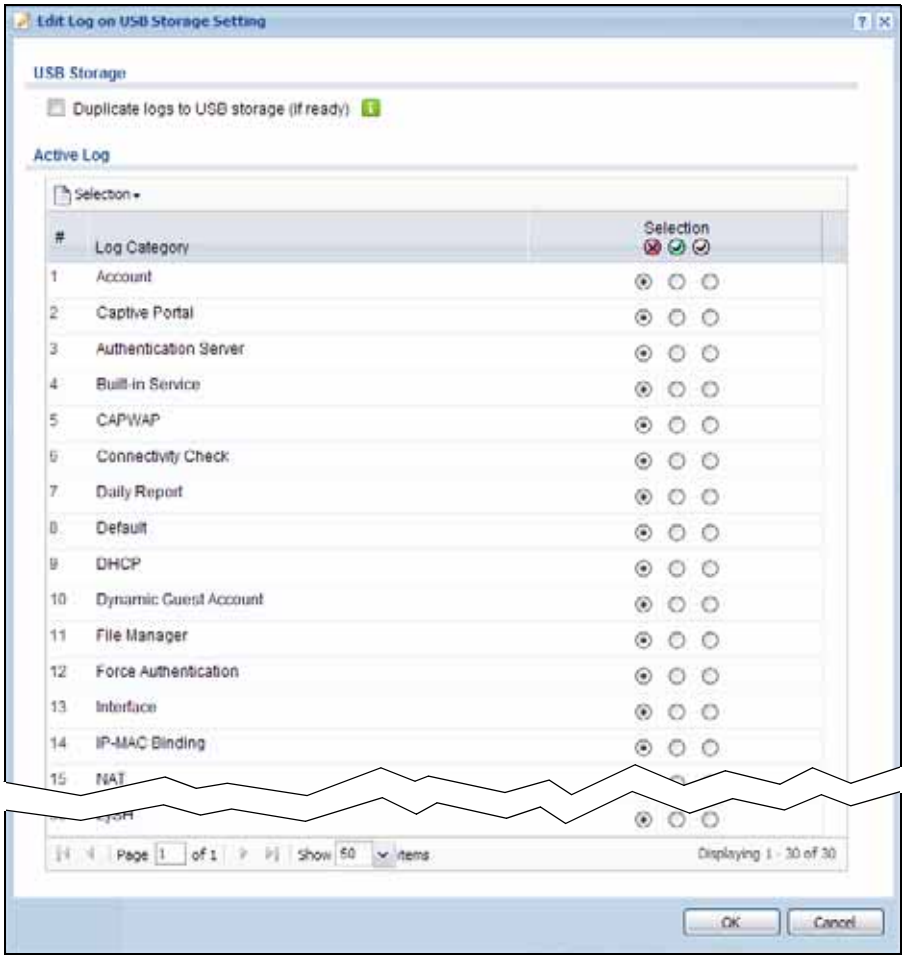
Таблица 175 Экран Configuration > Log & Report > Log Settings > Edit (System Log)

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы активировать функцию консолидации журналов. Функция консолидации журналов агрегирует два и более сообщений в журнале, которые созданы в пределах указанного интервала консолидации журналов (**Log Consolidation Interval**). На вкладке **View Log** текст «[count=*x*]», где *x* – это количество исходных сообщений в журнале, прибавляется в конце значения в поле **Message** при агрегировании нескольких сообщений из журнала.
Log Consolidation Interval	Укажите, с какой периодичностью (в секундах) необходимо консолидировать информацию в журналах. Если одно и то же сообщение встречается в журнале два и более раз, то оно агрегируется в одно сообщение с текстом «[count=*x*]», где *x* – это количество исходных сообщений в журнале, добавленным к содержимому поля **Message**.
OK	Нажмите эту кнопку, чтобы сохранить изменения и вернуться к предыдущему экрану.
Cancel	Нажмите эту кнопку, чтобы вернуться к предыдущему экрану без сохранения изменений.

29.3.3 Экран Edit USB Storage Log Settings

Экран **Edit Log on USB Storage Setting** позволяет управлять детальными настройками сохранения журналов на подключенный USB-накопитель. Перейдите на экран **Log Settings Summary** и нажмите на пиктограмму **Edit** для USB-накопителя.

Рисунок 202 Экран Configuration > Log & Report > Log Settings > Edit (USB Storage)



Поля экрана описаны в следующей таблице.

Таблица 176 Экран Configuration > Log & Report > Log Settings > Edit (USB Storage)

ПОЛЕ	ОПИСАНИЕ
Duplicate logs to USB storage (if ready)	Выберите эту опцию, чтобы устройство NXC сохраняло копию системных журналов на подключенный USB-накопитель. Перечень сообщений, которые нужно включить в сохраняемую копию, определяется настройками в разделе **Active Log**.
Active Log	
Selection	Воспользуйтесь выпадающим списком **Selection**, чтобы изменить настройки для всех категорий журналов. **disable all logs** (красный символ X) – не рассылать журналы с удаленных серверов для всех категорий журналов. **enable normal logs** (зеленая «галочка») – рассылать сообщения журналов и оповещения с удаленных серверов для всех категорий журналов. **enable normal logs and debug logs** (желтая «галочка») – рассылать сообщения журналов, оповещения и отладочную информацию для всех категорий журналов.
#	В этом поле содержится порядковое значение, не связанное с каким-либо параметром.
Log Category	Это поле показывает все категории сообщений. Категория **Default** включает в себя отладочные сообщения, генерируемые программным обеспечением с открытым исходным кодом.

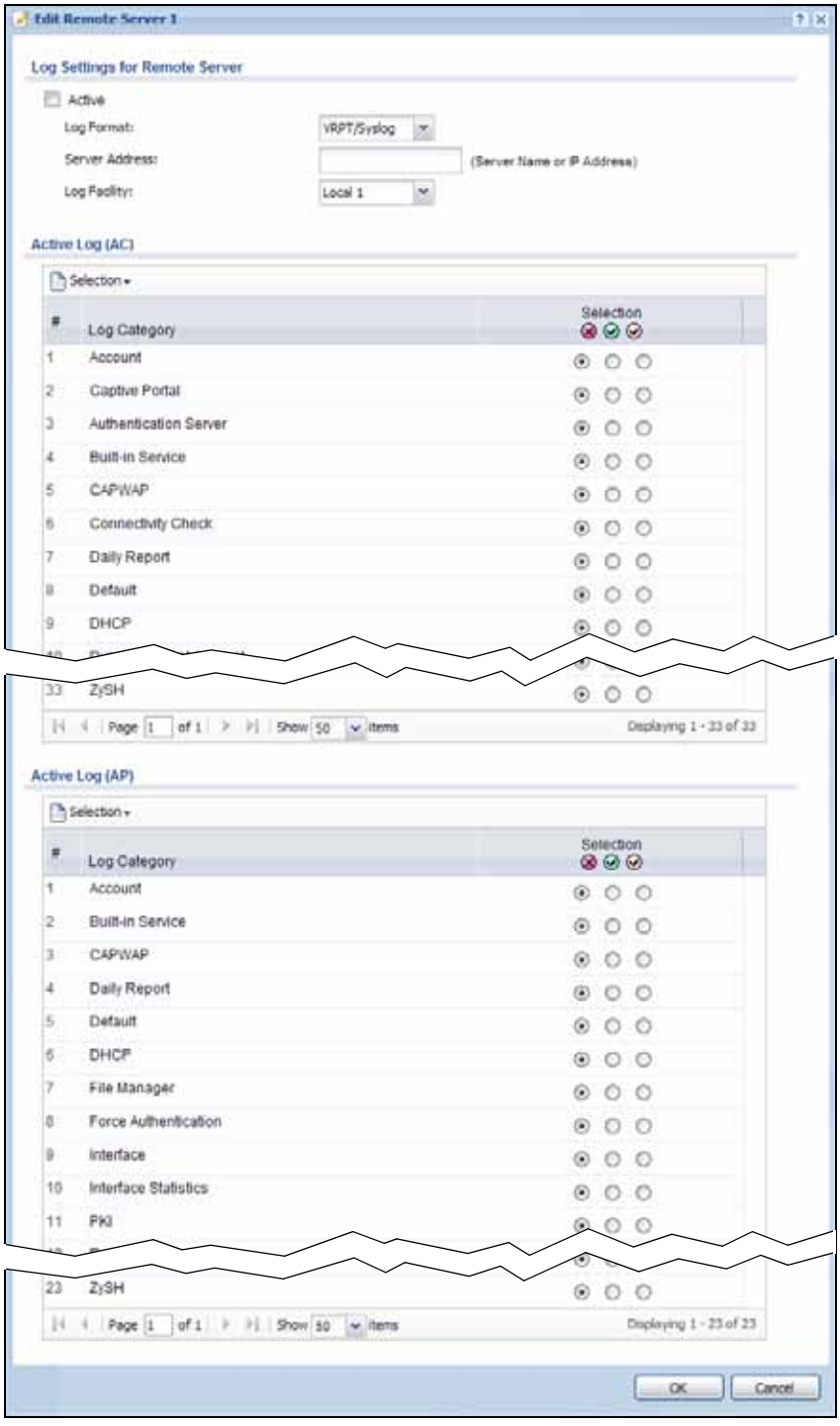
Таблица 176 Экран Configuration > Log & Report > Log Settings > Edit (USB Storage)

ПОЛЕ	ОПИСАНИЕ
Selection	Укажите, какую информацию следует заносить в журнал для каждой категории журналов **Log Category** (кроме **All Logs**; см. ниже). Возможные варианты: **disable all logs** (красный символ X) – не заносить в журнал никакой информации из этой категории **enable normal logs** (зеленая «галочка») – заносить в журнал обычную информацию и оповещения для данной категории **enable normal logs and debug logs** (желтая «галочка») – заносить в журнал обычную информацию, оповещения и отладочную информацию для данной категории
OK	Нажмите эту кнопку, чтобы сохранить изменения и вернуться к предыдущему экрану.
Cancel	Нажмите эту кнопку, чтобы вернуться к предыдущему экрану без сохранения изменений.

29.3.4 Экран Edit Remote Server Log Settings

Этот экран позволяет управлять настройками всех журналов на удаленных серверах (syslog). Перейдите на экран **Log Settings Summary** и нажмите на пиктограмму **Edit** для соответствующего удаленного сервера.

Рисунок 203 Экран Configuration > Log & Report > Log Settings > Edit (Remote Server)



Поля экрана описаны в следующей таблице.

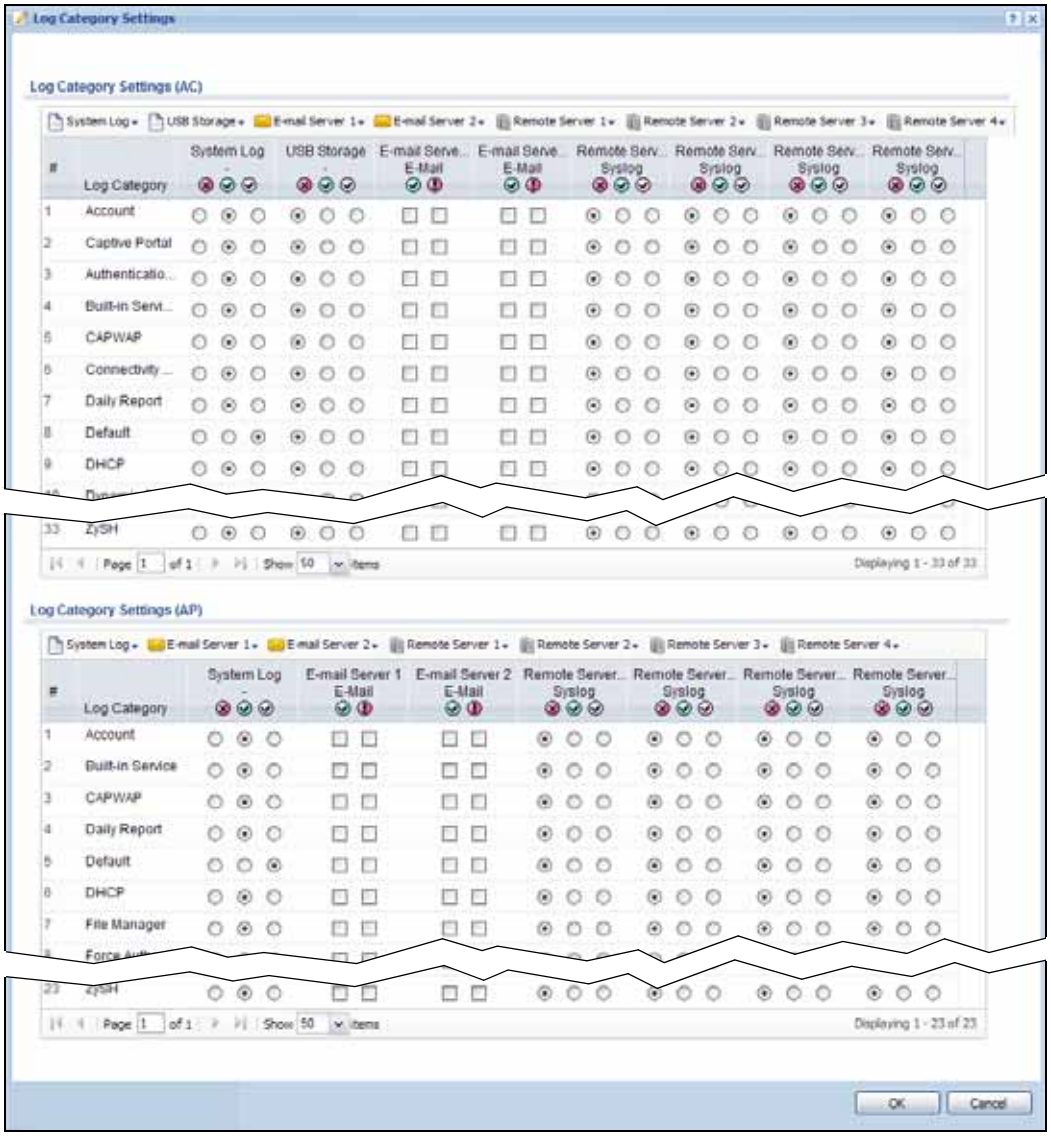
Таблица 177 Экран Configuration > Log & Report > Log Settings > Edit (Remote Server)

ПОЛЕ	ОПИСАНИЕ
Log Settings for Remote Server	
Active	Установите этот переключатель, если необходимо включить отправку информации из журнала в соответствии с настройками, заданными в этом разделе. Перечень сообщений, которые должны попадать в журнал, определяется настройками в разделе **Active Log**.
Log Format	Это поле показывает формат информации в журнале. Оно доступно только для чтения. **VRPT/Syslog** – Vantage Report от ZyXEL, формат, совместимый с форматом syslog. **CEF/Syslog** – Common Event Format, формат, совместимый с форматом syslog.
Server Address	Введите имя или IP-адрес сервера syslog, на который нужно отправлять информацию из журнала.
Log Facility	Выберите функцию распределения журналов (log facility). Функция распределения журналов позволяет заносить сообщения журнала в разные файлы на сервере syslog. Более подробную информацию об этом можно найти в документации к программному обеспечению syslog.
Active Log	
Selection	Воспользуйтесь выпадающим списком **Selection**, чтобы изменить настройки для всех категорий журналов. **disable all logs** (красный символ X) – не рассылать журналы с удаленных серверов для всех категорий журналов. **enable normal logs** (зеленая «галочка») – рассылать сообщения журналов и оповещения с удаленных серверов для всех категорий журналов. **enable normal logs and debug logs** (желтая «галочка») – рассылать сообщения журналов, оповещения и отладочную информацию для всех категорий журналов.
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным адресом.
Log Category	Это поле показывает все категории сообщений. Здесь отображается то же значение, которое было указано в полях **Display** и **Category** на вкладке **View Log**. Категория **Default** включает в себя отладочные сообщения, генерируемые программным обеспечением с открытым исходным кодом.
Selection	Укажите, какую информацию следует заносить в журнал для каждой категории журналов **Log Category** (кроме **All Logs**; см. ниже). Возможные варианты: **disable all logs** (красный символ X) – не заносить в журнал никакой информации из этой категории **enable normal logs** (зеленая «галочка») – заносить в журнал обычную информацию и оповещения для данной категории **enable normal logs and debug logs** (желтая «галочка») – заносить в журнал обычную информацию, оповещения и отладочную информацию для данной категории
OK	Нажмите эту кнопку, чтобы сохранить изменения и вернуться к предыдущему экрану.
Cancel	Нажмите эту кнопку, чтобы вернуться к предыдущему экрану без сохранения изменений.

29.3.5 Экран Log Category Settings

Этот экран позволяет просматривать и одновременно изменять перечень информации, которую нужно включать в системный журнал, переносить на USB-накопитель, в профили электронной почты и на удаленные серверы. Другие настройки на этом экране изменить нельзя (например, параметры, определяющие, куда и с какой периодичностью должна рассылаться информация из журналов, или имена удаленных серверов). Чтобы открыть этот экран, перейдите на экран **Log Settings Summary** и нажмите кнопку **Log Category Settings**.

Рисунок 204 Экран Configuration > Log & Report > Log Settings > Log Category Settings



Этот экран предлагает различные варианты просмотра перечня сообщений, которые должны попадать в каждый журнал и каждое оповещение. (Категория **Default** включает в себя отладочные сообщения, генерируемые программным обеспечением с открытым исходным кодом).

Поля экрана описаны в следующей таблице.

Таблица 178 Экран Configuration > Log & Report > Log Settings > Log Category Settings

ПОЛЕ	ОПИСАНИЕ
System log	Воспользуйтесь выпадающим списком **System Log**, чтобы изменить настройки для всех категорий журналов. **disable all logs** (красный символ X) – не заносить никакую информацию для любых категорий системного журнала и не отправлять никакие сообщения из журналов по электронной почте на почтовые серверы 1 и 2. **enable normal logs** (зеленая «галочка») – создавать сообщения и оповещения для всех категорий системного журнала. Если на почтовых серверах 1 или 2 включены нормальные журналы, то устройство NXC будет отправлять им сообщения журналов по электронной почте. **enable normal logs and debug logs** (желтая «галочка») – создавать сообщения, оповещения и отладочную информацию для всех категорий. Устройство NXC не рассылает по электронной почте отладочную информацию, даже если эта опция включена.
USB Storage	Воспользуйтесь выпадающим списком **USB Storage**, чтобы изменить настройки сохранения журналов на подключенном USB-накопителе. **disable all logs** (красный символ X) – не копировать никакую информацию из журналов любой категории на подключенный USB-накопитель. **enable normal logs** (зеленая «галочка») – создавать сообщения в журналах и оповещения для всех категорий журналов и сохранять их на подключенном USB-накопителе. **enable normal logs and debug logs** (желтая «галочка») – создавать сообщения в журналах, оповещения и отладочную информацию для всех категорий журналов и сохранять их на подключенном USB-накопителе.
E-mail Server 1	Воспользуйтесь выпадающим списком **E-Mail Server 1**, чтобы изменить настройки почтовой рассылки журналов на почтовом сервера 1 для всех категорий журналов. Опция disable all logs, выбранная в выпадающем списке **System Log**, имеет больший приоритет по сравнению с настройками для почтового сервера 1. **enable normal logs** (зеленая «галочка») – отправлять сообщения журнала по электронной почте для всех категорий на почтовый сервер 1. **enable alert logs** (красный восклицательный знак) – отправлять оповещения для всех категорий на почтовый сервер 1.
E-mail Server 2	Воспользуйтесь выпадающим списком **E-Mail Server 2**, чтобы изменить настройки почтовой рассылки журналов на почтовом сервера 2 для всех категорий журналов. Опция disable all logs, выбранная в выпадающем списке **System Log**, имеет больший приоритет по сравнению с настройками для почтового сервера 2. **enable normal logs** (зеленый переключатель) – отправлять сообщения журнала по электронной почте для всех категорий на почтовый сервер 2. **enable alert logs** (красный восклицательный знак) – отправлять оповещения для всех категорий на почтовый сервер 2.
Remote Server 1~4	Для каждого удаленного сервера выберите соответствующую опцию в выпадающем списке **Selection**, чтобы изменить настройки для всех категорий журналов. **disable all logs** (красный символ X) – не рассылать журналы с удаленных серверов для всех категорий журналов. **enable normal logs** (зеленая «галочка») – рассылать сообщения журналов и оповещения с удаленных серверов для всех категорий журналов. **enable normal logs and debug logs** (желтая «галочка») – рассылать сообщения журналов, оповещения и отладочную информацию для всех категорий журналов.

Таблица 178 Экран Configuration > Log & Report > Log Settings > Log Category Settings

ПОЛЕ	ОПИСАНИЕ
#	В этом поле содержится порядковое значение, не связанное с каким-либо конкретным адресом.
Log Category	Это поле показывает все категории сообщений. Здесь отображается то же значение, которое было указано в полях **Display** и **Category** на вкладке **View Log**. Категория **Default** включает в себя отладочные сообщения, генерируемые программным обеспечением с открытым исходным кодом.
System log	Выберите события, которые необходимо заносить в журнал, по категориям журналов (**Log Category**). Существует три варианта: **disable all logs** (красный символ X) – не заносить в журнал никакой информации из этой категории **enable normal logs** (зеленая «галочка») – создавать сообщения в журнале и оповещения для этой категории **enable normal logs and debug logs** (желтая «галочка») – создавать сообщения в журнале, оповещения и отладочную информацию для этой категории; устройство NXC не рассылает отладочную информацию по электронной почте, даже если эта опция включена.
USB Storage	Укажите, для каких категорий журналов необходимо сохранять информацию из журналов на подключенный USB-накопитель. Существует три варианта: **disable all logs** (красный символ X) – не заносить в журнал никакой информации из этой категории **enable normal logs** (зеленая «галочка») – сохранять сообщения в журнале и оповещения для этой категории **enable normal logs and debug logs** (желтая «галочка») – сохранять сообщения в журнале, оповещения и отладочную информацию для этой категории.
E-mail Server 1 E-mail	Укажите, должны ли события каждой категории попадать в сообщения журнала, если для этой категории предусмотрена рассылка по электронной почте (зеленая «галочка») и/или рассылка оповещений (красный восклицательный знак) в соответствии с настройками на почтовом сервере **E-Mail Server 1**. Устройство NXC не рассылает по электронной почте отладочную информацию, даже если она попадает в системный журнал **System log**.
E-mail Server 2 E-mail	Укажите, должны ли события каждой категории попадать в сообщения журнала, если для этой категории предусмотрена рассылка по электронной почте (зеленая «галочка») и/или рассылка оповещений (красный восклицательный знак) в соответствии с настройками на почтовом сервере **E-Mail Server 2**. Устройство NXC не рассылает по электронной почте отладочную информацию, даже если она попадает в системный журнал **System log**.
Remote Server 1~4	Для каждого удаленного сервера укажите, какую информацию следует заносить в журнал для каждой категории журналов **Log Category** (кроме **All Logs**; см. ниже). Возможные варианты: **disable all logs** (красный символ X) – не заносить в журнал никакой информации из этой категории **enable normal logs** (зеленая «галочка») – заносить в журнал обычную информацию и оповещения для данной категории **enable normal logs and debug logs** (желтая «галочка») – заносить в журнал обычную информацию, оповещения и отладочную информацию для данной категории
OK	Нажмите эту кнопку, чтобы сохранить изменения и вернуться к предыдущему экрану.
Cancel	Нажмите эту кнопку, чтобы вернуться к предыдущему экрану без сохранения изменений.

30

Диспетчер файлов

30.1 Обзор

Настройки устройства NXC сохраняются в файлах конфигурации. Сценарии командной строки – это файлы команд, которые можно хранить на устройстве NXC и выполнять по мере необходимости. Можно применить файл конфигурации или запустить сценарий командной строки без перезагрузки устройства NXC. На устройстве NXC можно сохранить несколько файлов конфигурации и файлов сценариев командной строки. Файлы конфигурации и сценарии командной строки можно изменять в текстовом редакторе и выгружать на устройство NXC. Файлы конфигурации имеют расширение .conf, сценарии командной строки – расширение .zysh.

30.1.1 О чем рассказывается в этой главе

- Экран **Configuration File** (разд. 30.2 на стр. 376) позволяет сохранять файлы конфигурации и выбирать для них имена. Файлы конфигурации можно загружать с устройства и выгружать на устройство.
- Экран **Firmware Package** (разд. 30.3 на стр. 379) содержит сведения о текущей версии встроенного программного обеспечения и позволяет выгружать встроенное программное обеспечение на устройство NXC.
- Экран **Shell Script** (разд. 30.4 на стр. 382) позволяет сохранять, именовать, загружать, выгружать и запускать файлы сценариев командной строки.

30.1.2 Что необходимо знать

Описанные ниже определения и понятия могут пригодиться при чтении этой главы.

Файлы конфигурации и сценарии командной строки

При применении файла конфигурации устройство NXC использует заводские настройки по умолчанию для всех параметров, которые отсутствуют в файле конфигурации. При выполнении сценария командной строки устройством NXC выполняются только команды из этого сценария. Прочие настройки не изменяются.

Эти файлы имеют одинаковый синтаксис, который эквивалентен последовательному запуску команд интерфейса командной строки вручную. Пример показан ниже.

Рисунок 205 Файл конфигурации / сценарий командной строки: Пример

```
# войти в режим настроек
configure terminal
# изменить пароль администратора
username admin password 4321 user-type admin
# настроить параметры интерфейса ge3
interface ge3
ip address 172.16.37.240 255.255.255.0
ip gateway 172.16.37.254 metric 1
exit
# создать адресные объекты для удаленного управления
# использовать адресную группу, если нужно перейти к удаленному управлению
позже
address-object TW_SUBNET 172.16.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# включить доступ по протоколу Telnet (по умолчанию этот протокол не включен
в отличие от остальных служб)
ip telnet server
# открыть межсетевой экран WLAN-NXC для TW_TEAM для удаленного управления
firewall WLAN NXC insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

Несмотря на то, что файлы конфигурации и сценарии командной строки имеют одинаковый синтаксис, устройство NXC применяет файлы конфигурации и выполняет сценарии командной строки по-разному. Ниже объясняется, в чем состоит разница.

Таблица 179 Файлы конфигурации и сценарии командной строки на устройстве NXC

Файлы конфигурации (.conf)	Сценарии командной строки (.zysh)
• Выполняют сброс до конфигурации по умолчанию. • Переходят в режим настройки командной строки (CLI **Configuration**). • Выполняют команды в файле конфигурации.	• Переходят в привилегированный режим командной строки (CLI **Privilege**). • Выполняют команды сценария командной строки.

Пример, приведенный выше, необходимо запустить как сценарий командной строки, поскольку первая команда выполняется в привилегированном (**Privilege**) режиме. Если убрать первую команду, то этот пример нужно будет запустить как файл конфигурации, поскольку остальные команды выполняются в режиме настройки (**Configuration**).

Комментарии в файлах конфигурации и сценариях командной строки

В файле конфигурации или сценарии командной строки введите в начале строки символ «#» или «!», и тогда устройство NXC будет трактовать эту строку как комментарий.

В файлах конфигурации или сценариях командной строки можно использовать оператор «exit» или командную строку, состоящую из единственного символа «!», для вывода устройства NXC из субкомандного режима.

Примечание: Оператор «exit» или символ «!» должны следовать за субкомандами, чтобы вывести устройство NXC из субкомандного режима.

Строка 3 в следующем примере осуществляет выход из субкомандного режима.

```
interface ge1
ip address dhcp
!
```

Строки 1 и 3 в следующем примере являются комментариями, а строка 4 выполняет выход из субкомандного режима.

```
!
interface ge1
# этот интерфейс – клиент DHCP
!
```

Строки 1 и 2 являются комментариями. Строка 5 выполняет выход из субкомандного режима.

```
! это от Джо
# 2008/04/05
interface ge1
ip address dhcp
!
```

Ошибки в файлах конфигурации и сценариях командной строки

В процессе применения файла конфигурации или выполнения сценария командной строки устройство NXC обрабатывает соответствующий файл построчно. Устройство NXC проверяет первую строку и выполняет ее, если ошибок не обнаружено. Затем переходит к следующей строке. При обнаружении ошибки устройство NXC прекращает применять файл конфигурации или выполнять сценарий командной строки и генерирует журнал.

Имеется возможность изменить способ применения файла конфигурации или выполнения сценария командной строки. Добавьте в файл конфигурации или сценарий командной строки строку `setenv stop-on-error off`. Теперь устройство NXC будет игнорировать любые ошибки в файле конфигурации или сценарии командной строки и выполнит все корректные команды. При этом устройство NXC, как и прежде, запишет все ошибки в журнал.

30.2 Экран Configuration File

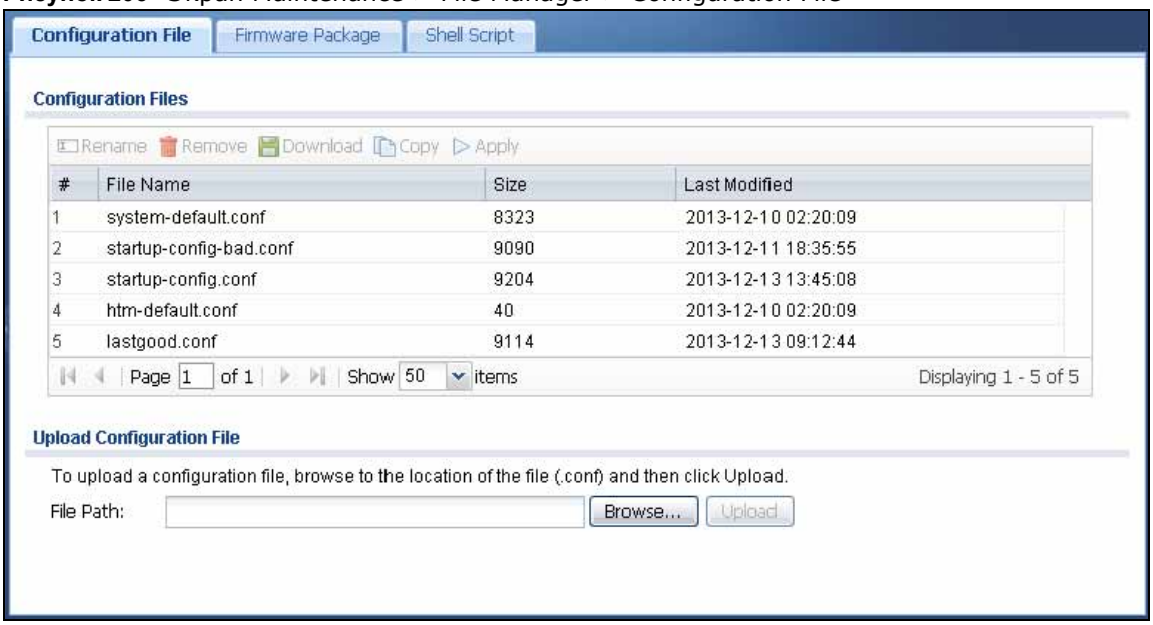
Чтобы открыть этот экран, выберите в меню **Maintenance > File Manager > Configuration File**. Экран **Configuration File** служит для сохранения, запуска и именования файлов конфигурации. Можно загружать файлы конфигурации с устройства NXC на компьютер и выгружать файлы конфигурации с компьютера на устройство NXC.

После того, как выполнены все настройки на устройстве NXC, и оно работает надлежащим образом, настоятельно рекомендуется сделать резервную копию файла конфигурации перед тем, как вносить дальнейшие изменения в конфигурацию. Резервная копия файла конфигурации может пригодиться, если потребуется вернуться к предшествующим настройкам.

Применение файла конфигурации при перезагрузке

- Если при перезапуске устройства NXC (через интерфейс администрирования или в результате отключения – включения питания) отсутствует файл startup-config.conf, то устройство NXC использует файл конфигурации **system-default.conf** с настройками для устройства NXC по умолчанию.
- Если файл **startup-config.conf** есть, устройство NXC проверяет его на наличие ошибок и применяет его. Если ошибок не обнаружено, устройство NXC использует этот файл и копирует его в файл конфигурации под названием **lastgood.conf**, используемый в качестве резервного. Если ошибки найдены, устройство NXC генерирует журнал, копирует файл конфигурации **startup-config.conf** в файл конфигурации **startup-config-bad.conf** и пробует воспользоваться существующим файлом конфигурации **lastgood.conf**. Если файла конфигурации **lastgood.conf** нет, или в нем тоже есть ошибки, устройство NXC применяет файл конфигурации **system-default.conf**.
- Имеется возможность изменить способ применения файла **startup-config.conf**. Добавьте в него команду `setenv-startup stop-on-error off`. Устройство NXC будет игнорировать любые ошибки в файле **startup-config.conf** и применит все корректные команды. При этом устройство NXC, как и прежде, запишет все ошибки в журнал.

Рисунок 206 Экран Maintenance > File Manager > Configuration File



Не выключайте устройство NXC во время выгрузки файла конфигурации.

Поля экрана описаны в следующей таблице.

Таблица 180 Экран Maintenance > File Manager > Configuration File

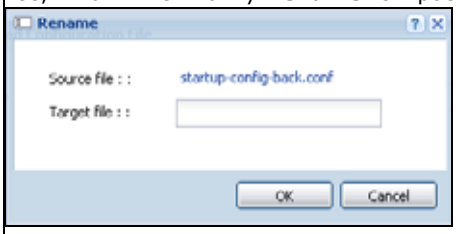
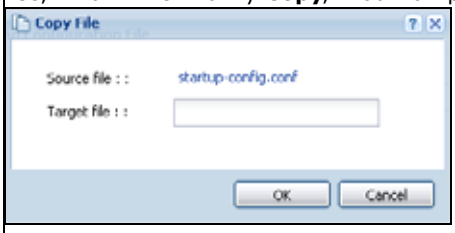
ПОЛЕ	ОПИСАНИЕ
Rename	С помощью этой кнопки можно изменить название файла конфигурации на устройстве NXC. Переименовать можно только файлы конфигурации, сохраненные вручную. Файлы **lastgood.conf**, **system-default.conf** и **startup-config.conf** переименованию не подлежат. Кроме того, нельзя назвать какой-либо файл конфигурации именем другого файла конфигурации на устройстве NXC. Щелкните по строке, соответствующей нужному файлу конфигурации, чтобы выбрать ее, и нажмите кнопку **Rename**. Откроется окно **Rename File**.  Укажите новое имя для файла конфигурации. Длина имени должна быть не более 25 символов (допускается использование символов a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Нажмите кнопку **OK**, чтобы сохранить копию, или кнопку **Cancel, чтобы закрыть этот экран, не сохраняя копию файла конфигурации**.
Remove	**Щелкните по строке, соответствующей нужному файлу конфигурации, чтобы выбрать ее, и нажмите кнопку Remove**, чтобы удалить его с устройства NXC. Удалить можно только файлы конфигурации, сохраненные вручную. Файлы **system-default.conf**, **startup-config.conf** и **lastgood.conf** удалению не подлежат. Появится всплывающее окно с предложением подтвердить удаление файла конфигурации. Нажмите кнопку **OK**, чтобы удалить файл конфигурации, или кнопку **Cancel, чтобы закрыть экран, не удаляя файл конфигурации**.
Download	Щелкните по строке, соответствующей нужному файлу конфигурации, чтобы выбрать ее, и нажмите кнопку **Download**, чтобы сохранить файл конфигурации на компьютер.
Copy	С помощью этой кнопки можно сохранить копию файла конфигурации на устройстве NXC. Щелкните по строке, соответствующей нужному файлу конфигурации, чтобы выбрать ее, и нажмите кнопку **Copy**, чтобы открыть экран **Copy File**.  Укажите имя для копии файла конфигурации. Длина имени должна быть не более 25 символов (допускается использование символов a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Нажмите кнопку **OK**, чтобы сохранить копию, или кнопку **Cancel, чтобы закрыть этот экран, не сохраняя копию файла конфигурации**.

Таблица 180 Экран Maintenance > File Manager > Configuration File (продолжение)

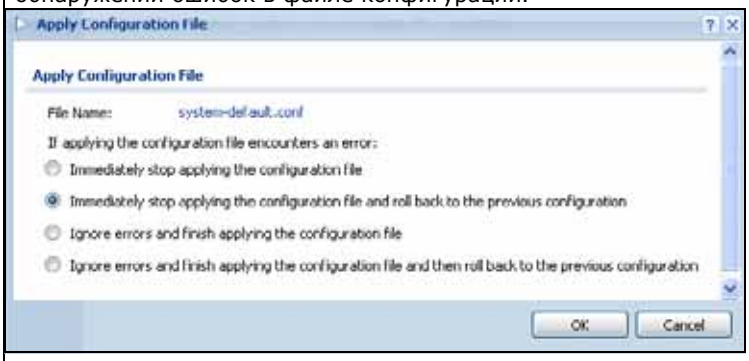
ПОЛЕ	ОПИСАНИЕ
Apply	С помощью этой кнопки можно выбрать определенный файл конфигурации, который устройство NXC будет использовать. Щелкните по строке, соответствующей нужному файлу конфигурации, чтобы выбрать ее, и нажмите кнопку **Apply**. Устройство NXC будет использовать выбранный файл конфигурации. Для перехода на новый файл конфигурации перезагрузка устройства NXC не требуется, придется лишь подождать несколько минут, пока система перейдет на новую конфигурацию. На следующем экране можно выбрать алгоритм поведения устройства NXC при обнаружении ошибок в файле конфигурации.  **Immediately stop applying the configuration file** (Немедленно прекратить применение файла конфигурации) – эту опцию выбирать не рекомендуется, поскольку оставшаяся часть конфигурации останется пустой. Например, если до первой ошибки не были сконфигурированы интерфейсы, то единственным способом связи с устройством может оказаться консольный порт. **Immediately stop applying the configuration file and roll back to the previous configuration** (Немедленно прекратить применение файла конфигурации и совершить откат к предыдущей конфигурации) – в этом случае устройство NXC совершит загрузку с использованием полностью корректного файла конфигурации с максимально возможной скоростью. **Ignore errors and finish applying the configuration file** (Игнорировать ошибки и применить файл конфигурации до конца) – в этом случае устройство применит корректные части файла конфигурации и сгенерирует журналы ошибок для всех ошибок, обнаруженных в файле конфигурации. Соответственно, устройство NXC применит значительную часть конфигурации, а журналы можно будет проанализировать на предмет исправления ошибок. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** (Игнорировать ошибки и применить файл конфигурации до конца, а затем совершить откат к предыдущей конфигурации) – в этом случае устройство NXC применит корректные части файла конфигурации, сгенерирует журналы ошибок для всех ошибок, обнаруженных в файле конфигурации, и выполнит загрузку с использованием полностью корректного файла конфигурации. Нажмите кнопку **OK**, чтобы начать применение файла конфигурации на устройстве NXC или кнопку **Cancel**, чтобы закрыть экран
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу конфигурации. В этом поле содержится порядковое значение, не связанное с каким-либо конкретным адресом. Общее количество файлов конфигурации, которые можно создать, зависит от их размеров и доступного пространства во флэш-памяти.

Таблица 180 Экран Maintenance > File Manager > Configuration File (продолжение)

ПОЛЕ	ОПИСАНИЕ
File Name	В этом столбце отображается имя, которое идентифицирует файл конфигурации. Следующие файлы конфигурации удалить или переименовать невозможно. Файл **system-default.conf** содержит настройки по умолчанию для устройства NXC. Выберите этот файл и нажмите кнопку **Apply**, чтобы сбросить все параметры устройства NXC до настроек по умолчанию. Этот файл конфигурации входит в пакет встроенного программного обеспечения, который выгружается на устройство. Файл **startup-config.conf** – это файл конфигурации, который устройство NXC использует в настоящее время. Если изменить какие-либо настройки в ходе сессии администрирования и сохранить изменения, то они попадут в этот файл конфигурации. Устройство NXC вносит изменения, сделанные в интерфейсе Web-конфигуратора, в файл конфигурации при нажатии кнопок **Apply** и **OK**. Изменения, вносимые посредством команд, попадают в файл конфигурации при выполнении команды `write`. Файл **lastgood.conf** – это последний корректный файл конфигурации, который был сохранен при последней перезагрузке устройства. Если случайно был выгружен и применен файл конфигурации с ошибкой, применение настроек из файла lastgood.conf позволит вернуться к корректной конфигурации.
Size	Этот столбец показывает размер файла конфигурации (в Кбайт).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения отдельных файлов конфигурации.
Upload Configuration File	В нижней части экрана расположены элементы управления, с помощью которых можно выгрузить новый или ранее сохраненный файл конфигурации с компьютера на устройство NXC Выгрузить файлы конфигурации с именами **system-default.conf** и **lastgood.conf** нельзя. Если выгрузить файл **startup-config.conf**, то он заменит текущий файл конфигурации, и новые настройки будут немедленно применены.
File Path	Укажите в этом поле путь к файлу, который необходимо выгрузить, или нажмите кнопку **Browse ...**, чтобы найти его.
Browse...	Нажмите кнопку **Browse...**, чтобы найти файл .conf, который необходимо выгрузить. Файл конфигурации должен иметь разрешение «.conf». При попытке выгрузить файл в другом формате система выдаст сообщение об ошибке. Не забудьте разархивировать сжатые файлы (.zip) перед их выгрузкой.
Upload	Нажмите кнопку **Upload**, чтобы начать процесс выгрузки. Он может занять до двух минут.

30.3 Экран Firmware Package

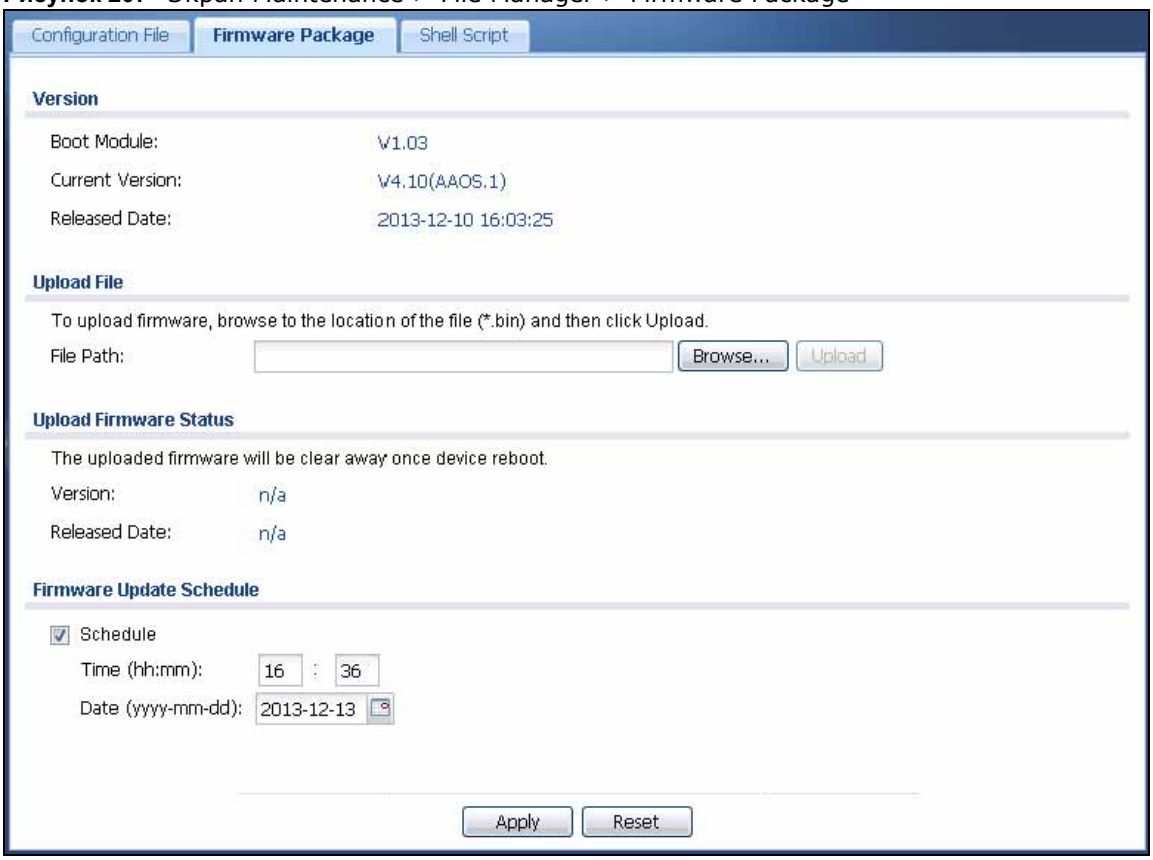
Чтобы открыть этот экран, выберите в меню **Maintenance > File Manager > Firmware Package**. Экран **Firmware Package** позволяет ознакомиться с текущей версией встроенного программного обеспечения и выгрузить встроенное программное обеспечение на устройство NXC.

Примечание: Для выгрузки встроенного программного обеспечения рекомендуется использовать Web-конфигуратор. Интерфейс командной строки следует использовать только в тех случаях, когда необходимо восстановить встроенное программное обеспечение. Чтобы узнать, как определить необходимость восстановления встроенного программного обеспечения и как его восстановить, обратитесь к Справочному руководству по интерфейсу командной строки.

Найдите нужный пакет встроенного программного обеспечения на сайте www.zyxel.com. Пакет, как правило, находится в файле с расширением .bin, названным по имени модели системы, например, «nxc.bin».

Обновление встроенного программного обеспечения может занять до пяти минут. Не выключайте и не перегружайте устройство NXC во время выгрузки встроенного программного обеспечения!

Рисунок 207 Экран Maintenance > File Manager > Firmware Package



Поля экрана описаны в следующей таблице.

Таблица 181 Экран Maintenance > File Manager > Firmware Package

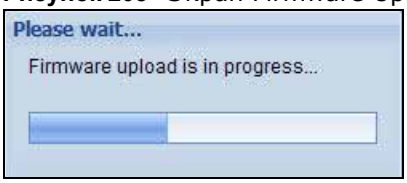
ПОЛЕ	ОПИСАНИЕ
Version	
Boot Module	Это версия модуля загрузки, которую устройство NXC использует в настоящий момент.

Таблица 181 Экран Maintenance > File Manager > Firmware Package (продолжение)

ПОЛЕ	ОПИСАНИЕ
Current Version	Это версия встроенного программного обеспечения, которая установлена на устройстве NXC в настоящий момент. Версия встроенного программного обеспечения включает в себя номер версии основного потока кода, код модели и номер релиза. Например, в строке V4.10(AAOS.1) V4.10 – это номер версии основного потока кода, AAOS – код модели NXC5500, а 1 означает «первый релиз».
Released Date	Это дата создания встроенного программного обеспечения.
Upload File	
File Path	Укажите в этом поле путь к файлу, который необходимо выгрузить, или нажмите кнопку **Browse ...**, чтобы найти его.
Browse...	Нажмите кнопку **Browse...**, чтобы найти файл .bin, который необходимо выгрузить. Не забудьте разархивировать сжатые файлы (.zip) перед их выгрузкой.
Upload	Нажмите кнопку **Upload**, чтобы начать процесс выгрузки. Он может занять до двух минут.
Upload Firmware Status	
Version	Это версия встроенного программного обеспечения, которое было выгружено.
Released Date	Это дата создания встроенного программного обеспечения.
Firmware Update Schedule	Можно создать расписание, в соответствии с которым устройство NXC установит встроенное программное обеспечение, которое было выгружено, в указанные дату и время.
Schedule	Выберите эту опцию, чтобы включить функцию планирования обновления встроенного программного обеспечения. Примечание: Чтобы включить функцию планирования, нужно выбрать эту опцию и нажать кнопку **Apply** перед тем, как выгрузить пакет встроенного программного обеспечения. В противном случае устройство NXC выполнит установку выгруженного пакета встроенного программного обеспечения немедленно.
Time (hh:mm)	Укажите время суток в 24-часовом формате (например, 23:00 эквивалентно 11:00 pm) для установки встроенного программного обеспечения.
Date (yyyy-mm-dd)	Выберите или укажите дату в формате год-месяц-дата для установки встроенного программного обеспечения.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в конфигурации устройства NXC.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

После появления экрана **Firmware Upload in Process**, сигнализирующего о том, что выполняется загрузка встроенного программного обеспечения, подождите две минуты, прежде чем выполнить вход на устройство NXC снова.

Рисунок 208 Экран Firmware Upload In Process



Примечание: После успешного обновления встроенного программного обеспечения устройство NXC автоматически выполняет перезагрузку.

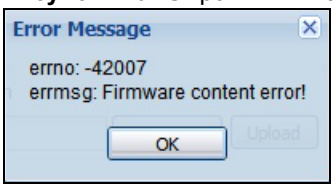
Устройство NXC автоматически перезагружается, что приводит к временному отключению от сети. В некоторых операционных системах на рабочем столе может появиться следующий значок.

Рисунок 209 Значок Network Temporarily Disconnected

Подождите пять минут, выполните вход на устройство и проверьте текущую версию встроенного программного обеспечения на экране **Dashboard**.

Если обновить встроенное программное обеспечение не удалось, на экране появится следующее сообщение.

Рисунок 210 Экран Firmware Upload Error



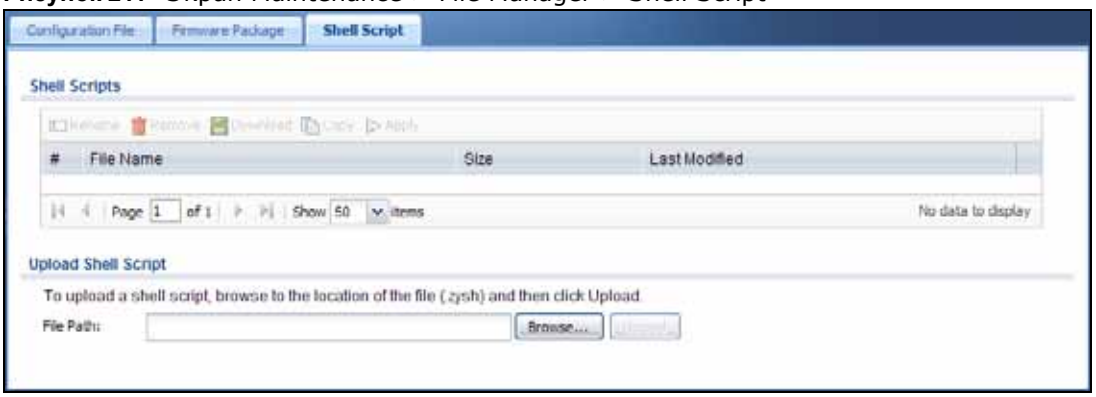
30.4 Экран Shell Script

С помощью файлов сценариев командной строки можно выполнить на устройстве NXC нужные наборы команд. Для создания файлов сценариев командной строки можно использовать текстовый редактор. Такие файлы должны иметь расширение «.zysh».

Чтобы открыть этот экран, выберите в меню **Maintenance > File Manager > Shell Script**. Экран **Shell Script** позволяет сохранять, именовать, загружать, выгружать и запускать файлы сценариев командной строки. На устройстве NXC можно хранить одновременно два и более файлов сценариев командной строки.

Примечание: В сценарии необходимо включать команду `write`. Если этого не сделать, то сделанные изменения будут потеряны после перезагрузки устройства NXC. В длинном сценарии нужно использовать несколько команд `write`.

Рисунок 211 Экран Maintenance > File Manager > Shell Script



Описание каждого из полей приведено в таблице ниже.

Таблица 182 Экран Maintenance > File Manager > Shell Script

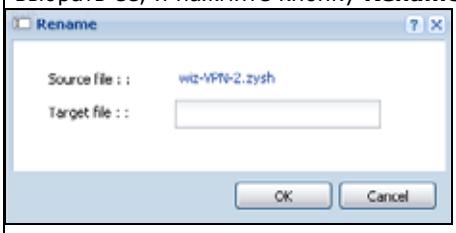
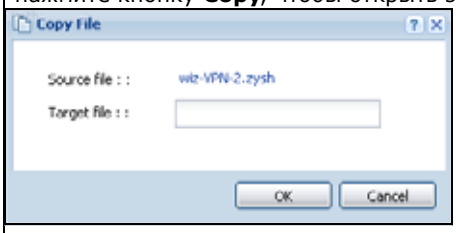
ПОЛЕ	ОПИСАНИЕ
Rename	С помощью этой кнопки можно изменить название файла сценария командной строки на устройстве NXC. Кроме того, нельзя назвать какой-либо файл сценария командной строки именем другого файла сценария командной строки на устройстве NXC. Щелкните по строке, соответствующей нужному файлу сценария командной строки, чтобы выбрать ее, и нажмите кнопку **Rename**. Откроется экран **Rename File**.  Укажите новое имя для файла сценария командной строки. Длина имени должна быть не более 25 символов (допускается использование символов a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Нажмите кнопку **OK**, чтобы сохранить копию, или кнопку **Cancel, чтобы закрыть этот экран, не сохраняя копию файла конфигурации**.
Remove	Щелкните по строке, соответствующей нужному файлу командной строки, чтобы выбрать ее, и нажмите кнопку **Delete**, чтобы удалить файл сценария командной строки с устройства NXC. Появится всплывающее окно с предложением подтвердить удаление файла сценария командной строки. Нажмите кнопку **OK**, чтобы удалить файл сценария командной строки, или кнопку **Cancel**, чтобы закрыть экран, не удаляя файл сценария командной строки.
Download	Щелкните по строке, соответствующей нужному файлу сценария командной строки, чтобы выбрать ее, и нажмите кнопку **Download**, чтобы сохранить его на компьютер.

Таблица 182 Экран Maintenance > File Manager > Shell Script (продолжение)

ПОЛЕ	ОПИСАНИЕ
Copy	С помощью этой кнопки можно сохранить копию файла сценария командной строки на устройстве NXC. Щелкните по строке, соответствующей нужному файлу конфигурации, чтобы выбрать ее, и нажмите кнопку **Copy**, чтобы открыть экран **Copy File**.  Укажите имя для копии файла сценария командной строки. Длина имени должна быть не более 25 символов (допускается использование символов a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Нажмите кнопку **OK**, чтобы сохранить копию, или кнопку **Cancel, чтобы закрыть этот экран, не сохраняя копию файла конфигурации**.
Apply	С помощью этой кнопки можно выбрать определенный файл сценария командной строки, который устройство NXC будет использовать. Щелкните по строке, соответствующей нужному файлу сценария командной строки, чтобы выбрать ее, и нажмите кнопку **Apply**. Устройство NXC будет использовать выбранный файл сценария командной строки. Возможно, необходимо будет подождать некоторое время, пока устройство NXC закончит применение команд.
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу сценария командной строки.
File Name	В этом столбце отображается имя, которое идентифицирует файл сценария командной строки.
Size	Этот столбец показывает размер файла сценария командной строки (в Кбайт).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения конкретных файлов сценариев командной строки.
Upload Shell Script	В нижней части экрана расположены элементы управления, с помощью которых можно выгрузить новый или ранее сохраненный файл сценария командной строки с компьютера на устройство NXC.
File Path	Укажите в этом поле путь к файлу, который необходимо выгрузить, или нажмите кнопку **Browse ...**, чтобы найти его.
Browse...	Нажмите кнопку **Browse...**, чтобы найти файл .zysh, который необходимо выгрузить.
Upload	Нажмите кнопку **Upload**, чтобы начать процесс выгрузки. Он может занять несколько минут.

31

Диагностика

31.1 Обзор

Используйте экраны диагностики для поиска и устранения неполадок.

31.1.1 О чем рассказывается в этой главе

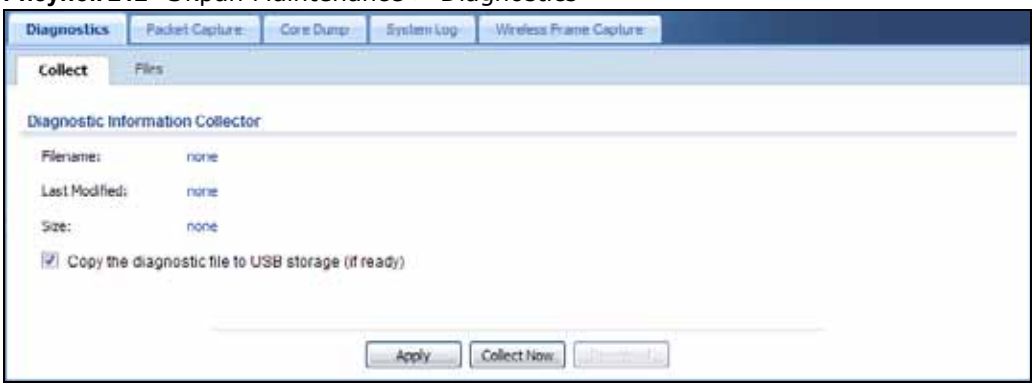
- Экран **Diagnostics** (разд. 31.2 на стр. 385) позволяет сгенерировать файл, содержащий сведения о конфигурации устройства NXC, и диагностическую информацию. Если потребуется, этот файл можно предоставить в службу поддержки клиентов для поиска и устранения неполадок.
- Экран **Packet Capture** (разд. 31.3 на стр. 387) позволяет вести запись пакетов, проходящих через устройство NXC.
- Экраны **Core Dump** (разд. 31.4 на стр. 392) позволяют сохранить дамп ядра процесса на подключенный USB-накопитель в случае аномального завершения процесса (сбоя). Если потребуется, этот файл можно предоставить в службу поддержки клиентов для поиска и устранения неполадок.
- Экраны **System Log** (разд. 31.5 на стр. 394) позволяют загружать файлы системных журналов с подключенного USB-накопителя на компьютер.
- Экраны **Wireless Frame Capture** (разд. 31.6 на стр. 394) позволяют записывать сетевой трафик, проходящий через интерфейсы точек доступа, подключенных к устройству NXC.

31.2 Экран Diagnostics

Этот экран предлагает легкий способ генерации файла, содержащего сведения о конфигурации устройства NXC, и диагностическую информацию. Возможно, необходимо будет сгенерировать такой файл с тем, чтобы отправить его в службу поддержки клиентов для последующего поиска и устранения неполадок.

Выберите в меню **Maintenance > Diagnostics**, чтобы открыть экран **Diagnostic**.

Рисунок 212 Экран Maintenance > Diagnostics



Поля экрана описаны в следующей таблице.

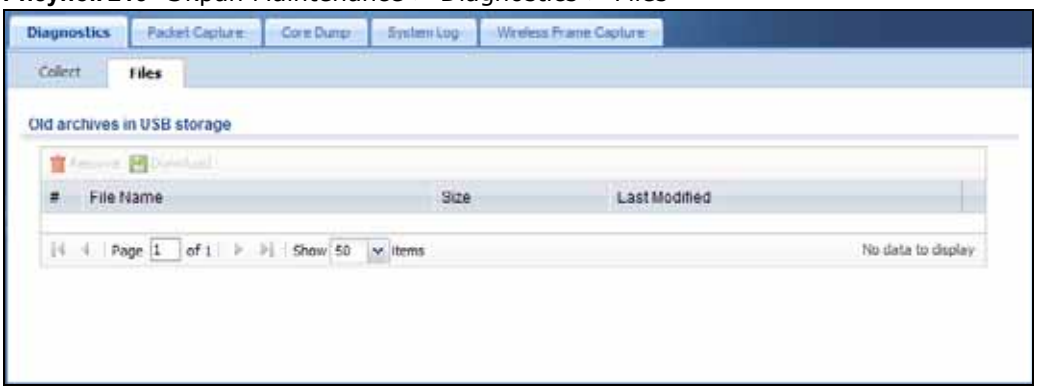
Таблица 183 Экран Maintenance > Diagnostics

ПОЛЕ	ОПИСАНИЕ
Filename	Это имя недавно созданного файла диагностики.
Last modified	Это дата и время создания последнего файла диагностики. Значение в этом поле имеет следующий формат: гггг-мм-дд чч:мм:сс.
Size	Это размер недавно созданного файла диагностики.
Copy the diagnostic file to USB storage (if ready)	Выберите эту опцию, чтобы устройство NXC создало дополнительную копию файла диагностики на подключенном USB-накопителе.
Apply	Нажмите кнопку **Apply**, чтобы сохранить сделанные изменения.
Collect Now	Нажмите эту кнопку, чтобы запустить создание на устройстве NXC нового файла диагностики.
Download	Нажмите эту кнопку, чтобы сохранить самый последний из созданных файлов диагностики на компьютер.

31.2.1 Файлы диагностики

Выберите в меню **Maintenance > Diagnostics > Files**, чтобы открыть экран управления файлами диагностики. Этот экран содержит перечень файлов с диагностической информацией, которые устройство NXC собрало и сохранило на подключенном USB-накопителе. Возможно, когда-нибудь необходимо будет отправить эти файлы в службу поддержки клиентов для последующего поиска и устранения неполадок.

Рисунок 213 Экран Maintenance > Diagnostics > Files



Поля экрана описаны в следующей таблице.

Таблица 184 Экран Maintenance > Diagnostics > Files

ПОЛЕ	ОПИСАНИЕ
Remove	Выберите ненужные файлы и нажмите кнопку **Remove**, чтобы удалить их с устройства NXC. Для выбора двух и более файлов воспользуйтесь клавишами [Shift] и/или [Ctrl]. Появится всплывающее окно с предложением подтвердить удаление файлов.
Download	Выберите нужный файл и нажмите кнопку **Download**, чтобы сохранить его на компьютер.
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу. Общее количество файлов, которое можно сохранить, зависит от их размеров и доступного дискового пространства.
File Name	В этом столбце отображается имя, которое идентифицирует файл.
Size	Этот столбец показывает размер файла (в байтах).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения отдельных файлов.

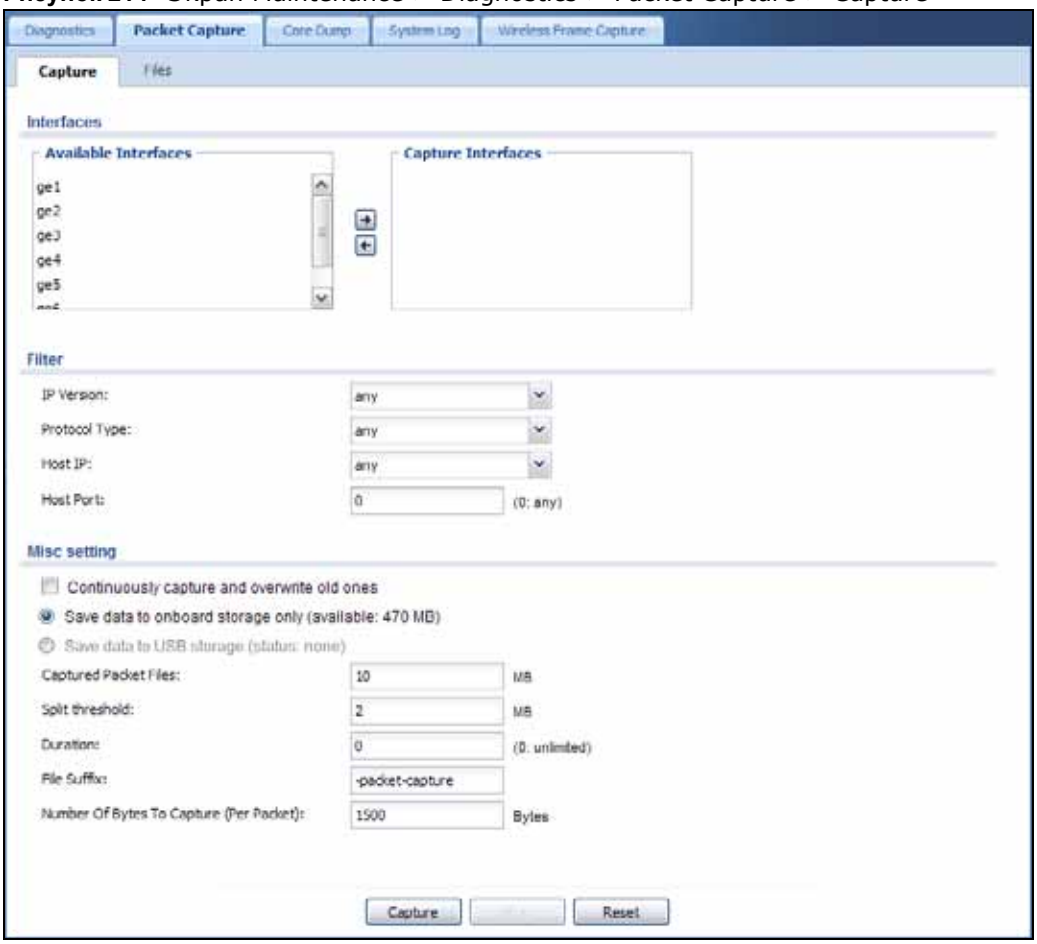
31.3 Экран Packet Capture

С помощью этого экрана можно включить запись сетевого трафика, проходящего через интерфейсы устройства NXC. Анализ записей пакетов может помочь при идентификации неполадок в сети.

Выберите в меню **Maintenance > Diagnostics > Packet Capture**, чтобы открыть экран записи пакетов.

Примечание: Вновь записываемые файлы будут записаны поверх существующих файлов с тем же именем. Чтобы этого избежать, можно поменять значение в поле **File Suffix**.

Рисунок 214 Экран Maintenance > Diagnostics > Packet Capture > Capture



Поля экрана описаны в следующей таблице.

Таблица 185 Экран Maintenance > Diagnostics > Packet Capture

ПОЛЕ	ОПИСАНИЕ
Interfaces	Поле **Available Interfaces** содержит список включенных интерфейсов. Выберите интерфейсы, для которых необходимо включить запись пакетов, и нажмите кнопку с правой стрелкой, чтобы переместить их в поле **Capture Interfaces**. Для выбора двух и более объектов воспользуйтесь клавишами [Shift] и/или [Ctrl].
IP Version	Выберите версию протокола IP (Internet Protocol), посредством которого осуществляется маршрутизация трафика по сетям и Интернету. Выберите опцию **any**, чтобы включить запись пакетов для трафика, отправляемого всеми версиями протокола IP.
Protocol Type	Выберите тип протокола для трафика, чьи пакеты необходимо записывать. Выберите опцию **any**, чтобы включить запись пакетов для всех видов трафика.
Host IP	Выберите объект IP-адреса хоста, для которого необходимо вести запись пакетов. Выберите опцию **any**, чтобы включить запись пакетов для всех хостов. Выберите опцию **User Defined**, если необходимо указать IP-адрес.
Host Port	Это поле доступно для изменения, если в поле **Protocol Type** выбрана одна из опций **any**, **tcp** или **udp**. Укажите номер порта для трафика, который необходимо записывать.
Continuously capture and overwrite old ones	Выберите эту опцию, чтобы устройство NXC продолжало вести запись трафика, перезаписывая при этом старые записи в случае нехватки дискового пространства.

Таблица 185 Экран Maintenance > Diagnostics > Packet Capture (продолжение)

ПОЛЕ	ОПИСАНИЕ
Save data to onboard storage only	Выберите эту опцию, чтобы устройство NXC сохраняло записи пакетов только на устройстве NXC. В этом поле отображается также размер доступного хранилища. Примечание: Устройство NXC резервирует некоторый объем пространства во встроенном хранилище в качестве буфера.
Save data to USB storage	Выберите эту опцию, чтобы устройство NXC сохраняло записи пакетов только на USB-накопителе, подключенном к устройству NXC. Экран Status: **Unused** – подключенный USB-накопитель был демонтирован вручную с использованием кнопки **Remove Now**, либо устройство NXC по каким-то причинам не может его смонтировать. **none** – к устройству не подключены USB-накопители. **available** – устройство NXC может работать с USB-накопителем. В этом поле отображается также объем доступного дискового пространства. **service deactivated** – функция USB-накопителя отключена, и устройство NXC не может хранить системный журнал и другую диагностическую информацию на подключенном USB-накопителе. Примечание: Устройство NXC резервирует некоторый объем пространства на USB-накопителе в качестве буфера.
Captured Packet Files	В случае сохранения пакетов только во встроенном хранилище устройства NXC укажите максимальный объем в мегабайтах для совокупного размера всех файлов записей на устройстве NXC. В случае сохранения пакетов на подключенном USB-накопителе укажите максимальный объем в мегабайтах для каждого файла записи. Примечание: Если имеются созданные ранее файлы записей и при этом опция **Continuously capture and overwrite old ones** не выбрана, то, возможно, придется указать больший размер или удалить имеющиеся файлы записей. Допустимый диапазон зависит от доступного размера встроенного хранилища/ дискового пространства на USB-накопителе. Устройство NXC останавливает запись и генерирует файл записи либо когда файл достигает указанного размера, либо когда истекает временной интервал, указанный в поле **Duration**.
Split threshold	Укажите максимальный размер в мегабайтах для отдельных файлов записей пакетов. По достижении файлом записи пакетов указанного размера устройство NXC начинает запись в другой файл.
Duration	Укажите лимит времени в секундах для записи. Устройство NXC останавливает запись и генерирует файл записи либо когда истек указанный период времени, либо когда файл достигает размера, указанного в поле **Captured Packet Files**. **0** означает отсутствие временного лимита.
File Suffix	Введите текст, который будет добавлен в конец файла (перед точкой и расширением), чтобы помочь идентифицировать файлы записей пакетов. Изменение суффикса позволяет избежать ситуации, когда вновь создаваемые файлы пакетов начинают затирать существующие файлы с тем же именем. Формат имени файла выглядит следующим образом: «interface name-file suffix.cap», например, «vlan2-packet-capture.cap».

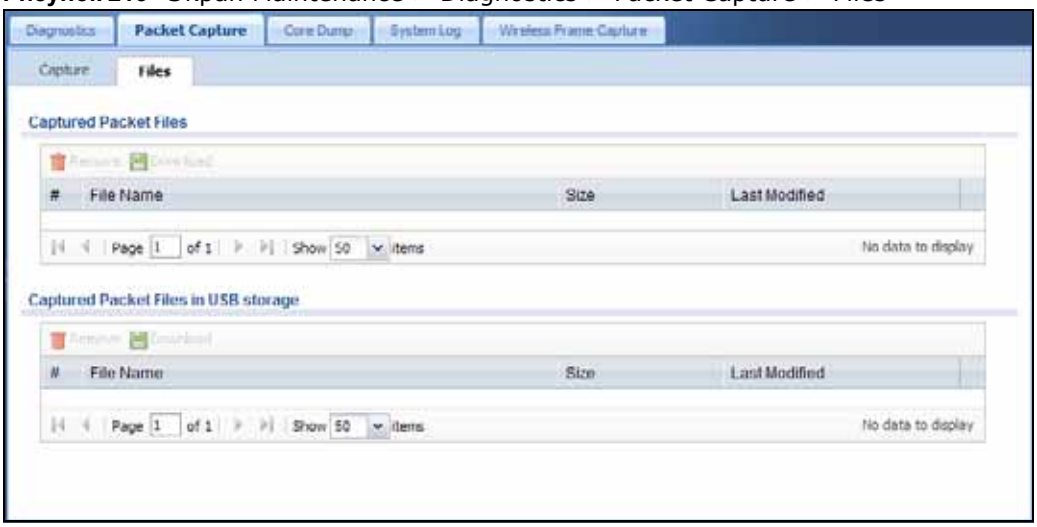
Таблица 185 Экран Maintenance > Diagnostics > Packet Capture (продолжение)

ПОЛЕ	ОПИСАНИЕ
Number Of Bytes To Capture (Per Packet)	Укажите максимальное количество байт, записываемых для одного пакета. Устройство NXC автоматически отсекает все байты, выходящие за пределы указанного количества. Соответственно, необходимо учесть, что реальный размер пакетов может оказаться больше, чем размер записанных пакетов, которые просматриваются с помощью анализатора пакетов.
Capture	При нажатии этой кнопки устройство NXC начнет запись пакетов в соответствии с настройками на этом экране. Можно продолжать настройку других параметров устройства NXC во время записи пакетов, однако изменить настройки записи пакетов в это время нельзя. Процесс записи пакетов может повлиять на производительность или пропускную способность устройства NXC. По завершении записи устройство NXC сохраняет отдельный файл записи для каждого выбранного интерфейса. Общее количество сохраняемых файлов записи пакетов зависит от размеров файлов и доступного пространства во флэш-памяти. После переполнения флэш-памяти запись новых пакетов станет невозможной.
Stop	Нажмите эту кнопку, чтобы остановить идущий в данный момент процесс записи пакетов и сгенерировать отдельный файл записи для каждого выбранного интерфейса.
Reset	Нажмите эту кнопку, чтобы вернуть на экран настройки, сохраненные ранее.

31.3.1 Файлы записей пакетов

Выберите в меню **Maintenance > Diagnostics > Packet Capture > Files**, чтобы открыть экран для управления файлами записей пакетов. Этот экран показывает список файлов записей пакетов, хранящихся на устройстве NXC или подключенном USB-накопителе. Можно загрузить файлы на компьютер для изучения с помощью анализатора пакетов (его также называют сетевым анализатором или анализатором протоколов), например, Wireshark.

Рисунок 215 Экран Maintenance > Diagnostics > Packet Capture > Files



Поля экрана описаны в следующей таблице.

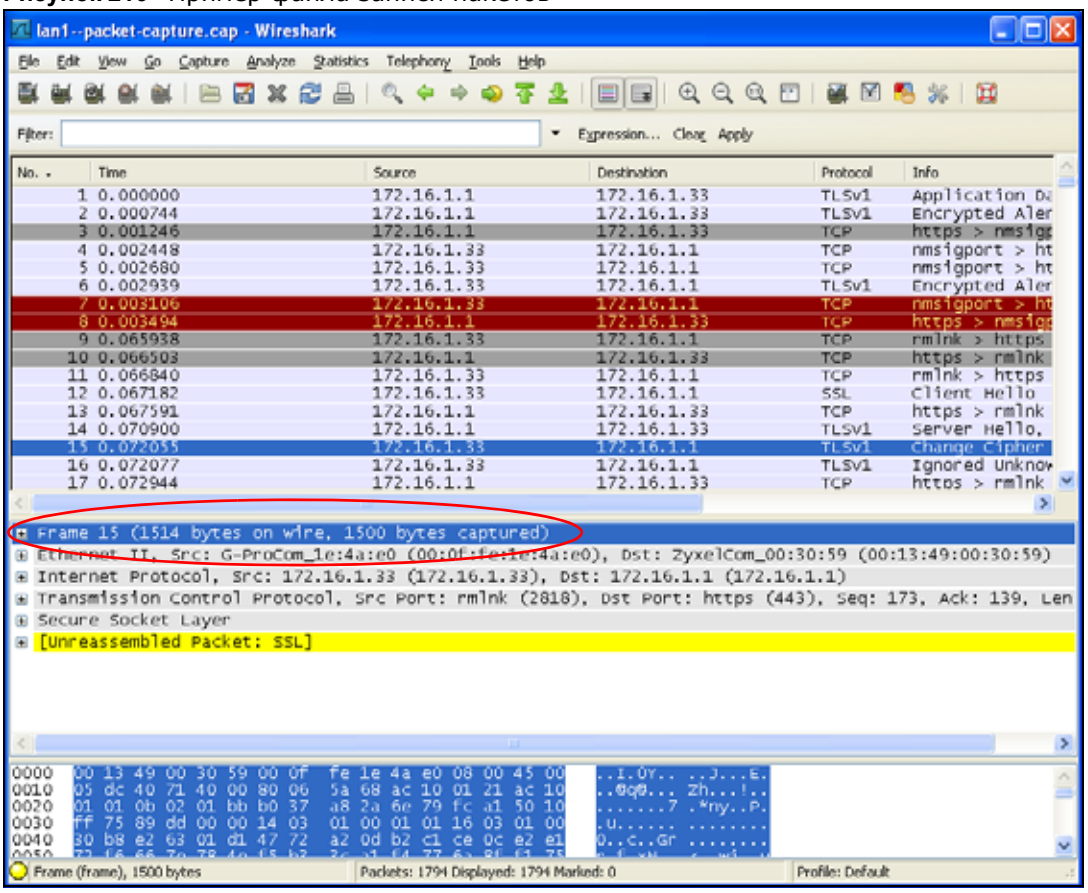
Таблица 186 Экран Maintenance > Diagnostics > Packet Capture > Files

ПОЛЕ	ОПИСАНИЕ
Remove	Выберите ненужные файлы и нажмите кнопку **Remove**, чтобы удалить их с устройства NXC. Для выбора двух и более файлов воспользуйтесь клавишами [Shift] и/или [Ctrl]. Появится всплывающее окно с предложением подтвердить удаление файлов.
Download	Выберите нужный файл и нажмите кнопку **Download**, чтобы сохранить его на компьютер.
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу записи пакетов. Общее количество сохраняемых файлов записи пакетов зависит от размеров файлов и доступного пространства во флэш-памяти.
File Name	В этом столбце отображается имя, которое идентифицирует файл. Формат имени файла выглядит следующим образом: имя интерфейса-суффикс файла.cap.
Size	Этот столбец показывает размер файла записи пакетов (в байтах).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения отдельных файлов.

31.3.2 Пример просмотра файла записи пакетов

Ниже показан пример файла записи пакетов, загруженный для просмотра в инструмент анализа пакетов Wireshark. Обратите внимание, что кадр 15 имеет размер 1514 байт, тогда как записанный размер составляет только 1500 байт. Устройством NXC данный кадр был обрезан, так как в поле **Number Of Bytes To Capture (Per Packet)** на экране записи пакетов было установлено значение 1500 байт.

Рисунок 216 Пример файла записи пакетов



31.4 Экран Core Dump

Экран **Core Dump** позволяет сохранить дамп ядра процесса с устройства NXC на подключенный USB-накопитель в случае аномального завершения процесса (сбоя). Если потребуется, этот файл можно предоставить в службу поддержки клиентов для поиска и устранения неполадок.

Выберите в меню **Maintenance > Diagnostics > Core Dump**, чтобы открыть следующий экран.

Рисунок 217 Экран Maintenance > Diagnostics > Core Dump

Поля экрана описаны в следующей таблице.

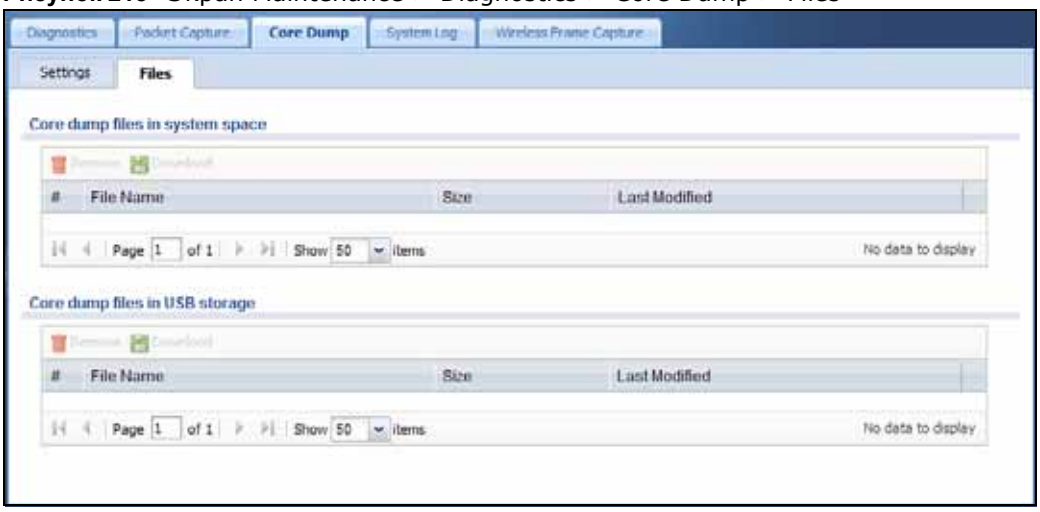
Таблица 187 Экран Maintenance > Diagnostics > Core Dump

ПОЛЕ	ОПИСАНИЕ
Save core dump to USB storage (if ready)	Установите этот переключатель, чтобы устройство NXC сохраняло дамп ядра процесса на подключенный USB-накопитель в случае аномального завершения процесса (сбоя). Если снять этот переключатель, то устройство NXC будет сохранять только
Apply	Нажмите **Apply**, чтобы сохранить эти настройки.
Reset	Нажмите кнопку **Reset**, чтобы вернуть последние сохраненные настройки для экрана.

31.4.1 Файлы дампов ядра

Выберите в меню **Maintenance > Diagnostics > Core Dump > Files**, чтобы открыть экран для управления файлами дампов ядра. Этот экран показывает список файлов дампов ядра, хранящихся на устройстве NXC или подключенном USB-накопителе. Возможно, когда-нибудь необходимо будет отправить эти файлы в службу поддержки клиентов для последующего поиска и устранения неполадок.

Рисунок 218 Экран Maintenance > Diagnostics > Core Dump > Files



Поля экрана описаны в следующей таблице.

Таблица 188 Экран Maintenance > Diagnostics > Core Dump > Files

ПОЛЕ	ОПИСАНИЕ
Remove	Выберите ненужные файлы и нажмите кнопку **Remove**, чтобы удалить их с устройства NXC. Для выбора двух и более файлов воспользуйтесь клавишами [Shift] и/или [Ctrl]. Появится всплывающее окно с предложением подтвердить удаление файлов.
Download	Выберите нужный файл и нажмите кнопку **Download**, чтобы сохранить его на компьютер.
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу дампа ядра. Общее количество сохраняемых файлов дампов ядра зависит от размеров файлов и доступного пространства во флэш-памяти.
File Name	В этом столбце отображается имя, которое идентифицирует файл.

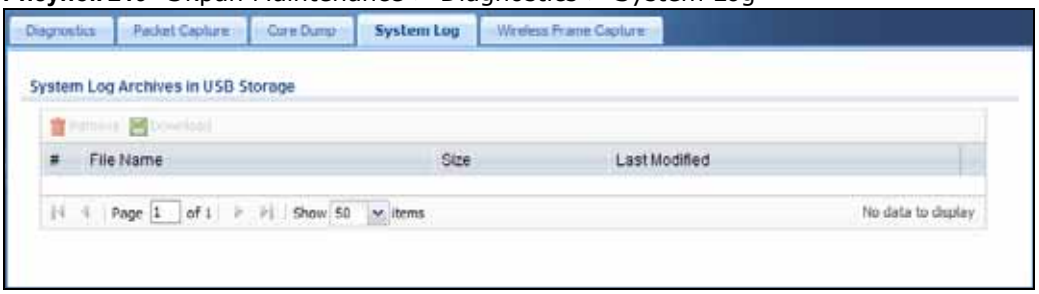
Таблица 188 Экран Maintenance > Diagnostics > Core Dump > Files (продолжение)

ПОЛЕ	ОПИСАНИЕ
Size	Этот столбец показывает размер файла (в байтах).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения отдельных файлов.

31.5 Экран System Log

Выберите в меню **Maintenance > Diagnostics > System Log**, чтобы открыть экран для управления файлами системных журналов. Этот экран показывает список файлов системных журналов, хранящихся на подключенном USB-накопителе. Файлы хранятся в формате записей, разделенных запятой (comma separated value, csv). Их можно загрузить себе на компьютер и открыть в удобном приложении, например, Microsoft Excel.

Рисунок 219 Экран Maintenance > Diagnostics > System Log



Поля экрана описаны в следующей таблице.

Таблица 189 Экран Maintenance > Diagnostics > System Log

ПОЛЕ	ОПИСАНИЕ
Remove	Выберите ненужные файлы и нажмите кнопку **Remove**, чтобы удалить их с устройства NXC. Для выбора двух и более файлов воспользуйтесь клавишами [Shift] и/или [Ctrl]. Появится всплывающее окно с предложением подтвердить удаление файлов.
Download	Выберите нужный файл и нажмите кнопку **Download**, чтобы сохранить его на компьютер.
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу. Общее количество файлов, которое можно сохранить, зависит от их размеров и доступного дискового пространства.
File Name	В этом столбце отображается имя, которое идентифицирует файл.
Size	Этот столбец показывает размер файла (в байтах).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения отдельных файлов.

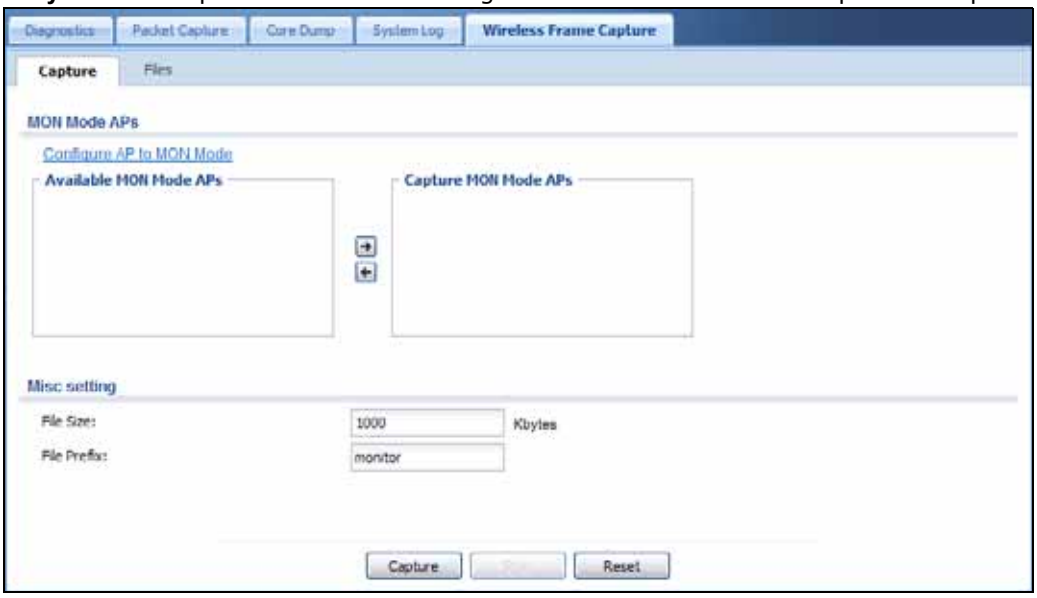
31.6 Экран Wireless Frame Capture

С помощью этого экрана можно вести запись беспроводного сетевого трафика, проходящего через интерфейсы точек доступа, подключенных к устройству NXC. Анализ записей таких кадров может помочь при идентификации неполадок в сети.

Выберите в меню **Maintenance > Diagnostics > Wireless Frame Capture**, чтобы открыть этот экран.

Примечание: Вновь записываемые файлы будут записаны поверх существующих файлов с тем же именем. Чтобы этого избежать, можно поменять значение в поле **File Prefix**.

Рисунок 220 Экран Maintenance > Diagnostics > Wireless Frame Capture > Capture



Поля экрана описаны в следующей таблице.

Таблица 190 Экран Maintenance > Diagnostics > Wireless Frame Capture > Capture

ПОЛЕ	ОПИСАНИЕ
MON Mode APs	
Configure AP to MON Mode	Щелкните по этой ссылке, чтобы перейти к экрану **Configuration > Wireless > AP Management**, с помощью которого можно перевести одну или несколько точек доступа в режим мониторинга.
Available MON Mode APs	Этот столбец показывает, какие точки доступа в беспроводной сети в настоящее время переведены в режим мониторинга. Воспользуйтесь клавишами со стрелками, если необходимо убрать какие-либо точки доступа из этого списка и перенести их в список **Captured MON Mode APs**.
Capture MON Mode APs	Это столбец показывает точки доступа, работающие в режиме мониторинга и выбранные для записи беспроводных кадров.
Misc Setting	

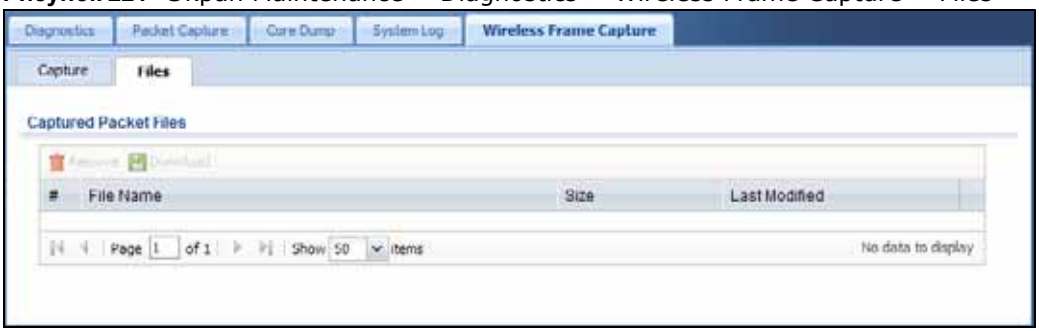
Таблица 190 Экран Maintenance > Diagnostics > Wireless Frame Capture > Capture

ПОЛЕ	ОПИСАНИЕ
File Size	Укажите максимальный лимит в килобайтах для совокупного размера всех файлов записей на устройстве NXC, включая существующие файлы записей и любые новые генерируемые файлы записей. Примечание: Если имеются старые файлы записей, то, возможно, необходимо будет установить более высокий лимит или удалить какие-то из имеющихся файлов записей. Значение для этого поля должно выбираться из диапазона от 1 до 50000. Устройство NXC останавливает запись и генерирует файл записи либо когда файл достигает указанного размера, либо когда истекает временной интервал, указанный в поле **Duration**.
File Prefix	Укажите текст, который будет добавляться в начале имени файла для более легкой идентификации файлов записи кадров. Можно менять префикс в том числе и для того, чтобы создавать новые файлы записей кадров каждый раз, когда выполняете процедуру записи кадров. В этом случае вновь создаваемые файлы записи кадров не будут затирать уже существующие. Формат имени файла выглядит следующим образом: [префикс файла].cap. Например, «monitor.cap».
Capture	При нажатии этой кнопки устройство NXC начнет запись кадров в соответствии с настройками на экране. Можно продолжать настройку других параметров устройства NXC во время записи кадров, однако изменить настройки записи кадров в это время нельзя. Процесс записи кадров может повлиять на производительность или пропускную способность устройства NXC. По завершении записи устройство NXC сохраняет общий файл записи для всех точек доступа. Общее количество сохраняемых файлов записи кадров зависит от размеров файлов и доступного пространства во флэш-памяти. После переполнения флэш-памяти запись новых кадров станет невозможной.
Stop	Нажмите эту кнопку, чтобы остановить идущий в данный момент процесс записи кадров и сгенерировать отдельный файл записи для каждого выбранного интерфейса.
Reset	Нажмите эту кнопку, чтобы вернуть на экран настройки, сохраненные ранее.

31.6.1 Файлы записей беспроводных кадров

Выберите в меню **Maintenance > Diagnostics > Wireless Frame Capture > Files**, чтобы открыть этот экран. Этот экран содержит список файлов записей беспроводных кадров, которые сформировало устройство NXC. Можно загрузить файлы на компьютер для изучения с помощью анализатора пакетов (его также называют сетевым анализатором или анализатором протоколов), например, Wireshark.

Рисунок 221 Экран Maintenance > Diagnostics > Wireless Frame Capture > Files



Поля экрана описаны в следующей таблице.

Таблица 191 Экран Maintenance > Diagnostics > Wireless Frame Capture > Files

ПОЛЕ	ОПИСАНИЕ
Remove	Выберите ненужные файлы и нажмите кнопку **Remove**, чтобы удалить их с устройства NXC. Для выбора двух и более файлов воспользуйтесь клавишами [Shift] и/или [Ctrl]. Появится всплывающее окно с предложением подтвердить удаление файлов.
Download	Выберите нужный файл и нажмите кнопку **Download**, чтобы сохранить его на компьютер.
#	В этом столбце отображается некоторый номер для каждой записи, соответствующей определенному файлу записи пакетов. Общее количество сохраняемых файлов записи пакетов зависит от размеров файлов и доступного пространства во флэш-памяти.
File Name	В этом столбце отображается имя, которое идентифицирует файл. Формат имени файла выглядит следующим образом: имя интерфейса-суффикс файла.cap.
Size	Этот столбец показывает размер файла записи пакетов (в байтах).
Last Modified	Этот столбец показывает дату и время внесения последних изменений или сохранения отдельных файлов.

32

Анализ алгоритма обработки пакетов

32.1 Обзор

С помощью этой функции можно получить полное представление о том, как устройство NXC определяет адресата для пересылки пакета, и как изменяется IP-адрес источника в соответствии с текущими настройками. Эта функция позволяет получить сводную информацию обо всех настройках маршрутизации и трансляции SNAT и помогает находить и устранять все связанные с ними неполадки.

32.1.1 О чем рассказывается в этой главе

- Экран **Routing Status** (разд. 32.2 на стр. 398) показывает общий алгоритм маршрутизации и настройки для каждой функции маршрутизации.
- Экран **SNAT Status** (разд. 32.3 на стр. 401) показывает общий алгоритм трансляции IP-адресов источников (SNAT) и настройки для каждой функции SNAT.

32.2 Экран Routing Status

Экран **Routing Status** позволяет увидеть текущий алгоритм маршрутизации и быстро перейти к конкретным настройкам маршрутизации. Щелкните по функциональному блоку в разделе **Routing Flow**, чтобы показать связанные (активированные) маршруты в разделе **Routing Table**. Чтобы открыть этот экран, выберите в меню **Maintenance** > **Packet Flow Explore**.

Алгоритм применения правил маршрутизации может меняться в зависимости от того:

- была ли выбрана опция **use policy route to override direct route** на экране **CONFIGURATION > Network > Routing > Policy Route**.
- используются ли маршруты на основе политик для управления трансляцией NAT 1-1 с помощью команды `control-virtual-server-rules activate`.

Примечание: Если пакет отвечает критериям правила маршрутизации, устройство NXC предпринимает соответствующее действие и не выполняет никаких дальнейших проверок алгоритма.

Рисунок 222 Экран Maintenance > Packet Flow Explore > Routing Status (Direct Route)

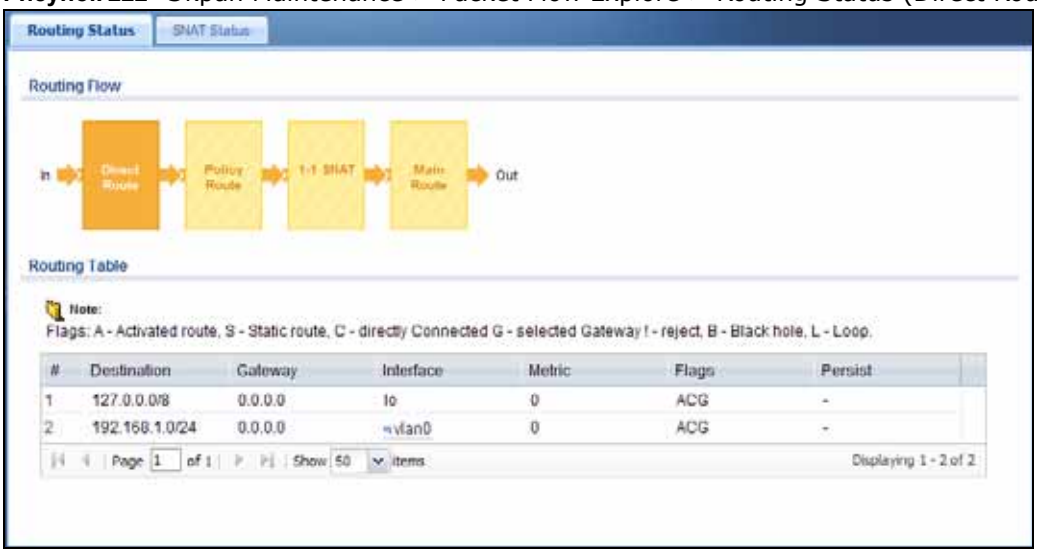


Рисунок 223 Экран Maintenance > Packet Flow Explore > Routing Status (Policy Route)

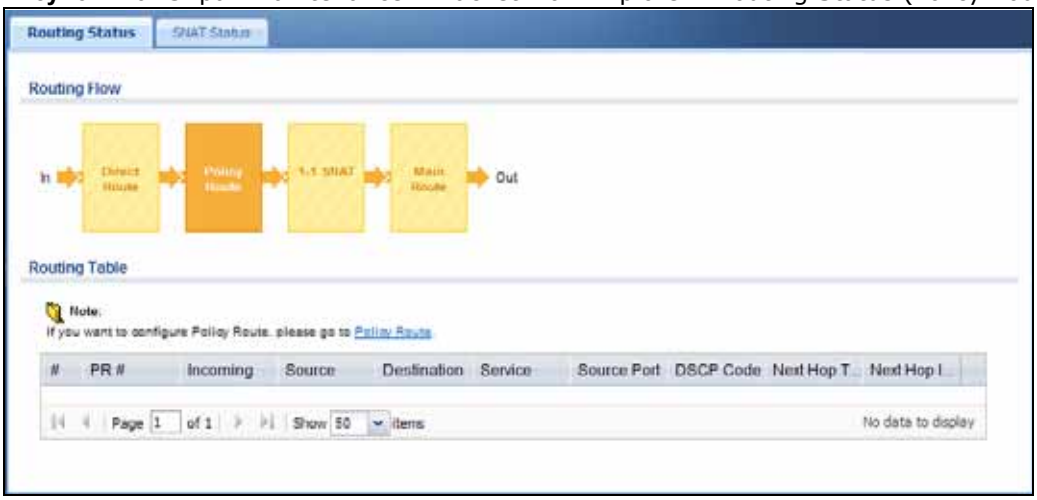


Рисунок 224 Экран Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

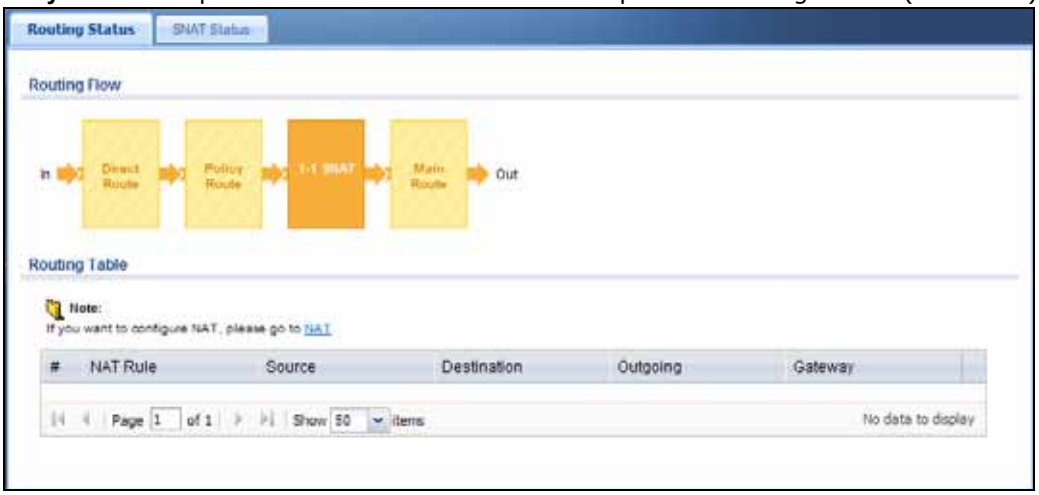
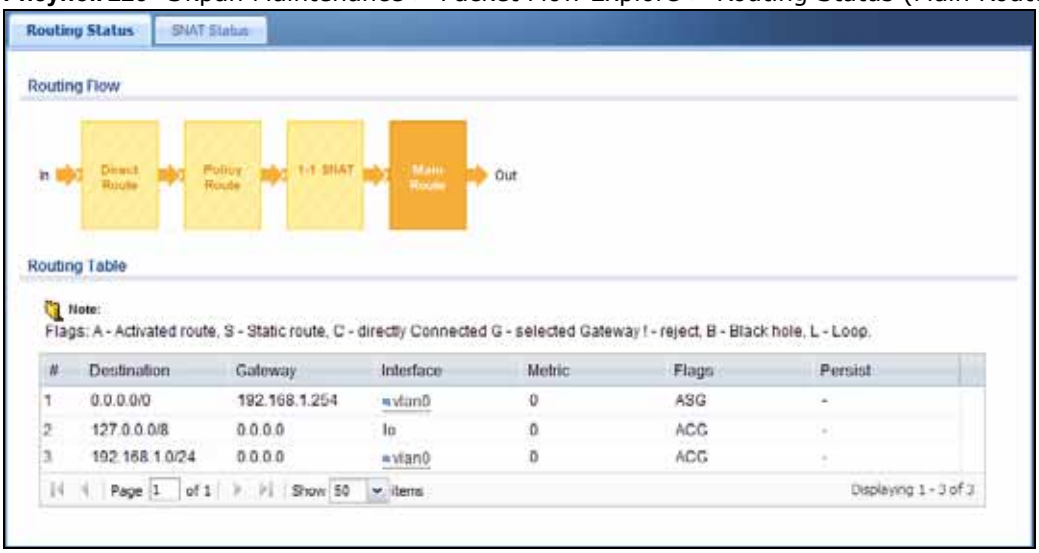


Рисунок 225 Экран Maintenance > Packet Flow Explore > Routing Status (Main Route)



Поля экрана описаны в следующей таблице.

Таблица 192 Экран Maintenance > Packet Flow Explore > Routing Status

ПОЛЕ	ОПИСАНИЕ
Routing Flow	Этот раздел описывает алгоритм определения маршрута, по которому нужно направить пакет, устройством NXC. Щелкните по функциональному блоку, чтобы отобразить связанные настройки в разделе **Routing Table**.
Routing Table	В этом разделе будут показаны настройки, соответствующие функциональному блоку, выбранному в разделе **Routing Flow**.
Если щелкнуть по функциональным блокам **Direct Route** или **Main Route** в разделе **Routing Flow**, на экране появятся следующие поля.	
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
Destination	Это IP-адрес назначения для маршрута.
Gateway	Это IP-адрес шлюза следующего перехода или интерфейса, через который направляется трафик.
Interface	Это имя интерфейса, ассоциированного с данным маршрутом.
Metric	Это приоритет маршрута среди показанных маршрутов.
Flags	Это поле содержит дополнительную информацию о маршруте. Возможны следующие флаги: • **A** – этот маршрут в данный момент активирован. • **S** – это статический маршрут. • **C** – это маршрут прямого подключения. • **O** – это динамический маршрут, выученный по протоколу OSPF. • **R** – это динамический маршрут, выученный по протоколу RIP. • **G** – это маршрут до шлюза (маршрутизатора) в той же сети. • **!** – это маршрут, из-за которого не работает поиск маршрутов. • **B** – это маршрут, который отбрасывает пакеты. • **L** – это рекурсивный маршрут.
Persist	Это время, оставшееся для динамически выученного маршрута. Устройство NXC удаляет этот маршрут, когда этот счетчик дойдет до нуля.
Если щелкнуть по функциональному блоку **Policy Route** в разделе **Routing Flow**, на экране появятся следующие поля.	

Таблица 192 Экран Maintenance > Packet Flow Explore > Routing Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
PR #	Это номер активированного маршрута на основе политик. Если для этого маршрута действует какое-либо расписание, то на этом экране маршрут будет виден только в указанные в расписании часы.
Incoming	Это интерфейс, который принимает пакеты.
Source	Это IP-адрес (или IP-адреса) источников, с которых были отправлены пакеты.
Destination	Это IP-адрес (или IP-адреса) назначения, на которые были отправлены пакеты.
Service	Это название объекта службы. Значение **any** означает «все службы».
Source Port	Это имя объекта службы. Устройство NXC применяет маршрут на основе политик к пакетам, отправляемым с порта соответствующей службы. Значение **any** означает «порты всех служб».
DSCP Code	Это значение кода DSCP входящих пакетов, к которому применяется данный маршрут на основе политик.
Next Hop Type	Это тип следующего перехода, на который отправляются пакеты.
Next Hop Info	• Это основной маршрут, если выбран тип следующего перехода **Auto**. • Это имя интерфейса и IP-адрес шлюза, если выбран тип следующего перехода **Interface /GW**.
Если щелкнуть по функциональному блоку **1-1 SNAT** в разделе **Routing Flow**, на экране появятся следующие поля.	
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
NAT Rule	Это имя активированного правила NAT 1:1 или Many 1:1 в таблице NAT.
Source	Это исходный IP-адрес (или IP-адреса) источника. Значение **any** означает любой IP-адрес.
Destination	Это исходный IP-адрес (или IP-адреса) назначения. Значение **any** означает любой IP-адрес.
Outgoing	Это имя интерфейса, который передает пакеты со стороны устройства NXC.
Gateway	Это IP-адрес шлюза, находящегося в той же сети, что и исходящий интерфейс.

32.3 Экран SNAT Status

Экран **SNAT Status** позволяет просмотреть алгоритм трансляции SNAT и быстро перейти к конкретным настройкам трансляции адресов источника (source NAT, SNAT). Щелкните по функциональному блоку в разделе **SNAT Flow**, чтобы показать связанные правила SNAT (активированные) в разделе **SNAT Table**. Чтобы открыть этот экран, выберите в меню **Maintenance** > **Packet Flow Explore** > **SNAT Status**.

Алгоритм применения правил трансляции SNAT может менять в зависимости от того:

- используются ли маршруты на основе политик для управления трансляцией NAT 1-1 с помощью команды `control-virtual-server-rules activate`.

Примечание: Если пакет отвечает критериям правила трансляции SNAT, устройство NXC предпринимает соответствующее действие и не выполняет никаких дальнейших проверок алгоритма.

Рисунок 226 Экран Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

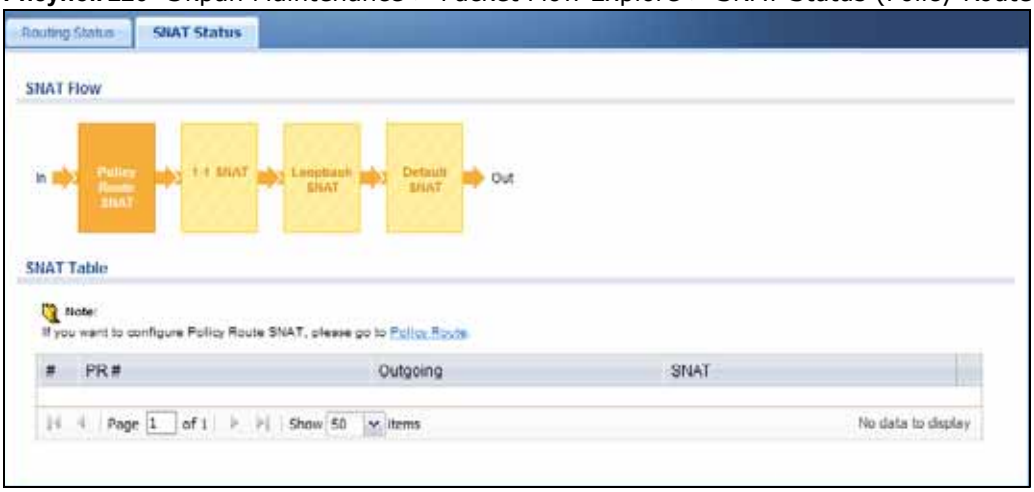


Рисунок 227 Экран Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

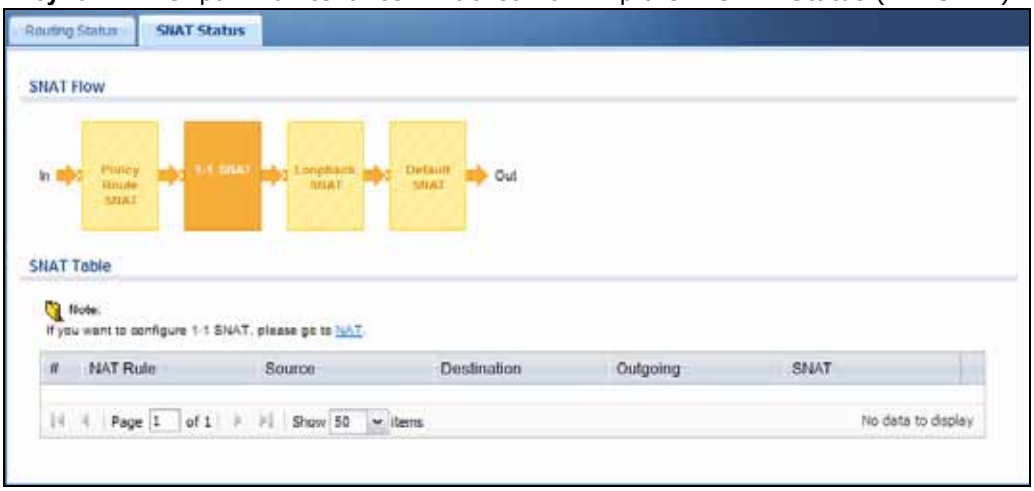


Рисунок 228 Экран Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

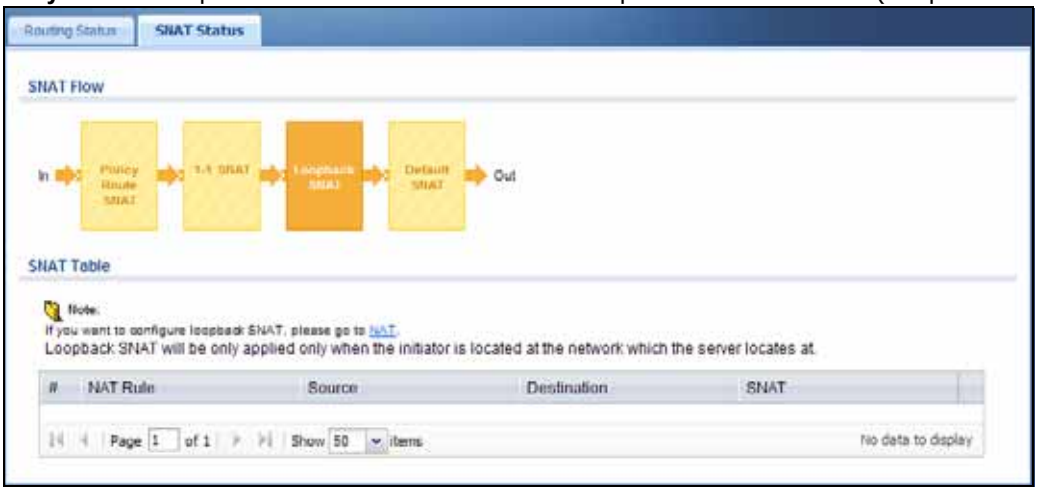
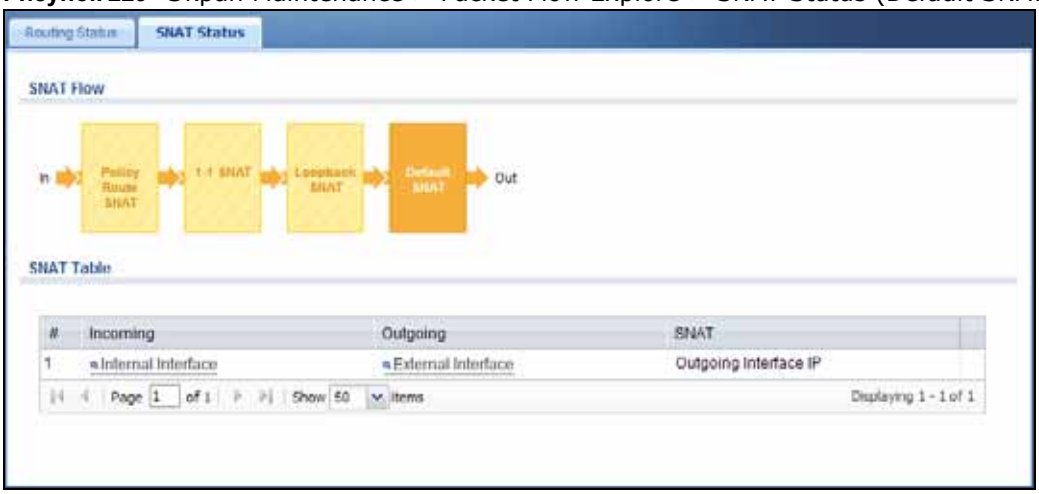


Рисунок 229 Экран Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



Поля экрана описаны в следующей таблице.

Таблица 193 Maintenance > Packet Flow Explore > SNAT Status

ПОЛЕ	ОПИСАНИЕ
SNAT Flow	Этот раздел показывает алгоритм изменения устройством NXC IP-адреса источника в соответствии с правилами, настроенными на устройстве NXC. Щелкните по функциональному блоку, чтобы показать связанные настройки в разделе **SNAT Table**.
SNAT Table	Перечень полей в таблице, содержащейся в этом разделе, может меняться в зависимости от того, какой функциональный блок был выбран в разделе **SNAT Flow**.
Если щелкнуть по функциональному блоку **Policy Route SNAT** в разделе **SNAT Flow**, на экране появятся следующие поля.	
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
PR #	Это номер активированного маршрута на основе политик, который использует трансляцию SNAT.
Outgoing	Это исходящий интерфейс, который использует данный маршрут для передачи пакетов.
SNAT	Это IP-адрес (или IP-адреса) источника, который в итоге использует правило трансляции SNAT.
Если щелкнуть по функциональному блоку **1-1 SNAT** в разделе **SNAT Flow**, на экране появятся следующие поля.	
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
NAT Rule	Это имя активированного правила трансляции NAT, которое использует трансляцию SNAT.
Source	Это исходный IP-адрес (или IP-адреса) источника.
Destination	Это исходный IP-адрес (или IP-адреса) назначения.
Outgoing	Это исходящий интерфейс, который правило трансляции SNAT использует для передачи пакетов.
SNAT	Это IP-адрес (или IP-адреса) источника, который в итоге использует правило трансляции SNAT.
Если щелкнуть по функциональному блоку **Loopback SNAT** в разделе **SNAT Flow**, на экране появятся следующие поля.	
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.

Таблица 193 Maintenance > Packet Flow Explore > SNAT Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
NAT Rule	Это имя активированного правила трансляции NAT, которое использует трансляцию SNAT и включает обратную петлю трансляции NAT.
Source	Это исходный IP-адрес (или IP-адреса) источника. Значение **any** означает любой IP-адрес.
Destination	Это исходный IP-адрес (или IP-адреса) назначения. Значение **any** означает любой IP-адрес.
SNAT	Это поле указывает на IP-адрес источника, который в итоге использует правило трансляции SNAT. Например, опция **Outgoing Interface IP** означает, что устройство NXC использует IP address указанного исходящего интерфейса как IP-адрес источника для соответствующих критериям пакетов, которые он отправляет в соответствии с данным правилом.
Если щелкнуть по функциональному блоку **Default SNAT** в разделе **SNAT Flow**, на экране появятся следующие поля.	
#	Данное поле представляет собой порядковое значение, не связанное с каким-либо параметром.
Incoming	Это поле указывает на внутренний интерфейс (или интерфейсы), на который приходят пакеты.
Outgoing	Это поле указывает на внешний интерфейс (или интерфейсы), с которых передаются пакеты.
SNAT	Это поле указывает на IP-адрес источника, который в итоге использует правило трансляции SNAT. Например, опция **Outgoing Interface IP** означает, что устройство NXC использует IP address указанного исходящего интерфейса как IP-адрес источника для соответствующих критериям пакетов, которые он отправляет в соответствии с данным правилом.

33

Перезагрузка

33.1 Обзор

Здесь описан процесс перезагрузки устройства.

33.1.1 Что необходимо знать

Изменения, внесенные через Web-конфигуратор, сохраняются автоматически и не пропадают при перезагрузке. При внесении изменений через интерфейс командной строки, однако, необходимо использовать команду `write` для сохранения настроек перед перезагрузкой. В противном случае изменения после перезагрузки будут потеряны.

Перезагрузка (reboot) отличается от сброса (reset); сброс возвращает устройство к настройкам по умолчанию.

33.2 Экран Reboot

С помощью этого экрана удаленные пользователи могут выполнить перезагрузку устройства. Чтобы открыть этот экран, выберите в меню **Maintenance** > **Reboot**.

Рисунок 230 Экран Maintenance > Reboot

Нажмите кнопку **Reboot**, чтобы перезагрузить устройство NXC. Подождите несколько минут до появления экрана входа в систему. Если экран входа в систему не появляется, введите IP-адрес устройства в строке адреса веб-браузера.

Выполнить перезагрузку устройства NXC также можно с помощью соответствующей команды интерфейса командной строки.

34

Завершение работы устройства

34.1 Обзор

С помощью этого экрана можно завершить работу устройства.

Перед выключением устройства NXC или отсоединением питания необходимо обязательно выбрать в меню Maintenance > Shutdown > Shutdown или ввести команду `shutdown`. Невыполнение этого требования может привести к повреждению встроенного программного обеспечения.

34.1.1 Что необходимо знать

При завершении работы все данные, находящиеся в кэше, записываются в локальное хранилище, и происходит остановка системных процессов. Завершение работы отличается от сброса; сброс возвращает устройство к настройкам по умолчанию.

34.2 Экран Shutdown

Чтобы открыть этот экран, выберите в меню **Maintenance** > **Shutdown**.

Рисунок 231 Экран Maintenance > Shutdown

Нажмите на кнопку **Shutdown**, чтобы завершить работу устройства NXC. Дождитесь завершения работы устройства перед тем, как выключить его вручную или отключить от источника питания. Завершение работы устройства не приводит к его выключению.

Завершить работу устройства NXC можно также с помощью команды `shutdown`.

35

Поиск и устранение неполадок

35.1 Обзор

В данной главе описаны некоторые способы разрешения проблем, с которыми можно столкнуться при эксплуатации устройства.

35.1.1 Общие неисправности

В этом разделе содержится ряд советов и рекомендаций по поиску и устранению неполадок на устройстве.

Ни один из индикаторов не горит.

Удостоверьтесь, что шнур питания подключен к устройству NXC и соответствующему источнику питания. Удостоверьтесь, что оба шнура питания подключены к устройству NXC и к соответствующему источнику питания. Удостоверьтесь, что оба переключателя питания на устройстве NXC включены. Убедитесь, что устройство NXC включено. Проверьте все кабельные соединения.

Если индикаторы все равно не горят, то, возможно, неисправно оборудование. В этом случае необходимо связаться с местным поставщиком.

Не могу подключиться к устройству NXC из локальной сети.

- Проверьте кабельное соединение между устройством NXC и компьютером или коммутатором.
- Направьте ping-запрос с компьютера, находящегося в локальной сети, на устройство NXC. Удостоверьтесь, что на компьютере установлена сетевая карта Ethernet, и она исправно функционирует. Также убедитесь, что ее IP-адрес находится в той же подсети, что и IP-адрес устройства NXC.
- На компьютере выберите в меню **Start** > **Programs** > **Accessories** > **Command Prompt**. В окне **Command Prompt** наберите команду «ping», затем укажите IP-адрес устройства NXC в локальной сети (по умолчанию – 192.168.1.1) и нажмите клавишу [ENTER]. От устройства NXC должен прийти отклик.
- Если забыт пароль для входа на устройство NXC, воспользуйтесь кнопкой **RESET**. Нажмите эту кнопку и удерживайте ее нажатой в течение примерно 5 секунд (или до тех пор, пока индикатор **PWR** не начнет мигать). Эта кнопка возвращает заводские настройки по умолчанию для устройства NXC (пароль 1234, IP-адрес в локальной сети 192.168.1.1 и т.д.; более подробную информацию можно найти в Руководстве пользователя).

- Если IP-адрес устройства NXC забыт, можно подключиться к устройству через консольный порт и узнать адрес с помощью терминальных команд. Подключите компьютер к порту **CONSOLE** с помощью консольного кабеля. На компьютере должна быть установлена коммуникационная программа для эмуляции терминала (например, HyperTerminal). Для нее должны быть заданы следующие параметры: эмуляция терминала VT100, без проверки четности, 8 битов данных, 1 стоп-бит, без управления потоком и скорость порта 115200 бит/с.

У меня нет доступа к Интернету.

- Проверьте подключение устройства NXCк разъему Ethernet шлюза Интернет. Удостоверьтесь, что устройство, играющее роль шлюза Интернет (например, DSL-модем), функционирует корректно.
- Если устройство NXC работает в режиме по умолчанию (режиме моста), убедитесь, что DHCP-сервер, к которому подключено устройство NXC, выделяет IP-адреса надлежащим образом.
- Проверьте настройки безопасности устройства NXC, а также настройки интерфейсов и VLAN, чтобы убедиться в том, что клиентское устройств не было случайно исключено из числа устройств, которым разрешен доступ к сети или к Интернету.

Устройство NXC не применяет дополнительный маршрут на основе политик, который я создал.

Устройство NXC проверяет маршруты на основе политик в том порядке, в котором они присутствуют в списке. Соответственно, убедитесь, что дополнительный маршрут на основе политик идет в списке перед всеми остальными маршрутами, критериям которых трафик может также соответствовать.

Я не могу указать нужное мне имя интерфейса.

Формат имен всех интерфейсов, кроме интерфейсов Ethernet, подчиняется крайне жестким правилам. Каждое имя должно состоять из 2-4 букв (тип интерфейса) и следующего за ними числа (x, ограничивается максимальным количеством интерфейсов данного типа). Например, интерфейсы VLAN могут именоваться vlan0, vlan1, vlan2, ... и т.д.

Мои правила и настройки, которые применяются к определенному интерфейсу, больше не работают.

Возможно, у данного интерфейса поменялся IP-адрес. Чтобы избежать такой ситуации, создайте объект IP-адреса на основе данного интерфейса. В этом случае устройство NXC будет автоматически обновлять все правила и настройки, которые используют данный объект, при каждом изменении параметров IP-адреса данного интерфейса. Например, в случае изменения

IP-адреса интерфейса ge1 устройство NXC автоматически обновит соответствующий объект адреса подсети ge1 на основе данного интерфейса.

Хакеры получили доступ к моей беспроводной сети, в которой используется шифрование по протоколу WEP.

Протокол WEP является крайне небезопасным. Его шифр злоумышленник может взломать, воспользовавшись широко доступными программными средствами. Настоятельно рекомендуется использовать более эффективный механизм обеспечения безопасности. Используйте максимально мощный механизм обеспечения безопасности из числа тех, которые поддерживают все беспроводные устройства в сети. Рекомендуем использовать технологии WPA2 или WPA2-PSK.

Установленный мною таймер повторной аутентификации не работает в схеме безопасности беспроводной сети.

Если аутентификацию беспроводных станций выполняет сервер RADIUS, то таймер повторной аутентификации сервера RADIUS имеет приоритет перед введенными настройками. Измените настройки сервера RADIUS, если необходимо использовать другой интервал таймера повторной аутентификации.

Устройство NXC не применяет заданное ограничение пропускной способности для входящего трафика к интерфейсу.

На момент написания настоящего документа устройство NXC не поддерживает управление пропускной способностью ingress (то есть входящей пропускной способностью).

Устройство NXC маршрутизирует и применяет трансляцию SNAT для трафика с одних интерфейсов и не применяет ее к трафику с других интерфейсов.

Устройство NXC автоматически применяет трансляцию SNAT для трафика, который оно передает с внутренних интерфейсов на внешние. Например, оно делает это для трафика, идущего из локальной сети в сеть WAN. Чтобы добавить параметры маршрутизации и настройки SNAT для интерфейса, в настройках которого в поле **Interface Type** выбрана опция **General**, необходимо вручную настроить маршруты на основе политик. Кроме того, можно настроить маршруты на основе политик, заменяющие правила маршрутизации и алгоритмы SNAT по умолчанию для интерфейса, в настройках которого в поле **Interface Type** выбрана опция **Internal** или **External**.

Устройство NXC постоянно сбрасывает соединение.

Если IP-адрес альтернативного шлюза в локальной сети находится в той же подсети, что и IP-адрес устройства NXC в локальной сети, то возвратный трафик может идти в обход устройства NXC. Эта ситуация называется асимметричным или «треугольным» маршрутом. Это вынуждает устройство NXC сбрасывать соединение, поскольку оно не получает подтверждения.

Я изменил IP-адрес локальной сети и теперь не могу подключиться к Интернету.

Устройство NXC автоматически обновляет адресные объекты, созданные на основе IP-адреса, подсети или шлюза какого-либо интерфейса, при изменении настроек IP-адреса этого интерфейса. Тем не менее, придется вручную изменить свойства всех адресных объектов в локальной сети, которые не были созданы на основе этого интерфейса.

Я не могу настроить на сервере RADIUS аутентификацию учетной записи администратора устройства NXC по умолчанию.

Аутентификация учетной записи **admin** по умолчанию всегда происходит локально, независимо от настроек метода аутентификации.

Устройство NXC не может аутентифицировать учетные записи типа ext-user, которые я создал.

Для аутентификации учетной записи «ext-user» требуется использовать внешний сервер (AD, LDAP или RADIUS). Если устройство NXC попробует аутентифицировать пользователя типа **ext-user** с использованием локальной базы данных, такая попытка всегда завершится неудачей.

Я не могу добавить администраторов в пользовательскую группу с обычными пользователями.

Пользователей с правами «admin» невозможно добавить в одну группу с пользователями, имеющими права «access».

Я не могу добавить учетную запись администратора по умолчанию (admin) в группу пользователей.

Учетную запись по умолчанию **admin** невозможно включить в какую-либо группу пользователей.

Созданное мною расписание не применяется в указанные интервалы времени.

Удостоверьтесь, что текущие настройки даты и времени на устройстве NXC корректны.

Я не могу получить сертификат для импорта на устройство NXC.

1. На экране **My Certificates** можно импортировать сертификат, который совпадает с соответствующим запросом на сертификат, сгенерированным устройством NXC. Можно также импортировать сертификат в формате PKCS#12, включающий в себя открытый и секретный ключи.
2. Перед импортом необходимо удалить все пробелы в имени файла сертификата.
3. Система поддерживает импорт сертификатов, предоставленных исключительно в файлах следующих форматов:
   - Двоичный X.509: Это рекомендация ITU-T, которая описывает форматы сертификатов X.509.
   - X.509 с кодировкой PEM (Base-64): Этот формат почты с повышенной конфиденциальностью (Privacy Enhanced Mail) использует буквы в нижнем и верхнем регистрах и цифры для преобразования двоичного сертификата X.509 в печатную форму.
   - Двоичный PKCS#7: Это стандарт, который определяет общий синтаксис данных (включая цифровые подписи), которые могут быть зашифрованы. Файл в формате PKCS #7 используют для передачи сертификата с открытым ключом. Секретный ключ в этот файл не включается. В настоящее время устройство NXC разрешает импорт файла PKS#7, который содержит один сертификат.
   - PKCS#7 с шифрованием PEM (Base-64): Этот формат почты с повышенной конфиденциальностью (Privacy Enhanced Mail) использует буквы в нижнем и верхнем регистрах и цифры для преобразования двоичного сертификата PKCS#7 в печатную форму.
   - Двоичный PKCS#12: Это формат для передачи сертификатов с открытым и секретным ключами. Секретный ключ в файле PKCS #12 содержится в конверте, защищенном паролем. Пароль к файлу не связан с открытым или секретным паролем к сертификату. Пароль создается при экспорте файла PKCS #12, и его необходимо будет указать для дешифровки содержимого при импорте файла на устройство NXC.

Примечание: Будьте внимательны, не преобразуйте случайно двоичный файл в текстовый в процессе передачи. Это легко может произойти, потому что многие программы по умолчанию используют текстовый формат файлов для передачи.

Я не могу получить доступ к устройству NXC с компьютера, подключенного к Интернету.

Проверьте правила управления службами.

Я выгрузил логотип для отображения в левом верхнем углу страницы входа в Web-конфигуратор и захожу на эту страницу, но логотип не отображается должным образом.

Убедитесь, что файл логотипа имеет формат GIF, JPG или PNG, а его размер не превышает 100 Кбайт.

Я выгрузил логотип для использования в качестве фона для экрана или окна, но он не отображается должным образом.

Убедитесь, что файл логотипа имеет формат GIF, JPG или PNG, а его размер не превышает 100 Кбайт.

Пропускная способность NXC уменьшилась после того, как я начал собирать статистику по трафику.

Сбор данных может привести к уменьшению пропускной способности устройства NXC в плане передачи трафика.

Я вижу только новые журналы. Старые журналы пропали.

При достижении максимального количества сообщений в журнале новые сообщения начинают автоматически перетирать существующие, начиная с самых старых.

Команды в моем конфигурационном файле или сценарии командной строки не работают как полагается.

- В файле конфигурации или сценарии командной строки введите в начале строки символ «#» или «!», и тогда устройство NXC будет трактовать эту строку как комментарий.
- В файлах конфигурации или сценариях командной строки можно использовать оператор «exit» или командную строку, состоящую из единственного символа «!», для вывода устройства NXC из субкомандного режима.
- Не забудьте включить команду `write` в сценарии. В противном случае сделанные изменения будут потеряны при перезагрузке устройства NXC. В длинном сценарии нужно использовать несколько команд `write`.

Примечание: Оператор «exit» или символ «!» должны следовать за субкомандами, чтобы вывести устройство NXC из субкомандного режима.

Я не могу выгрузить встроенное программное обеспечение с помощью команд.

Для выгрузки встроенного программного обеспечения рекомендуется использовать Web-конфигуратор. Интерфейс командной строки следует использовать только в тех случаях, когда необходимо восстановить встроенное программное обеспечение. Чтобы узнать, как определить необходимость восстановления встроенного программного обеспечения и как его восстановить, обратитесь к Справочному руководству по интерфейсу командной строки.

При записи пакетов мне удалось записать меньшее количество пакетов, чем я рассчитывал, либо запись выполнить вообще не удалось.

Параметр **File Size** на экране записи пакетов устанавливает максимальное ограничение для совокупного размера всех файлов записей на устройстве NXC, включая существующие файлы записей и любые новые генерируемые файлы записей. Если имеются старые файлы записей, то, возможно, необходимо будет установить более высокий лимит или удалить какие-то из имеющихся файлов записей.

Устройство NXC останавливает запись и генерирует файл записи либо когда файл достигает размера, указанного в поле **File Size**, либо когда истекает временной интервал, указанный в поле **Duration**.

Не могу найти файлы записей пакетов, созданные ранее.

Новые файлы записываются поверх существующих файлов с тем же именем. Чтобы этого избежать, можно поменять значение в поле **File Suffix**.

35.1.2 Беспроводная сеть

В этом разделе содержатся советы по устранению неполадок на беспроводных устройствах, подключенных к устройству NXC.

Беспроводные клиенты не могут подключиться к точке доступа.

- Возможно, имеется несоответствие в конфигурациях точки доступа и устройства NXC. Это может быть следствием целого ряда проблем, таких, как неправильная топология VLAN, неправильные профили точек доступа, неверные настройки безопасности для соединения между точкой доступа и устройством NXC и т.д.

  В разд. 5.11 на стр. 75 можно найти информацию о том, как проверить, что идентификатор сети VLAN управления точки доступа совпадает с идентификатором сети VLAN управления, установленным на устройстве NXC для данной точки доступа.

  В разд. 5.11.1 на стр. 77 можно найти информацию о том, как проверить, что конфигурация данной точки доступа не вступает в конфликт с параметрами, установленными для данной точки доступа на устройстве NXC.

- MAC-адрес беспроводного клиента может присутствовать в списке фильтрации по MAC-адресам. В разд. 18.3.3 на стр. 246 можно найти подробную информацию об управлении фильтром по MAC-адресам на устройстве NXC.

- Беспроводному клиенту, возможно, не удается получить IP-адрес:

  Если устройство NXC работает в режиме моста, проверьте настройки на DHCP-сервере, ассоциированном с сетью.

  Проверьте собственные сетевые настройки беспроводного клиента, чтобы убедиться, что они предусматривают автоматическое получение IP-адреса.

  Если устройство NXC или подключенное к нему устройство, обеспечивающее доступ в Интернет, управляют сетью со статическими IP-адресами, удостоверьтесь, что параметры сервера, обеспечивающие выделение этих IP-адресов, настроены корректно.

  Проверьте собственные сетевые настройки беспроводного клиента, чтобы удостовериться, что ему уже назначен статический IP-адрес.

- Беспроводному клиенту, возможно, не удалось пройти аутентификацию на сервере аутентификации. Удостоверьтесь, что профиль точки доступа, назначенный данной точке доступа, использует профиль безопасности, который имеет правильные настройки и соответствует настройкам безопасности, используемым устройством NXC. Например, если на точке доступа установлен режим безопасности WPA/WPA2, то необходимо убедиться, что сервер аутентификации поддерживает и использует последовательный механизм аутентификации 802.1x. Более подробную информацию можно найти в гл. 18 на стр. 230 и в гл. 7 на стр. 99.

  Если профиль точки доступа использует профиль безопасности SSID, в соответствии с которым точка доступа задействует внешний сервер для аутентификации беспроводных клиентов по MAC-адресу, проверьте настройки аутентификации по MAC-адресу этого профиля безопасности SSID (см. разд. 18.3.2.1 на стр. 242).

- Включите журналирование работы точки доступа в беспроводной сети (см. разд. 29.3.2 на стр. 362).

- Проверьте в журнале точки доступа в беспроводной сети (разд. 5.17 на стр. 88) записи, относящиеся к WTP. Аббревиатура WTP расшифровывается как «Wireless Terminal Point» («беспроводная терминальная точка») и является эквивалентом точки доступа.

- Если решить проблему самостоятельно не удается, то перед тем, как обратиться в службу поддержки клиентов, воспользуйтесь встроенными средствами записи беспроводных кадров (гл. 31 на стр. 385) для записи данных, которые могут помочь более детально проанализировать проблему. Чтобы воспользоваться встроенными средствами записи беспроводных кадров, необходимо вначале перевести вторую точку доступа, находящуюся поблизости, в режим мониторинга (гл. 7 на стр. 99).

Состояние точки доступа регистрируется как оффлайн, хотя точка доступа находится в режиме онлайн.

- Проверьте сетевые соединения между устройством NXC и точкой доступа, чтобы убедиться в том, что они не повреждены.
- Возможно, точка доступа работает нестабильно. Отключите ее от сети, выключите питание, подождите некоторое время, затем снова подключите ее к сети и посмотрите, не исчезла ли проблема.
- Возможно, отключен процесс (daemon) CAPWAP. Можно воспользоваться встроенными инструментами диагностики устройства NXC и консолью командной строки для записи отладочных сообщений CAPWAP, которые впоследствии могут быть предоставлены в службу поддержки клиентов для анализа. Дополнительную информацию можно найти в гл. 3 на стр. 29.

Не удается аутентифицировать беспроводного клиента через непокидаемый портал.

Если непокидаемый портал переадресует беспроводного клиента на страницу «Не удалось выполнить вход» или страницу внутренней ошибки сервера, то это означает, что сервер аутентификации может быть недоступен. Удостоверьтесь, что устройство NXC может установить связь с сервером аутентификации вне локальной сети. Для этого откройте окно консоли и направьте ping-запрос на IP-адрес сервера.

Если непокидаемый портал использует внешний веб-портал:

- Удостоверьтесь, что параметры непокидаемого портала, ссылающиеся на внешний портал, настроены правильно. Необходимо проверить поле **Login URL**.
- Убедитесь в правильности настроек внешнего веб-сервера.
- Внешний веб-сервер рекомендуется размещать в той же подсети, в которой находятся пользователи, попадающие на страницу входа в систему.

Устройство NXC направляет беспроводных клиентов на страницу выхода из системы по умолчанию вместо страницы входа в систему.

Убедитесь в правильности настройки поля **Login URL**, отвечающего за связь непокидаемого портала с внешним порталом.

Режим балансировки нагрузки со стороны беспроводных клиентов для моих точек доступа не работает.

- Убедитесь, что у всех точек доступа, обслуживающих этих беспроводных клиентов, совпадают идентификатор сети SSID, параметры безопасности и настройки радиопередатчика.
- Удостоверьтесь, что все эти точки доступа принадлежат одному широковещательному домену.
- Убедитесь, что эти беспроводные клиенты находятся в диапазоне остальных точек доступа; если они находятся в диапазоне только одной точки доступа, то режим балансировки нагрузки может быть неэффективен.

На экране **Monitor > Wireless > AP Info > AP List** нет индикатора режима балансировки нагрузки, ассоциированного с какой-либо из точек доступа, принимающих участие в балансировке нагрузки.

- Убедитесь, что профиль точки доступа, содержащий настройки балансировки нагрузке, корректно назначен рассматриваемым точкам доступа.
- Задача балансировки нагрузки могла быть завершена, поскольку далее балансировка нагрузки для рассматриваемых точек доступа не требуется.

35.2 Сброс устройства NXC

Если невозможно установить связь с устройством NXC никаким образом, попробуйте перезагрузить его, выключив и снова включив питание. Если и после этого установить связь с устройством NXC никаким образом не получается, или забыт пароль администратора, можно сбросить конфигурацию устройства NXC до настроек по умолчанию. Любые файлы конфигурации или сценарии командной строки, которые были сохранены на устройстве NXC, должны быть доступны и после сброса настроек.

Воспользуйтесь описанной ниже процедурой, чтобы вернуть конфигурацию устройства NXC к настройкам по умолчанию. Настройки, описанные в файле startup-config.conf, будут заменены настройками из файла system-default.conf.

Примечание: Данная процедура удалит текущую конфигурацию.

1 Убедитесь, что индикатор **SYS** горит и при этом не мигает.

2 Нажмите кнопку **RESET** и удерживайте ее нажатой до тех пор, пока индикатор **SYS** не начнет мигать. (Обычно это происходит примерно через пять секунд).

3 Отпустите кнопку **RESET** и дождитесь перезагрузки устройства NXC.

Теперь должна появиться возможность доступа к устройству NXC с использованием настроек по умолчанию.

35.3 Дополнительная помощь в устранении неполадок

Ищите дополнительную информацию, которая может помочь в устранении проблем, возникших с устройством конкретной модели, на сайте www.zyxel.com.

A

Описание журналов

В этом разделе приведено описание сообщений, которые могут встречаться в журналах.

Журналы ZySH содержат сообщения о внутренних ошибках системы.

Таблица 194 Журналы ZySH

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Invalid message queue. Maybe someone starts another zysh daemon.	Неверная очередь сообщений. Возможно, кто-то запустил еще один процесс (демон) zysh.
ZySH daemon is instructed to reset by %d	%d направил инструкцию сброса на демон ZySH 1-я перем.: номер pid
System integrity error!	Ошибка целостности системы!
Group OPS	групповые операции
cannot close property group	невозможно правильно закрыть группу свойств
cannot close group	невозможно закрыть группу
%s: cannot get size of group	%s: невозможно получить размер группы 1-я перем.: имя группы zysh
%s: cannot specify properties for entry %s	%s: невозможно указать свойства для записи %s 1-я перем.: имя группы zysh, 2-я перем.: имя записи zysh
%s: cannot join group %s, loop detected	%s: невозможно присоединиться к группе %s, обнаружена петля 1-я перем.: имя группы zysh, 2-я перем.: имя группы zysh
cannot create, too many groups (>%d)	невозможно создать, слишком много групп (>%d) 1-я перем.: макс. кол-во групп
%s: cannot find entry %s	%s: невозможно найти запись %s 1-я перем.: имя группы zysh, 2-я перем.: имя записи zysh
%s: cannot remove entry %s	%s: невозможно удалить запись %s 1-я перем.: имя группы zysh, 2-я перем.: имя записи zysh
List OPS	операции со списками
can't alloc entry: %s!	невозможно выделить запись: %s! 1-я перем.: имя записи zysh
can't retrieve entry: %s!	невозможно извлечь запись: %s! 1-я перем.: имя записи zysh
can't get entry: %s!	невозможно получить запись: %s! 1-я перем.: имя записи zysh

Таблица 194 Журналы ZySH (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
can't print entry: %s!	невозможно распечатать запись: %s! 1-я перем.: имя записи zysh
%s: cannot retrieve entries from list!	%s: невозможно извлечь записи из списка! 1-я перем.: имя списка zysh
can't get name for entry %d!	невозможно получить имя для записи %d! 1-я перем.: порядковый номер записи zysh
can't get reference count: %s!	невозможно получить эталонный счетчик: %s! 1-я перем.: имя списка zysh
can't print entry name: %s!	невозможно распечатать имя записи: %s! 1-я перем.: имя записи zysh
Can't append entry: %s!	невозможно добавить запись: %s! 1-я перем.: имя записи zysh
Can't set entry: %s!	невозможно установить запись: %s! 1-я перем.: имя записи zysh
Can't define entry: %s!	невозможно определить запись: %s! 1-я перем.: имя записи zysh
%s: list is full!	%s: список заполнен! 1-я перем.: имя списка zysh
Can't undefine %s	невозможно отменить определение %s 1-я перем.: имя списка zysh
Can't remove %s	невозможно удалить %s 1-я перем.: имя списка zysh
Table OPS	операции с таблицами
%s: cannot retrieve entries from table!	%s: невозможно извлечь записи из таблицы! 1-я перем.: имя таблицы zysh
%s: index is out of range!	%s: индекс вне диапазона! 1-я перем.: имя таблицы zysh
%s: cannot set entry #%d	%s: невозможно установить запись #%d 1-я перем.: имя таблицы zysh, 2-я перем.: номер записи zysh
%s: table is full!	%s: таблица заполнена! 1-я перем.: имя таблицы zysh
%s: invalid old/new index!	%s: неверный старый/новый индекс! 1-я перем.: имя таблицы zysh
Unable to move entry #%d!	невозможно переместить запись #%d! 1-я перем.: номер записи zysh
%s: invalid index!	%s: неверный индекс! 1-я перем.: имя таблицы zysh

Таблица 194 Журналы ZySH (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Unable to delete entry #%d!	невозможно удалить запись #%d! 1-я перем.: номер записи zysh
Unable to change entry #%d!	невозможно изменить запись #%d! 1-я перем.: номер записи zysh
%s: cannot retrieve entries from table!	%s: невозможно извлечь записи из таблицы! 1-я перем.: имя таблицы zysh
%s: invalid old/new index!	%s: неверный старый/новый индекс! 1-я перем.: имя таблицы zysh
Unable to move entry #%d!	невозможно переместить запись #%d! 1-я перем.: номер записи zysh
%s: apply failed at initial stage!	%s: не удалось применить на начальном этапе! 1-я перем.: имя таблицы zysh
%s: apply failed at main stage!	%s: не удалось применить на основном этапе! 1-я перем.: имя таблицы zysh
%s: apply failed at closing stage!	%s: не удалось применить на завершающем этапе! 1-я перем.: имя таблицы zysh

Таблица 195 Журналы пользователей

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
%s %s from %s has logged in EnterpriseWLAN	Пользователь выполнил вход на устройство NXC. 1-я перем. %s: Тип учетной записи пользователя. 2-я перем. %s: Имя пользователя. 3-я перем. %s: Тип службы, которую использует пользователь (HTTP, HTTPS, FTP, Telnet, SSH или консоль).
%s %s from %s has logged out EnterpriseWLAN	Пользователь выполнил выход из устройства NXC. 1-я перем. %s: Тип учетной записи пользователя. 2-я перем. %s: Имя пользователя. 3-я перем. %s: Тип службы, которую использует пользователь (HTTP, HTTPS, FTP, Telnet, SSH или консоль).
%s %s from %s has been logged out EnterpriseWLAN (re-auth timeout)	Устройство NXC прерывает сессию указанного пользователя по тайм-ауту повторной аутентификации. 1-я перем. %s: Тип учетной записи пользователя. 2-я перем. %s: Имя пользователя. 3-я перем. %s: Тип службы, которую использует пользователь (HTTP, HTTPS, FTP, Telnet, SSH или консоль).

Таблица 195 Журналы пользователей (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
%s %s from %s has been logged out EnterpriseWLAN (lease timeout)	Устройство NXC прерывает сессию указанного пользователя по тайм-ауту аренды. 1-я перем. %s: Тип учетной записи пользователя. 2-я перем. %s: Имя пользователя. 3-я перем. %s: Тип службы, которую использует пользователь (HTTP, HTTPS, FTP, Telnet, SSH или консоль).
%s %s from %s has been logged out EnterpriseWLAN (idle timeout)	Устройство NXC прерывает сессию указанного пользователя по тайм-ауту неактивности. 1-я перем. %s: Тип учетной записи пользователя. 2-я перем. %s: Имя пользователя. 3-я перем. %s: Тип службы, которую использует пользователь (HTTP, HTTPS, FTP, Telnet, SSH или консоль).
Console has been put into lockout state	Слишком много неудачных попыток входа в систему через порт консоли, поэтому устройство NXC блокирует попытки входа в систему через порт консоли.
Address %u.%u.%u.%u has been put into lockout state	Слишком много неудачных попыток входа в систему с данного IP-адреса, поэтому устройство NXC блокирует попытки входа в систему с данного IP-адреса. %u.%u.%u.%u: адрес источника при попытке входа пользователя в систему
Failed login attempt to EnterpriseWLAN from %s (login on a lockout address)	Попытка входа в систему с IP-адреса, заблокированного устройством NXC. %u.%u.%u.%u: адрес источника при попытке входа пользователя в систему
Failed login attempt to EnterpriseWLAN from %s (reach the max. number of user)	Устройство NXC заблокировало попытку входа, поскольку достигнуто максимальное число входов в систему, допустимое для данной службы. %s: имя службы
Failed login attempt to EnterpriseWLAN from %s (reach the max. number of simultaneous logon)	Устройство NXC заблокировало попытку входа, поскольку достигнуто максимальное число одновременных входов в систему для учетных записей администраторов или обычных пользователей. %s: имя службы
User %s has been denied access from %s	Устройство NXC заблокировало попытку входа в соответствии с настройками управления доступом. %s: имя службы
User %s has been denied access from %s	Устройство NXC заблокировало попытку входа под указанным именем, поскольку либо имя пользователя, либо пароль указаны неверно. 2-я перем. %s: имя службы
LDAP/AD: Wrong IP or Port. IP:%s, Port: %d	LDAP/AD: Неверный IP-адрес или порт. Проверьте настройку сервера AAA.
Domain-auth fail	Не удалось выполнить доменную аутентификацию. Проверьте настройки, связанные с доменной аутентификацией.
Failed to join domain: Access denied	Не удалось присоединиться к домену: Доступ запрещен. Проверьте сервер AD.

Таблица 196 Журналы регистрации

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Send registration message to MyZyXEL.com server has failed.	Устройству не удалось отправить сообщение о регистрации на MyZyXEL.com.
Get server response has failed.	Устройство отправило пакеты на сервер MyZyXEL.com, но не получило ответа. Причина может заключаться в ненормальной работе соединения.
Timeout for get server response.	zysh должен получить код возврата агента MyZyXEL.com; это сообщение в журнале появится по истечении тайм-аута.
User has existed.	Такое имя пользователя уже существует в базе данных MyZyXEL.com. Соответственно, это имя пользователя нельзя использовать для регистрации устройства, необходимо указать другое имя.
User does not exist.	Это имя пользователя отсутствует в базе данных MyZyXEL.com. Соответственно, его можно использовать для регистрации устройства.
Internal server error.	При поиске имени пользователя в базе данных MyZyXEL.com произошла ошибка.
Device registration has failed:%s.	Не удалось выполнить регистрацию устройства, сообщение об ошибке, возвращенное сервером MyZyXEL.com, будет добавлено к сообщению в журнале. %s: сообщение об ошибке, возвращенное сервером myZyXEL.com
Device registration has succeeded.	Устройство успешно зарегистрировано на сервере myZyXEL.com.
Registration has failed. Because of lack must fields.	Устройство получило неполный ответ от сервера myZyXEL.com, и это привело к ошибке синтаксического разбора.
%s:Trial service activation has failed:%s.	Не удалось выполнить пробную активацию указанной службы, сообщение об ошибке, возвращенное сервером MyZyXEL.com, будет добавлено к сообщению в журнале. 1-я перем. %s: имя службы 2-я перем. %s: сообщение об ошибке, возвращенное сервером myZyXEL.com
%s:Trial service activation has succeeded.	Пробная активация указанной службы успешно выполнена. %s: имя службы
Trial service activation has failed. Because of lack must fields.	Устройство получило неполный ответ от сервера myZyXEL.com, и это привело к ошибке синтаксического разбора.
Standard service activation has failed:%s.	Не удалось выполнить стандартную активацию службы, сообщение об ошибке, возвращенное сервером MyZyXEL.com, будет добавлено к сообщению в журнале. %s: сообщение об ошибке, возвращенное сервером myZyXEL.com
Standard service activation has succeeded.	Стандартная активация службы выполнена успешно.
Standard service activation has failed. Because of lack must fields.	Устройство получило неполный ответ от сервера myZyXEL.com, и это привело к ошибке синтаксического разбора.

Таблица 196 Журналы регистрации (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Service expiration check has failed:%s.	Не удалось выполнить проверку даты окончания срока действия службы, сообщение об ошибке, возвращенное сервером MyZyXEL.com, будет добавлено к сообщению в журнале. %s: сообщение об ошибке, возвращенное сервером myZyXEL.com
Service expiration check has succeeded.	Проверка даты окончания срока действия службы выполнена успешно.
Service expiration check has failed. Because of lack must fields.	Устройство получило неполный ответ от сервера myZyXEL.com, и это привело к ошибке синтаксического разбора.
Server setting error.	Устройство не может получить IP-адрес или полное имя (FQDN) сервера myZyXEL.com из локальной сети.
Resolve server IP has failed.	Устройству не удалось разрешить полное имя (FQDN) сервера myZyXEL.com в IP-адрес с помощью функции gethostbyname().
Verify server's certificate has failed.	Устройству не удалось обработать соединение HTTPS, поскольку оно не смогло проверить сертификат сервера myZyXEL.com.
Connect to MyZyXEL.com server has failed.	Устройству не удалось подключиться к серверу MyZyXEL.com.
Do account check.	Устройство начало поиск имени пользователя в базе данных MyZyXEL.com.
Do device register.	Устройство начало процедуру регистрации устройства.
Do trial service activation.	Устройство начало процедуру пробной активации службы.
Do standard service activation.	Устройство начало процедуру стандартной активации службы.
Do expiration check.	Устройство начало проверку даты окончания срока действия службы.
Build query message has failed.	В пакетах, отправленных устройством на сервер MyZyXEL.com, отсутствует часть информации.
Parse receive message has failed.	Устройству не удается произвести синтаксический разбор ответа, возвращенного сервером MyZyXEL.com. Возможно, отсутствуют некоторые обязательные поля.
Resolve server IP has failed. Update stop.	Процедура обновления остановлена, поскольку устройству не удалось разрешить полное имя (FQDN) сервера myZyXEL.com в IP-адрес с помощью функции gethostbyname().
Verify server's certificate has failed. Update stop.	Устройству не удалось обработать соединение HTTPS, поскольку оно не смогло проверить сертификат сервера myZyXEL.com. Процесс обновления остановлен.
Send download request to update server has failed.	Устройству не удалось отправить сообщение о загрузке на сервер обновлений.
Get server response has failed.	Устройство отправило пакеты на сервер MyZyXEL.com, но не получило ответа. Причина может заключаться в ненормальной работе соединения.
Timeout for get server response.	zysh должен получить код возврата агента MyZyXEL.com; это сообщение в журнале появится по истечении тайм-аута.
Send update request to update server has failed.	Устройству не удалось отправить сообщение об обновлении на сервер обновлений.

Таблица 196 Журналы регистрации (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Update has failed. Because of lack must fields.	Устройство получило неполный ответ от сервера обновлений, и это привело к ошибке синтаксического разбора.
Update server is busy now. File download after %d seconds.	Сервер обновлений перегружен, поэтому устройство будет ожидать указанное количество секунд, а затем снова направит запрос на загрузку на сервер обновлений.
Device has latest file. No need to update.	На устройстве уже установлена последняя версия этого файла, поэтому обновления не требуется.
Device has latest signature file; no need to update	На устройстве уже установлена последняя версия файла сигнатуры, поэтому обновления не требуется.
Connect to update server has failed.	Устройству не удается подключиться к серверу обновлений.
Wrong format for packets received.	Устройству не удается выполнить синтаксический разбор ответа, возвращенного сервером. Возможно, отсутствуют некоторые обязательные поля.
Server setting error. Update stop.	Устройству не удалось разрешить полное имя (FQDN) сервера обновлений в IP-адрес с помощью функции gethostbyname(). Процесс обновления остановлен.
Build query message failed.	В пакетах, отправленных устройством на сервер, отсутствует часть информации.
System protect signature download has succeeded.	Загрузка файла сигнатуры для защиты системы на устройство успешно выполнена.
System protect signature update has succeeded.	Файл сигнатуры для защиты системы успешно загружен и применен на устройстве.
System protect signature download has failed.	Устройству не удается загрузить файл сигнатуры для защиты системы после 3 повторных попыток.
Resolve server IP has failed.	Устройству не удалось разрешить полное имя (FQDN) сервера myZyXEL.com в IP-адрес с помощью функции gethostbyname().
Connect to MyZyXEL.com server has failed.	Устройству не удалось подключиться к серверу MyZyXEL.com.
Build query message has failed.	В пакетах, отправленных устройством на сервер, отсутствует часть информации.
Verify server's certificate has failed.	Устройству не удалось обработать соединение HTTPS, поскольку оно не смогло проверить сертификат сервера.
Get server response has failed.	Устройство отправило пакеты на сервер, но не получило ответа. Причина может заключаться в ненормальной работе соединения.
Expiration daily-check has failed:%s.	Не удалось выполнить ежедневную проверку окончания срока действия службы, сообщение об ошибке, возвращенное сервером MyZyXEL.com, будет добавлено к сообщению в журнале. %s: сообщение об ошибке, возвращенное сервером myZyXEL.com

Таблица 196 Журналы регистрации (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Do expiration daily-check has failed. Because of lack must fields.	Устройство получило неполный ответ на ежедневный запрос для проверки окончания срока действия службы, и полученные пакеты привели к ошибке синтаксического разбора.
Server setting error.	Устройство не может получить IP-адрес или полное имя (FQDN) сервера из локальной сети.
Do expiration daily-check has failed.	Не удалось выполнить ежедневную проверку окончания срока действия службы.
Do expiration daily-check has succeeded.	Ежедневная проверка окончания срока действия службы выполнена успешно.
System bootup. Do expiration daily-check.	Устройство выполнит ежедневную проверку окончания срока действия службы сразу по завершении загрузки.
After register. Do expiration daily-check immediately.	Устройство выполнит ежедневную проверку окончания срока действия службы сразу после регистрации устройства.
Time is up. Do expiration daily-check.	Устройство выполняет ежедневную проверку окончания срока действия службы каждые 24 часа.
Read MyZyXEL.com storage has failed.	Не удалось выполнить чтение данных из энергонезависимой памяти EEPROM.
Open /proc/MRD has failed.	При попытке получения MAC-адреса появляется сообщение об ошибке.
Unknown TLS/SSL version: %d.	Данное устройство поддерживает только протокол SSLv3. %d: Версия SSL, назначенная клиентом.
Load trusted root certificates has failed.	Устройству необходимо загрузить доверенный корневой сертификат для проверки сертификата сервера. Это сообщение появится в журнале, если устройству не удалось загрузить доверенный корневой сертификат.
Certificate has expired.	Не удалось выполнить проверку сертификата сервера, поскольку срок его действия истек.
Self signed certificate.	Не удалось выполнить проверку сертификата сервера, поскольку он является самоподписанным.
Self signed certificate in certificate chain.	Не удалось выполнить проверку сертификата сервера, поскольку в цепочке сертификатов сервера присутствует самоподписанный сертификат.
Verify peer certificates has succeeded.	Устройство успешно выполнило проверку сертификата сервера при обработке соединения HTTPS.
Certification verification failed: Depth: %d, Error Number(%d):%s.	Не удалось выполнить проверку сертификата сервера при обработке соединения HTTPS. Это сообщение указывает на причину неудачи. 1-я перем. %d: уровень в цепочке сертификатов 2-я перем. %d: номер ошибки %s: сообщения об ошибках
Certificate issuer name:%s.	Не удалось выполнить проверку указанного сертификата, поскольку устройство не смогло получить имя издателя сертификата. %s – имя сертификата.

Таблица 196 Журналы регистрации (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
The wrong format for HTTP header.	Заголовок пакета, возвращенного сервером, имеет неверный формат.
Timeout for get server response.	После отправки пакетов на сервер устройство не получило от сервера никакого ответа. Причина может заключаться в сетевой задержке.
Download file size is wrong.	Размер файла, загруженного для сервера приложений, отличается от длины контента
Parse HTTP header has failed.	Устройству не удается выполнить синтаксический разбор заголовка HTTP в ответе, возвращенном сервером. Возможно, отсутствует некоторые заголовки HTTP.

Таблица 197 Журналы ограничений на сессии

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Maximum sessions per host (%d) was exceeded.	%d – это максимальное одновременное количество сессий с одного хоста.

Таблица 198 Журналы маршрутов на основе политик

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Can't open bwm_entries	Маршрутизация на основе политик не может активировать функцию BWM.
Can't open link_down	Маршрутизация на основе политик не может определить состояние соединения (подключено/отключено).
Cannot get handle from UAM, user-aware PR is disabled	Политика, учитывающая сведения о пользователе, по каким-то причинам отключена.
mblock: allocate memory failed!	Не удалось применить правило маршрутизации на основе политик: недостаточно памяти.
pt: allocate memory failed!	Не удалось применить правило маршрутизации на основе политик: недостаточно памяти.
To send message to policy route daemon failed!	Не удалось отправить управляющее сообщение диспетчеру маршрутизации на основе политик.
The policy route %d allocates memory fail!	Не удалось применить правило маршрутизации на основе политик: недостаточно памяти. %d: номер правила в маршруте на основе политик
The policy route %d uses empty user group!	Используется пустая группа объектов. %d: номер правила в маршруте на основе политик
The policy route %d uses empty source address group!	Используется пустая группа объектов. %d: номер правила в маршруте на основе политик
The policy route %d uses empty destination address group!	Используется пустая группа объектов. %d: номер правила в маршруте на основе политик

Таблица 198 Журналы маршрутов на основе политик (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
The policy route %d uses empty service group	Используется пустая группа объектов. %d: номер правила в маршруте на основе политик
Policy-route rule %d was inserted.	Выполнена вставка правил в систему. %d: номер правила в маршруте на основе политик
Policy-route rule %d was appended.	Правила добавлены в систему. %d: номер правила в маршруте на основе политик
Policy-route rule %d was modified.	Правило изменено. %d: номер правила в маршруте на основе политик
Policy-route rule %d was moved to %d.	Правило перемещено. 1-я перем. %d: номер правила в исходном маршруте на основе политик 2-я перем. %d: номер правила в новом маршруте на основе политик
Policy-route rule %d was deleted.	Правило удалено. %d: номер правила в маршруте на основе политик
Policy-route rules were flushed.	Выполнена очистка правил маршрутизации на основе политик.
BWM has been activated.	Глобальная опция управления пропускной способностью на устройстве NXC включена.
BWM has been deactivated.	Глобальная опция управления пропускной способностью на устройстве NXC выключена.

Таблица 199 Встроенные журналы служб

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
User on %u.%u.%u.%u has been denied access from %s	Доступ к устройству по протоколу HTTP/HTTPS/TELNET/SSH/FTP/SNMP был запрещен. %u.%u.%u.%u – это IP-адрес %s – один из протоколов HTTP/HTTPS/SSH/SNMP/FTP/TELNET
HTTPS certificate:%s does not exist. HTTPS service will not work.	Администратор назначил для HTTPS несуществующий сертификат. %s – имя сертификата, назначенного пользователем
HTTPS port has been changed to port %s.	Администратор изменил номер порта для HTTPS. %s – номер порта
HTTPS port has been changed to default port.	Администратор вернул для HTTPS номер порта по умолчанию (443).
HTTP port has changed to port %s.	Администратор изменил номер порта для HTTP. %s – номер порта, назначенного пользователем
HTTP port has changed to default port.	Администратор вернул для HTTP номер порта по умолчанию (80).
SSH port has been changed to port %s.	Администратор изменил номер порта для SSH. %s – номер порта, назначенного пользователем

Таблица 199 Встроенные журналы служб (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
SSH port has been changed to default port.	Администратор вернул для SSH номер порта по умолчанию (22).
SSH certificate:%s does not exist. SSH service will not work.	Администратор назначил для SSH несуществующий сертификат. %s – имя сертификата, назначенного пользователем
SSH certificate:%s format is wrong. SSH service will not work.	После того, как администратор назначит сертификат для SSH, устройство должно преобразовать его в ключ, используемый для SSH. %s – имя сертификата, назначенного пользователем
TELNET port has been changed to port %s.	Администратор изменил номер порта для TELNET. %s – номер порта, назначенного пользователем
TELNET port has been changed to default port.	Администратор вернул для TELNET номер порта по умолчанию (23).
FTP certificate:%s does not exist.	Администратор назначил для FTP несуществующий сертификат. %s – имя сертификата, назначенного пользователем
FTP port has been changed to port %s.	Администратор изменил номер порта для FTP. %s – номер порта, назначенного пользователем
FTP port has been changed to default port.	Администратор вернул для FTP номер порта по умолчанию (21).
SNMP port has been changed to port %s.	Администратор изменил номер порта для SNMP. %s – номер порта, назначенного пользователем
SNMP port has been changed to default port.	Администратор вернул для SNMP номер порта по умолчанию (161).
Console baud has been changed to %s.	Администратор изменил скорость передачи в бодах для порта консоли. %s – скорость в бодах, назначенная пользователем
Console baud has been reset to %d.	Администратор вернул для порта консоли скорость в бодах по умолчанию (115200). %d – скорость в бодах по умолчанию
DHCP Server on Interface %s will not work due to Device HA status is Stand-By	Если интерфейс находится в режиме ожидания в схеме высокой доступности (HA), запустить DHCP-сервер на нем нельзя, иначе он вступит в конфликт с интерфейсом, работающем в режиме основного узла. %s – имя интерфейса
DHCP Server on Interface %s will be reapplied due to Device HA status is Active	Если интерфейс переходит в режим главного узла в схеме высокой доступности (HA), то на нем необходимо запустить DHCP-сервер. %s – имя интерфейса
DHCP's DNS option:%s has changed.	Поддержка опции DNS DHCP-пула со стороны интерфейса WAN. При смене состояния этого интерфейса (подключении/отключении) данное сообщение появится в журнале. %s – имя интерфейса. Опция DNS DHCP-пула получена от этого интерфейса

Таблица 199 Встроенные журналы служб (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Set timezone to %s.	Администратор изменил часовой пояс. %s – значение часового пояса
Set timezone to default.	Администратор вернул для часового пояса значение по умолчанию (0).
Enable daylight saving.	Администратор включил опцию перехода на летнее время.
Disable daylight saving.	Администратор отключил опцию перехода на летнее время.
DNS access control rules have been reached the maximum number.	Администратор попытался создать больше правил управления доступом DNS, чем разрешено (64).
DNS access control rule %u of DNS has been appended.	Администратор добавил новое правило. %u – номер правила
DNS access control rule %u has been inserted.	Администратор вставил новое правило. %u – номер правила
DNS access control rule %u has been appended	Администратор добавил новое правило. %u – номер правила
DNS access control rule %u has been modified	Администратор изменил правило %u. %u – номер правила
DNS access control rule %u has been deleted.	Администратор удалил правило %u. %u – номер правила
DNS access control rule %u has been moved to %d.	Администратор изменил порядковый номер правила с %u на %d. %u – предыдущий порядковый номер %d – новый порядковый номер
The default record of Zone Forwarder have reached the maximum number of 128 DNS servers.	Количество DNS-серверов в записи по умолчанию превысило 128.
Interface %s ping check is successful. Zone Forwarder adds DNS servers in records.	Проверка посредством ping пройдена успешно, добавление DNS-серверов в BIND. %s – имя интерфейса
Interface %s ping check is failed. Zone Forwarder removes DNS servers in records.	Не удалось пройти проверку посредством ping, удаление DNS-серверов из BIND. %s – имя интерфейса

Таблица 199 Встроенные журналы служб (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Interface %s ping check is disabled. Zone Forwarder adds DNS servers in records.`	Проверка посредством ping отключена, добавление DNS-серверов в BIND. %s – имя интерфейса
`Wizard apply DNS server failed.`	Не удалось применить параметры DNS-сервера с помощью мастера настройки.
`Wizard adds DNS server %s failed because DNS zone setting has conflictd.`	Не удалось применить параметры DNS-сервера с помощью мастера настройки из-за конфликта зоны (или зон) DNS. %s – IP-адрес DNS-сервера
`Wizard adds DNS server %s failed because Zone Forwarder numbers have reached the maximum number of 32.`	Не удалось применить параметры DNS-сервера с помощью мастера настройки, поскольку количество DNS-записей на устройстве достигло предельного значения. %s – IP-адрес DNS-сервера.
`Access control rules of %s have reached the maximum number of %u`	Достигнуто предельное количество правил управления доступом. %s – HTTP/HTTPS/SSH/SNMP/FTP/TELNET. %u – предельное количество правил управления доступом.
`Access control rule %u of %s was appended.`	Добавлено новое правило управления доступом для встроенной службы. %u – порядковый номер правила управления доступом. %s – HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was inserted.`	Правило управления доступом успешно вставлено. %u – порядковый номер правила управления доступом. %s – HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was modified.`	Правило управления доступом успешно изменено. %u – порядковый номер правила управления доступом. %s – HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %u of %s was deleted.`	Правило управления доступом успешно удалено. %u – порядковый номер правила управления доступом. %s – HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
`Access control rule %d of %s was moved to %d.`	Порядковый номер правила управления доступом успешно изменен. 1-я перем. %d – предыдущий порядковый номер. %s – HTTP/HTTPS/SSH/SNMP/FTP/TELNET. 2-я перем. %d – новый порядковый номер.
`SNMP trap can not be sent successfully`	Не удалось отправить «ловушку» SNMP удаленному хосту из-за сетевой ошибки

Таблица 200 Системный журнал

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Port %d is up!!	Если соединение подключено, %d – номер порта.
Port %d is down!!	Если соединение отключено, %d – номер порта.
%s is dead at %s	Процесс (daemon) исчез (был удален операционной системой). 1-я перем. %s: имя процесса, 2-я перем. %s: дата и время
%s process count is incorrect at %s	Счетчик процесса показывает неверное значение. 1-я перем. %s: имя процесса, 2-я перем. %s: дата и время
%s becomes Zombie at %s	Процесс присутствует, но не функционирует. 1-я перем. %s: имя процесса, 2-я перем. %s: дата и время Если объем используемой оперативной памяти превышает threshold-max, то он достигает значения %d%% :mem-threshold-max. Если объем используемых ресурсов локального хранилища превышает threshold-max, то объем используемых ресурсов файловой системы %s: Partition name достигает значения %d%%: disk-threshold-max. Если объем используемой оперативной памяти опускается ниже threshold-min, то объем используемых ресурсов системной памяти опускается ниже порогового значения %d%%: mem-threshold-min. Если объем используемых ресурсов локального хранилища опускается ниже threshold-min, то объем используемых ресурсов файловой системы %s: partition_name опускается ниже порогового значения %d%%: disk-threshold-min.
DHCP-сервер запущен со включенным безопасным режимом	DHCP-сервер запущен со включенным безопасным режимом.
DHCP-сервер запущен с отключенным безопасным режимом	DHCP-сервер запущен с отключенным безопасным режимом.
Received packet is not an ARP response packet	Полученный пакет не является пакетом ответа ARP.
Receive an ARP response	Устройство получило ответ ARP.
Receive ARP response from %s (%s)	Устройство получило ответ ARP от указанного источника.
The request IP is: %s, sent from %s	Устройство приняло запрос.
Received ARP response NOT for the request IP address	Устройство получило ответ ARP, который НЕ предназначен для запрашиваемого IP-адреса.
Receive an ARP response from the client issuing the DHCP request	Устройство получило ответ ARP от клиента, инициирующего DHCP-запрос.
Receive an ARP response from an unknown client	Устройство получило ответ ARP от неизвестного клиента.

Таблица 200 Системный журнал (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
In total, received %d arp response packets for the requested IP address	Устройство получило указанное совокупное число пакетов ответа ARP для запрашиваемого IP-адреса.
Clear arp cache successfully.	Очистка кэша ARP успешно выполнена.
Client MAC address is not an Ethernet address	MAC-адрес клиента не является адресом Ethernet.
DHCP request received via interface %s (%s:%s), src_mac: %s with requested IP: %s	Устройство получило DHCP-запрос через указанный интерфейс.
IP confliction is detected. Send back DHCP-NAK.	Обнаружен конфликт IP-адресов. Отправлен ответ DHCP-NAK.
Clear ARP cache done	Выполнена очистка кэша ARP.
Set manual time has succeeded. Current time is %s	Дата и время на устройстве были изменены вручную. %s – дата и время.
NTP update successful, current time is %s	Синхронизация устройства с сервером времени NTP успешно выполнена. %s – дата и время.
NTP update failed	Не удалось выполнить синхронизацию с сервером времени NTP.
Device is rebooted by administrator!	Администратор произвел перезагрузку устройства.
Insufficient memory.	Не удалось выделить системную память.
Update the profile %s has failed because of strange server response.	Не удалось обновить профиль из-за непонятного ответа сервера, %s – имя профиля.
Update the profile %s has succeeded because the IP address of FQDN %s was not changed.	Обновление профиля выполнено успешно, поскольку IP-адрес профиля остался неизменным, %s – имя профиля.
Update the profile %s has succeeded.	Обновление профиля выполнено успешно, %s – имя профиля.
Collect Diagnostic Information has failed – Server did not respond.	Не удалось завершить сбор диагностической информации из-за ошибки.
Collect Diagnostic Infomation has succeeded.	Скрипты сбора диагностики выполнены успешно.
Port %d is up!!	Соединение на указанном порту установлено.
Port %d is down!!	Нет соединения на указанном порту.

Таблица 201 Журналы проверки доступности соединений

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Can't open link_up2`	Не удается восстановить состояние маршрутизации link-down (нет соединения).
`Can not open %s.pid`	Не удается открыть файл идентификатора процесса проверки доступности соединений. %s: имя интерфейса
`Can not open %s.arg`	Не удается открыть файл конфигурации процесса проверки доступности соединений. %s: имя интерфейса
`The connectivity-check is activate for %s interface`	Состояние соединения на интерфейсе остается в состоянии activate («активировать») по завершении процесса проверки доступности соединений. %s: имя интерфейса
`The connectivity-check is fail for %s interface`	Состояние соединения на интерфейсе fail («нет соединения») по завершении процесса проверки доступности соединений. %s: имя интерфейса
`Can't get gateway IP of %s interface`	Процесс проверки доступности соединений не может получить IP-адрес шлюза для указанного интерфейса. %s: имя интерфейса
`Can't alloc memory`	Операционная система не может выделить ресурсы оперативной памяти для процесса проверки доступности соединений.
`Can't load %s module`	Процессу проверки доступности соединений не удается загрузить модуль для проверки состояния соединений (link-status). %s: модуль проверки доступности соединений, в настоящее время поддерживается только протокол ICMP.
`Can't handle 'isalive' function of %s module`	Процессу проверки доступности соединений не удается выполнить функцию «isalive» модуля для проверки состояния соединений (link-status). %s: модуль проверки доступности соединений, в настоящее время поддерживается только протокол ICMP.
`Create socket error`	Процессу проверки доступности соединений не удается получить сокет для отправки пакета.
`Can't get IP address of %s interface`	Процессу проверки доступности соединений не удается получить IP-адрес интерфейса. %s: имя интерфейса.
`Can't get flags of %s interface`	Процессу проверки доступности соединений не удается получить сведения о настройках интерфейса. %s: имя интерфейса
`Can't get NETMASK address of %s interface`	Процессу проверки доступности соединений не удается получить маску подсети интерфейса. %s: имя интерфейса
`Can't get BROADCAST address of %s interface`	Процессу проверки доступности соединений не удается получить широковещательный адрес интерфейса %s: имя интерфейса

Таблица 201 Журналы проверки доступности соединений (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Can't use MULTICAST IP for destination	Процессу проверки доступности соединений не удается использовать адрес многоадресной рассылки для проверки состояния соединений (link-status).
The destination is invalid, because destination IP is broadcast IP	Процессу проверки доступности соединений не удается использовать широковещательный адрес для проверки состояния соединений (link-status).
Can't get MAC address of %s interface!	Процессу проверки доступности соединений не удается получить MAC-адрес интерфейса. %s: имя интерфейса
To send ARP REQUEST error!	Процессу проверки доступности соединений не удается отправить пакет с запросом ARP.
The %s routing status seted to DEAD by connectivity-check	Функции маршрутизации на данном интерфейсе не удается переслать пакет. %s: имя интерфейса
The %s routing status seted ACTIVATE by connectivity-check	Функция маршрутизации на данном интерфейсе может переслать пакет. %s: имя интерфейса
The link status of %s interface is inactive	Не удалось выполнить проверку доступности соединений для указанного интерфейса.

Таблица 202 Журналы трансляции сетевых адресов (NAT)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
The NAT range is full	Таблица соответствий NAT переполнена.
%s FTP ALG has succeeded.	Шлюз FTP прикладного уровня (Application Layer Gateway, ALG) был включен или выключен. %s: включен (Enable) или выключен (Disable)
Extra signal port of FTP ALG has been modified.	Был изменен дополнительный порт шлюза ALG для FTP.
Signal port of FTP ALG has been modified.	Был изменен порт по умолчанию шлюза ALG для FTP.
%s H.323 ALG has succeeded.	Шлюз ALG для H.323 ALG был включен или выключен. %s: включен (Enable) или выключен (Disable)
Extra signal port of H.323 ALG has been modified.	Был изменен дополнительный сигнальный порт шлюза ALG для H.323.
Signal port of H.323 ALG has been modified.	Был изменен порт по умолчанию шлюза ALG для H.323.
%s SIP ALG has succeeded.	Шлюз ALG для SIP был включен или выключен. %s: включен (Enable) или выключен (Disable)
Extra signal port of SIP ALG has been modified.	Был изменен дополнительный порт шлюза ALG для SIP.

Таблица 202 Журналы трансляции сетевых адресов (NAT) (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Signal port of SIP ALG has been modified.`	Был изменен порт по умолчанию шлюза ALG для SIP.
`Register SIP ALG extra port=%d failed.`	Не удалось зарегистрировать дополнительный сигнальный порт шлюза ALG для SIP. %d: номер порта
`Register SIP ALG signal port=%d failed.`	Не удалось зарегистрировать сигнальный порт шлюза ALG для SIP. %d: номер порта
`Register H.323 ALG extra port=%d failed.`	Не удалось зарегистрировать дополнительный сигнальный порт шлюза ALG для H.323. %d: номер порта
`Register H.323 ALG signal port=%d failed.`	Не удалось зарегистрировать сигнальный порт шлюза ALG для H.323. %d: номер порта
`Register FTP ALG extra port=%d failed.`	Не удалось зарегистрировать дополнительный сигнальный порт шлюза ALG для FTP. %d: номер порта
`Register FTP ALG signal port=%d failed.`	Не удалось зарегистрировать сигнальный порт шлюза ALG для FTP. %d: номер порта

Таблица 203 Коды причин неудач при проверке пути сертификации

КОД	ОПИСАНИЕ
1	Несовпадение алгоритма между сертификатом и ограничениями поиска.
2	Несовпадение использования ключа между сертификатом и ограничениями поиска.
3	Сертификат был недействительным в данный промежуток времени.
4	(Не используется)
5	Сертификат является недействительным.
6	Не удалось корректно проверить подпись сертификата.
7	Сертификат был отозван и помещен в список CRL.
8	Сертификат не был добавлен в кэш.
9	Не удалось выполнить декодирование сертификата.
10	Не удалось найти сертификат (нигде).
11	Петля в сертификационной цепочке (не удалось найти доверенный корневой сертификат).
12	Сертификат содержит важное расширение, которое не удалось обработать.
13	Издатель сертификата является недействительным (отсутствует информация о центре сертификации).
14	(Не используется)
15	Список CRL устарел.
16	Список CRL является недействительным.
17	Не удалось корректно проверить подпись списка CRL.
18	Не удалось найти список CRL (нигде).
19	Не удалось добавить список CRL в кэш.
20	Не удалось выполнить декодирование списка CRL.

Таблица 203 Коды причин неудач при проверке пути сертификации (продолжение)

КОД	ОПИСАНИЕ
21	Список CRL не является действительным сейчас, но станет действительным в будущем.
22	Список CRL содержит дубли серийных номеров.
23	Нарушена непрерывность временного интервала.
24	Недоступна информация о времени.
25	Не удалось выполнить метод базы данных из-за тайм-аута.
26	Не удалось выполнить метод базы данных.
27	Не удалось выполнить проверку пути.
28	Достигнута предельная длина пути.

Таблица 204 Журналы интерфейсов

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Interface %s has been deleted.	Администратор удалил интерфейс. %s – имя интерфейса.
Interface %s has been changed.	Администратор изменил настройки интерфейса. %s: имя интерфейса.
Interface %s has been added.	Администратор добавил новый интерфейс. %s: имя интерфейса.
Interface %s is enabled.	Администратор включил интерфейс. %s: имя интерфейса.
Interface %s is disabled.	Администратор отключил интерфейс. %s: имя интерфейса.
Interface %s links down. Default route will not apply until interface %s links up.	Администратор указал на интерфейсе статический шлюз, но на этом интерфейсе нет соединения. В данный момент эта настройка будет сохранена, но маршрут не будет использоваться до тех пор, пока на интерфейсе не будет установлено соединение. 1-я перем. %s: имя интерфейса, 2-я перем. %s: имя интерфейса.
name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u,UpTime=%s	Журнал статистики по портам. Этот журнал будет отправлен на сервер VRPT. 1-я перем. %s: имя физического порта, 2-я перем. %s: состояние физического порта, 1-я перем. %u: количество отправленных пакетов для физического порта, 2-я перем. %u: количество принятых пакетов для физического порта, 3-я перем. %u: количество коллизий пакетов для физического порта, 4-я перем. %u: исходящая пропускная способность физического порта, байт/с, 5-я перем. %u: входящая пропускная способность физического порта, байт/с, 3-я перем. %s: время непрерывной работы физического порта.
name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u	Журнал статистики по интерфейсам. Этот журнал будет отправлен на сервер VRPT. 1-я перем. %s: имя интерфейса, 2-я перем. %s: состояние интерфейса, 1-я перем. %u: количество отправленных пакетов для данного интерфейса, 2-я перем. %u: количество принятых пакетов для данного интерфейса, 3-я перем. %u: количество коллизий пакетов для данного интерфейса, 4-я перем. %u: исходящая пропускная способность интерфейса, байт/с, 5-я перем. %u: входящая пропускная способность интерфейса, байт/с.
Interface %s connect failed: MS-CHAPv2 mutual authentication failed.	Не удалось выполнить аутентификацию MS-CHAPv2 (сервер должен поддерживать mS-CHAPv2 и уметь проверять, что аутентификация не прошла; сюда не относятся случаи, когда сервер не поддерживает MS-CHAPv2). %s: имя интерфейса.

Таблица 204 Журналы интерфейсов (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Interface %s connect failed: MS-CHAP authentication failed.	Не удалось выполнить аутентификацию MS-CHAP (сервер должен поддерживать MS-CHAP и уметь проверять, что аутентификация не прошла; сюда не относятся случаи, когда сервер не поддерживает MS-CHAP). %s: имя интерфейса.
Interface %s connect failed: CHAP authentication failed.	Не удалось выполнить аутентификацию CHAP (сервер должен поддерживать CHAP и уметь проверять, что аутентификация не прошла; сюда не относятся случаи, когда сервер не поддерживает CHAP). CHAP: имя интерфейса.
Interface %s connect failed: Peer not responding.	Соединение на данном интерфейсе будет разорвано, поскольку сервер не отправил ни одного пакета LCP. %s: имя интерфейса.
Interface %s connect failed: PAP authentication failed.	Не удалось выполнить аутентификацию PAP (сервер должен поддерживать PAP и уметь проверять, что аутентификация не прошла; сюда не относятся случаи, когда сервер не поддерживает PAP).
Interface %s create failed because has no member.	Интерфейс моста не имеет участников. %s: имя интерфейса моста.

Таблица 205 Журналы беспроводной сети

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Wlan %s is enabled.	Функция WLAN (IEEE 802.11 b и/или g) была включена. %s – номер слота, в который вставлен или может быть вставлен адаптер беспроводной сети.
Wlan %s is disabled.	Функция WLAN (IEEE 802.11 b и/или g) была выключена. %s – номер слота, в который вставлен или может быть вставлен адаптер беспроводной сети.
Wlan %s has been configured.	Настройки функции WLAN (IEEE 802.11 b и/или g) были изменены. %s – номер слота, в который вставлен или может быть вставлен адаптер беспроводной сети.
Interface %s has been configured.	Настройки указанного интерфейса беспроводной сети (%s) были изменены.
Interface %s has been deleted.	Указанный интерфейс беспроводной сети (%s) был удален.
Create interface %s has failed. Wlan device does not exist.	Беспроводному устройству не удалось создать указанный интерфейс беспроводной сети (%s). Удалите беспроводное устройство и установите его заново.
System internal error. No 802.1X or WPA enabled!	Не включена поддержка IEEE 802.1x или WPA.
System internal error. Error configuring WPA state!	Устройству NXC не удалось включить поддержку WPA для беспроводного устройства. Удалите беспроводное устройство и установите его заново.
System internal error. Error enabling WPA/ 802.1X!	Не удалось включить поддержку WPA/IEEE 802.1X на устройстве NXC.
Station has associated. Interface: %s, MAC: %s.	Беспроводной клиент с указанным MAC-адресом (вторая переменная %s) ассоциирован с указанным интерфейсом беспроводной сети (первая переменная %s).

Таблица 205 Журналы беспроводной сети (продолжение)

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
WPA or WPA2 enterprise EAP timeout. Interface: %s, MAC: %s.	Произошел тайм-аут EAP для беспроводного клиента, подключенного к указанному интерфейсу беспроводной сети (первая переменная %s). MAC-адрес беспроводного клиента указан в сообщении (вторая переменная %s).
Station association has failed. Maximum associations have reached the maximum number. Interface: %s, MAC: %s.	Беспроводному клиенту с указанным MAC-адресом (вторая переменная %s) не удалось подключиться к указанному интерфейсу беспроводной сети (первая переменная %s), поскольку на данном интерфейсе достигнуто предельное значение подключенных беспроводных клиентов.
WPA authentication has failed. Interface: %s, MAC: %s.	Беспроводному клиенту не удалось подключиться к указанному интерфейсу WLAN (первая переменная %s) из-за неверного ключа WPA. MAC-адрес беспроводного клиента указан в сообщении (вторая переменная %s).
Incorrect password for WPA or WPA2 enterprise internal authentication. Interface: %s, MAC: %s.	Беспроводной клиент указал неправильный пароль WPA или WPA2, поэтому ему не удалось пройти аутентификацию в локальной базе данных пользователей устройства NXC при попытке подключиться к указанному интерфейсу беспроводной сети (первая переменная %s). MAC-адрес беспроводного клиента указан в сообщении (вторая переменная %s).
Incorrect username or password for WPA or WPA2 enterprise internal authentication. Interface: %s, MAC: %s.	Беспроводной клиент указал неправильное имя пользователя или неправильный пароль WPA или WPA2, поэтому ему не удалось пройти аутентификацию в локальной базе данных пользователей устройства NXC при попытке подключиться к указанному интерфейсу беспроводной сети (первая переменная %s). MAC-адрес беспроводного клиента указан в сообщении (вторая переменная %s).
System internal error. %s: STA %s could not extract EAP-Message from RADIUS message	Произошла ошибка при попытке извлечь сообщение EAP из сообщения RADIUS. Первая переменная %s – интерфейс беспроводной сети. Вторая переменная %s – MAC-адрес беспроводного клиента.

Таблица 206 Журналы учетных записей

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Account %s %s has been deleted.	Пользователь удалил профиль учетной записи провайдера услуг Интернет. 1-я перем. %s: тип профиля, 2-я перем. %s: имя профиля.
Account %s %s has been changed.	Пользователь изменил настройки профиля учетной записи провайдера услуг Интернет. 1-я перем. %s: тип профиля, 2-я перем. %s: имя профиля.
Account %s %s has been added.	Пользователь добавил новый профиль учетной записи провайдера услуг Интернет. 1-я перем. %s: тип профиля, 2-я перем. %s: имя профиля.

Таблица 207 Журналы вынужденной аутентификации

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
Force User Authentication will be enabled due to http server is enabled.	Функция вынужденной аутентификации пользователей (Force User Authentication) будет включена, поскольку был включен HTTP-сервер.
Force User Authentication will be disabled due to http server is disabled.	Функция вынужденной аутентификации пользователей (Force User Authentication) будет выключена, поскольку был выключен HTTP-сервер.
Force User Authentication may not work properly!	

Таблица 208 Журналы менеджера файлов

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
ERROR:#%s, %s	Не удалось применить настройки, сообщение в журнале будет содержать команду интерфейса командной строки и сообщение об ошибке. 1-я перем. %s – командная строка интерфейса командной строки. 2-я перем. %s – сообщение об ошибке, явившееся результатом выполнения этой команды.
WARNING:#%s, %s	Не удалось применить настройки, сообщение в журнале будет содержать команду интерфейса командной строки и предупредительное сообщение. 1-я перем. %s – командная строка интерфейса командной строки. 2-я перем. %s – предупредительное сообщение, явившееся результатом выполнения этой команды.
ERROR:#%s, %s	Не удалось выполнить сценарий, сообщение в журнале будет содержать команду интерфейса командной строки, при выполнении которой произошла ошибка, и сообщение об ошибке. 1-я перем. %s – командная строка интерфейса командной строки. 2-я перем. %s – сообщение об ошибке, явившееся результатом выполнения этой команды.
WARNING:#%s, %s	Не удалось выполнить сценарий, сообщение в журнале будет содержать команду интерфейса командной строки, ставшую причиной предупреждения, и предупредительное сообщение. 1-я перем. %s – командная строка интерфейса командной строки. 2-я перем. %s – предупредительное сообщение, явившееся результатом выполнения этой команды.
Resetting system...	Выполняется сброс настроек перед применением файла конфигурации.
System resetted. Now apply %s..	После сброса настроек система начала применение файла конфигурации. %s – имя файла конфигурации.
Running %s...	Администратор запустил указанный сценарий командной строки. %s – имя файла сценария.

Таблица 209 Логи DHCP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Can't find any lease for this client - %s, DHCP pool full!`	Все IP-адреса из пула DHCP уже назначены DHCP-клиентам, поэтому найти IP-адрес для указанного DHCP-клиента не получается.
`DHCP server offered %s to %s(%s)`	DHCP-сервер выделил указанный IP-адрес компьютеру с указанными именем хоста и MAC-адресом.
`Requested %s from %s(%s)`	Устройство NXC получило DHCP-запрос на указанный IP-адрес от компьютера с указанными именем хоста и MAC-адресом.
`No applicable lease found for DHCP request - %s !`	DHCP-серверу не удалось найти указанный IP-адрес, который можно было бы отдать в аренду в ответ на запрос со стороны DHCP-клиента.
`DHCP released %s with %s(%s)`	DHCP-клиент освободил указанный IP-адрес. Имя хоста и адрес DHCP-клиента указаны в сообщении.
`Sending ACK to %s`	DHCP-сервер получил от DHCP-клиента информационный пакет и отправляет подтверждение ACK клиенту.
`DHCP server assigned %s to %s(%s)`	DHCP-сервер назначил клиенту запрашиваемый IP-адрес. Имя хоста и адрес DHCP-клиента указаны в сообщении.

Таблица 210 Журналы ежедневных отчетов для почтовой рассылки

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Email Daily Report has been activated.`	Функция ежедневной рассылки отчетов была включена. Устройство NXC будет ежедневно, в соответствии с расписанием, отправлять по электронной почте отчет по выбранным позициям, если соответствующие параметры настроены корректно.
`Email Daily Report has been deactivated.`	Функция ежедневной рассылки отчетов была отключена. Устройство NXC не будет ежедневно выполнять рассылку отчетов по электронной почте.
`Email daily report has been sent successfully.`	Устройство NXC успешно выполнило отправку ежедневного отчета по электронной почте.
`Cannot resolve mail server address %s.`	Неверно указан SMTP-адрес для ежедневной рассылки отчетов.
`Mail server authentication failed.`	Неверно указаны имя пользователя или пароль для подключения к почтовому серверу, указанному в настройках для ежедневной рассылки отчетов.
`Failed to send report. Mail From address %s1 is inconsistent with SMTP account %s2.`	Имя пользователя и пароль для аутентификации на почтовом сервере указаны верно, но почтовый адрес отправителя не соответствует адресу, указанному в учетной записи SMTP.
`Failed to connect to mail server %s.`	Устройству NXC не удалось подключиться к почтовому серверу по протоколу SMTP (%s). Возможно, неверно указан адрес сервера, или существует проблема с подключением к сети устройства NXC или почтового сервера.

Таблица 211 Журналы привязки IP-MAC

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Drop packet %s-%u.%u.%u.%u-%02X:%02X:%02X:%02X:%02X:%02X`	Функция привязки IP-MAC отбросила пакет Ethernet. Сообщение содержит название интерфейса, через который пришел пакет, IP-адрес и MAC-адрес отправителя.
`Cannot bind ip-mac from dhcpd: %s#%u.%u.%u.%u#%02X:%02X:%02X:%02X:%02X:%02X.`	Функция привязки IP-MAC не может создать запись привязки IP-MAC в хэш-таблице. Сообщение содержит название интерфейса, через который пришел пакет, IP-адрес и MAC-адрес отправителя, а также тип привязки («s» – значит, статический, «d» – динамический).
`Cannot remove ip-mac binding from dhcpd: %s#%u.%u.%u.%u#%02X:%02X:%02X:%02X:%02X:%02X.`	Функция привязки IP-MAC не может удалить запись привязки IP-MAC из хэш-таблицы. Сообщение содержит название интерфейса, через который пришел пакет, IP-адрес и MAC-адрес отправителя, а также тип привязки («s» – значит, статический, «d» – динамический).

Таблица 212 Журналы сервера CAPWAP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`WLAN Controller Start. Registration Type:%s`	Запуск службы управления точками доступа. 1-я перем. %s: тип регистрации. {Always Accept – всегда принимать | Manual – Вручную}
`WLAN Controller Reset. Registration Type:%s`	Сброс службы управления точками доступа. 1-я перем. %s: тип регистрации. {Always Accept – всегда принимать | Manual – Вручную}
`WLAN Controller End.`	Остановка/завершение работы службы управления точками доступа.
`AP Connect. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Управляемая точка доступа подключена к серверу CAPWAP. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа.
`Указываемая модель точки доступа не совпадает с настоящей. MAC:%02x%02x%02x%02x%02x%02x, Model ID:%x`	CAPWAP сервер не поддерживает модель управляемой точки доступа. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %x: Идентификатор модели управляемой точки доступа.

Таблица 212 Журналы сервера CAPWAP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`AP Disconnect. MAC:%02x%02x%02x%02x%02x%02x, Name:%s, Reason:%s in %s State,Model:%s`	Произошло отключение управляемой точки доступа от сервера CAPWAP. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Причина отключения управляемой точки доступа. 9-я перем. %s: Наименование модели управляемой точки доступа.
`AP Add. MAC:%02x%02x%02x%02x%02x%02x, Model:%s`	Добавление точки доступа из списка неуправляемых в список управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Наименование модели управляемой точки доступа.
`AP Delete. MAC:%02x%02x%02x%02x%02x%02x, Model:%s`	Удаление точки доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Наименование модели управляемой точки доступа.
`Update AP Configure. MAC:%02x%02x%02x%02x%02x%02x, Model:%s`	Отправка настроек точке доступа, находящейся в списке управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Наименование модели управляемой точки доступа.
`Update AP Configure Fail. Wrong Configure Apply,MAC:%02x%02x%02x%02x%02x%02x, Model:%s`	Настройки отправлены точке доступа, находящейся в списке управляемых, однако от нее пришел ответ, сигнализирующий о том, что не удалось применить эти настройки. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Наименование модели управляемой точки доступа.
`AP Reboot. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Перезагрузка указанной точки доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа.

Таблица 212 Журналы сервера CAPWAP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Upgrade AP Firmware. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Обновление встроенного программного обеспечения точки доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа.
`Start Send Configuration to AP. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Начало отправки настроек на точку доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа.
`Sucess Send Configuration to AP. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Получение ответа на отправку настроек от точки доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа.
`Start Send Updating Configuration to AP. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Начало отправки запроса на обновление настроек на точке доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа.
`Sucess Send Updating Configuration to AP. MAC:%02x%02x%02x%02x%02x%02x, Name:%s,Model:%s`	Получение ответа на запрос обновления настроек от точки доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Наименование модели управляемой точки доступа. 8-я перем. %s: Описание управляемой точки доступа.
`Send Retransmit Configuration to AP. MAC:%02x%02x%02x%02x%02x%02x, Name:%s, Retry Count=%d,Model:%s,`	Повторная отправка настроек точке доступа из списка управляемых. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %s: Наименование модели управляемой точки доступа. 9-я перем. %d: Счетчик попыток.

Таблица 212 Журналы сервера CAPWAP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`AP SSID Stop. MAC:%02x%02x%02x%02x%02x%02x, Radio:%d, SSID:%s Stop.`	Управляемая точка доступа перестает выполнять широковещательную передачу сети SSID из-за отключения DTLS (Datagram Transport Layer Security, безопасность транспортного уровня датаграмм). 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем.: %d: Число радиомодулей управляемой точки доступа. 8-я перем.: %s: Имя сети SSID, широковещательную передачу которой прекратила точка доступа.
`VLAN setting is conflict.MAC:%02x:%02x:%02x:%02x:%02x:%02x,Model:%s, Mgnt. VID(AC):%d, %s, Mgnt. VID(AP):%d,%s`	Идентификатор VLAN ID на контроллере доступа не совпадает с идентификатором VLAN ID точки доступа. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа. 8-я перем. %d: VID , 9-я перем. %s: с тегами или без тегов 10-я перем. %d: VID , 11-я перем. %s: с тегами или без тегов
`AP doesn't support %s feature. MAC:%02x:%02x:%02x:%02x:%02x:%02x,AP:%s`	Точка доступа не поддерживает данную функцию. 1-я перем. %s: название функции 2-я перем. %02x~7-я перем. %02x: MAC-адрес управляемой точки доступа. 8-я перем. %s: Описание управляемой точки доступа.

Таблица 213 Журналы клиентов CAPWAP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`AP Start. Discovery Type:%s`	Запуск службы клиента CAPWAP. 1-я перем. %s: Тип обнаружения type {Static (Статический) | DHCP | DNS | Broadcast (Широковещательный)}
`AP Reset. Discovery Type:%s`	Сброс службы клиента CAPWAP. 1-я перем. %s: Тип обнаружения type {Static (Статический) | DHCP | DNS | Broadcast (Широковещательный)}
`Connect to WLAN Controller. IP:%s`	Клиент CAPWAP подключен к контроллеру беспроводной сети. 1-я перем. %s: IP-адрес контроллера беспроводной сети.
`Disconnect from WLAN Controller. IP:%s`	Клиент CAPWAP отключен от контроллера беспроводной сети. 1-я перем. %s: IP-адрес контроллера беспроводной сети.
`Updated Configuration by a WLAN Controller Success. Partial Update`	Контроллер беспроводной сети успешно выполнил обновление настроек.
`Updated Configuration by a WLAN Controller Fail.`	Контроллеру беспроводной сети не удалось произвести обновление настроек.

Таблица 213 Журналы клиентов CAPWAP

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`ReBoot by a WLAN Controller. IP:%s`	Перезагрузка точки доступа (WTP) контроллером беспроводной сети. 1-я перем. %s: IP-адрес контроллера беспроводной сети.
`Firmware Upgraded by WLAN Controller. IP:%s`	Контроллер беспроводной сети выполнил обновление встроенного программного обеспечения. 1-я перем. %s: IP-адрес контроллера беспроводной сети.
`Apply Configuration by a WLAN Controller Success.%s`	Контроллер беспроводной сети успешно применил настройки. 1-я перем. %s: Complete Update (Обновление завершено)
`WLAN Controller IP Changed. New Discovery Type:%s, WLAN Controller IP: %s`	Изменен IP-адрес контроллера доступа для точки доступа (WTP). 1-я перем. %s: Тип обнаружения type {Static (Статический) | DHCP | DNS | Broadcast (Широковещательный)} 2-я перем. %s: IP-адрес контроллера беспроводной сети
`AP Receiving Complete ZySH Configuration from WLAN Controller.`	Точка доступа WTP получает полную конфигурацию от контроллера беспроводной сети во время согласования протоколов CAPWAP. (состояние изменения конфигурации)
`AP Receiving Updating ZySH Configuration from WLAN Controller.`	Точка доступа WTP получает полную конфигурацию от контроллера беспроводной сети, когда точка доступа меняет конфигурацию. (состояние запуска)
`STA List Full. STA List of AP [%s] is Full`	Количество станций, подключенных к указанной точке доступа, достигло предельного значения. 1-я перем. %s: Описание точки доступа (WTP).
`DNS Query result is NULL.`	Не удалось выполнить DNS-запрос.

Таблица 214 Журналы балансировки нагрузки между точками доступа

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`kick station %02x:%02x:%02x:%02x:%02x:%02x`	Свидетельствует о том, что указанная станция была удалена из беспроводной сети точки доступа из-за перегрузки последней.

Таблица 215 Журналы мошеннических точек доступа

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`rogue ap detection is enabled.`	Указывает на обнаружение мошеннической точки доступа.

Таблица 216 Журналы записи беспроводных кадров

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`Capture done! check_size:%d, max_file_size:%d\n`	По завершении записи беспроводных кадров это сообщение показывает значения переменных check_size %d и max_file_size %d. 1-я перем. %d: совокупный размер файлов в каталоге. 2-я перем. %d: максимальный размер файлов.
`Can not initial monitor mode signal handler.\n`	Если точка доступа находится в режиме мониторинга, обработчик функционирует как процесс (daemon); это сообщение возвращается в том случае, если не удается инициализировать обработчик.

Таблица 217 Журналы функции DCS

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`dcs init failed!\n`	Указывает на то, что устройству NXC не удалось инициализировать процесс (daemon) dcs.
`init zylog fail\n`	Указывает на то, что устройству NXC не удалось инициализировать zylog.
`channel changed: %s %d -> %d\n`	Функция DCS перевела беспроводной интерфейс %s с канала %d на канал %d. 1-я перем. %s: имя интерфейса 1-я перем. %d: текущий канал 2-я перем. %d: новый канал
`dcs is terminated!`	Работа функции DCS была прервана по неизвестным причинам.

Таблица 218 Информация о станциях беспроводной сети

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`STA Association. Addr:%02x%02x%02x%02x%02x%02x, AP:%s`	К данной точке доступа подключен беспроводной клиент. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа.
`STA Disassociation. Addr:%02x%02x%02x%02x%02x%02x, AP:%s`	Беспроводной клиент отключен от данной точки доступа. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес управляемой точки доступа. 7-я перем. %s: Описание управляемой точки доступа.
`STA Roaming. MAC:%02x:%02x:%02x:%02x:%02x:%02x, From:%s, To:%s`	Беспроводной клиент переходит от одной точки доступа к другой. 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес станции. 7-я перем. %s: Описание исходной точки доступа (WTP). 8-я перем. %s: Описание целевой точки доступа (WTP).
`STA List Full. STA List of AP [%s] is Full`	Количество беспроводных клиентов, подключенных к данной точке доступа, достигло предельного значения. 1-я перем. %s: Описание управляемой точки доступа.

Таблица 218 Информация о станциях беспроводной сети

СООБЩЕНИЕ В ЖУРНАЛЕ	ОПИСАНИЕ
`STA Disassociation(%s).MAC:%02x:%02x:%02x:%02x:%02x:%02x,AP:%s`	Указывает на причину отключения беспроводного клиента от точки доступа. 1-я перем. %s: Причина отключения. 2-я перем. %02x~7-я перем. %02x: MAC-адрес беспроводного клиента. 8-я перем. %s: Описание управляемой точки доступа.
`AP Radio MAC=%02x:%02x:%02x:%02x:%02x:%02x, Reject Station MAC%02x:%02x:%02x:%02x:%02x:%02x, RSSI=%d dBm`	Точка доступа отклонила запрос беспроводного клиента на ассоциацию (подключение). 1-я перем. %02x ~ 6-я перем. %02x: MAC-адрес точки доступа. 7-я перем. %02x~12-я перем. %02x: MAC-адрес беспроводного клиента. 13-я перем. %d: значение RSSI

B

Часто используемые службы

В приведенной ниже таблице перечислен ряд наиболее часто используемых служб, с указанием соответствующих протоколов и номеров портов. Полный перечень номеров портов, кодов/типов ICMP и служб можно найти на сайте IANA (уполномоченной организации по распределению нумерации в сети Интернет).

- **Наименование**: Краткое описательное имя службы. Можно использовать это имя или создать другое, при желании.
- **Протокол**: Тип IP-протокола, используемого службой. Если в этом столбце указано **TCP/UDP**, данной службой используются одинаковые номера портов как для TCP, так и для UDP. Если в этом столбце указано **ОПРЕДЕЛЯЕТСЯ ПОЛЬЗОВАТЕЛЕМ**, в столбце **Порт(ы)** указывается номер протокола IP, а не номер порта.
- **Порты(ы)**: Значение в данном столбце зависит от значения в столбце **Протокол**. Более подробную информацию о номерах портов можно найти в RFC 1700.
  - Если в столбце **Протокол** указано **TCP**, **UDP** или **TCP/UDP**, в данном столбце указывается номер порта IP.
  - Если в столбце **Протокол** стоит **ОПРЕДЕЛЯЕТСЯ ПОЛЬЗОВАТЕЛЕМ**, в данном столбце указывается номер протокола IP.
- **Описание**: Краткое описание приложений, которые используют службу, или ситуаций, в которых используется служба.

Таблица 219 Часто используемые службы

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Определяется пользователем	51	Данная служба используется протоколом туннелирования IPSEC AH (заголовок аутентификации).
AIM/New-ICQ	TCP	5190	Служба Интернет-сообщений AOL. Также используется как порт прослушивания ICQ.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Протокол пограничной маршрутизации.
BOOTP_CLIENT	UDP	68	Клиент DHCP.
BOOTP_SERVER	UDP	67	Сервер DHCP.
CU-SEEME	TCP UDP	7648 24032	Популярное решение для видеоконференций от White Pines Software.
DNS	TCP/UDP	53	Сервер доменных имен, служба, определяющая соответствие между именами в Интернете (такими как www.zyxel.com) и IP-адресами.
ESP (IPSEC_TUNNEL)	Определяется пользователем	50	Данная служба используется протоколом туннелирования IPSEC ESP (Encapsulation Security Protocol).
FINGER	TCP	79	Finger – команда в UNIX или в Интернете, используемая для поиска зарегистрированных в системе пользователей.

Таблица 219 Часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
FTP	TCP TCP	20 21	Программа передачи файлов, программа, обеспечивающая быструю передачу файлов, в том числе файлов большого размера, которые не всегда возможно передать по электронной почте.
H.323	TCP	1720	Данный протокол используется программой NetMeeting.
HTTP	TCP	80	Протокол передачи гипертекста – протокол клиент/сервер для сети World Wide Web.
HTTPS	TCP	443	HTTPS – защищенные сессии http, часто используемые в электронной коммерции.
ICMP	Определяется пользователем	1	Межсетевой протокол контрольных сообщений часто используется для диагностики или маршрутизации.
ICQ	UDP	4000	Популярная программа для Интернет-чата.
IGMP (MULTICAST)	Определяется пользователем	2	Межсетевой протокол управления группами используется при отправке пакетов определенной группе хостов.
IKE	UDP	500	Алгоритм обмена ключами в Интернете используется для распространения ключей и управления ключами.
IRC	TCP/UDP	6667	Еще одна популярная программа Интернет-чата.
MSN Messenger	TCP	1863	Данный протокол используется службой сообщений Microsoft Networks.
NEW-ICQ	TCP	5190	Программа Интернет-чата.
NEWS	TCP	144	Протокол новостных групп.
NFS	UDP	2049	Сетевая файловая система NFS – распределенная файловая служба клиент/сервер, обеспечивающая прозрачный доступ к совместному использованию файлов в сети.
NNTP	TCP	119	Сетевой протокол передачи новостей представляет собой механизм доставки для службы новостей USENET.
PING	Определяется пользователем	1	Packet INternet Groper – протокол, рассылающий эхо-запросы ICMP для проверки доступности удаленного хоста.
POP3	TCP	110	Почтовый протокол Post Office Protocol версии 3 позволяет клиентским компьютерам получать электронную почту с сервера POP3 с использованием временного подключения (TCP/IP или другого).
PPTP	TCP	1723	Протокол туннелирования «точка-точка» обеспечивает защищенную передачу данных через общедоступные сети. Этот порт используется для управляющего канал.
PPTP_TUNNEL (GRE)	Определяется пользователем	47	Протокол туннелирования «точка-точка» PPTP обеспечивает защищенную передачу данных через общедоступные сети. Этот порт используется для канала передачи данных.
RCMD	TCP	512	Служба удаленных команд.
REAL_AUDIO	TCP	7070	Служба потоковой передачи аудио обеспечивает трансляцию звука через Интернет в реальном времени.

Таблица 219 Часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
REXEC	TCP	514	Процесс (daemon) удаленного исполнения.
RLOGIN	TCP	513	Удаленный вход в систему.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Протокол потоковой передачи реального времени (управления средой передачи) RTSP обеспечивает удаленное управление потоками мультимедиа в Интернете.
SFTP	TCP	115	Простой протокол передачи файлов.
SMTP	TCP	25	Простой протокол пересылки почты представляет собой стандарт обмена сообщениями через Интернет. SMTP позволяет передавать сообщения с одного сервера электронной почты на другой.
SNMP	TCP/UDP	161	Простой протокол сетевого управления.
SNMP-TRAPS	TCP/UDP	162	«Ловушки», используемые в протоколе SNMP (RFC:1215).
SQL-NET	TCP	1521	Язык структурированных запросов SQL – интерфейс доступа к данным в различных системах баз данных, в том числе на мейнфреймах, системах среднего уровня, UNIX-системах и сетевых серверах.
SSH	TCP/UDP	22	Программа удаленного входа в систему через защищенную оболочку.
STRM WORKS	UDP	1558	Протокол Stream Works.
SYSLOG	UDP	514	Syslog обеспечивает передачу системных контрольных журналов на сервер UNIX.
TACACS	UDP	49	Протокол входа в систему, используемый для систем TACACS (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet – протокол входа в систему и эмуляции терминала, часто используемый в Интернете и UNIX-системах. Работает в сетях TCP/IP. Основное назначение данного протокола – удаленный вход пользователей на хост-системы.
TFTP	UDP	69	Тривиальный протокол передачи файлов – сходный с FTP протокол передачи файлов в Интернете, отличается от FTP использованием протокола UDP (User Datagram Protocol) вместо TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Еще одно решение для видеоконференций.

C

Импорт сертификатов

В этом приложении описывается процедура импорта сертификатов с открытым ключом в веб-браузер.

Веб-браузеры используют сертификаты с открытым ключом для проверки легитимности защищенных веб-сайтов. Когда центр сертификации, например, VeriSign, Comodo или Network Solutions, получает запрос на сертификат от оператора веб-сайта, он подтверждает, что веб-домен и контактная информация в запросе соответствуют аналогичным данным, содержащимся в публичной записи регистратора доменного имени. Если они совпадают, то центр сертификации выпускает сертификат для оператора веб-сайта, который затем размещает его у себя на сайте и предлагает его браузерам всех посетителей сайта, информируя их о том, что их сайт является легитимным.

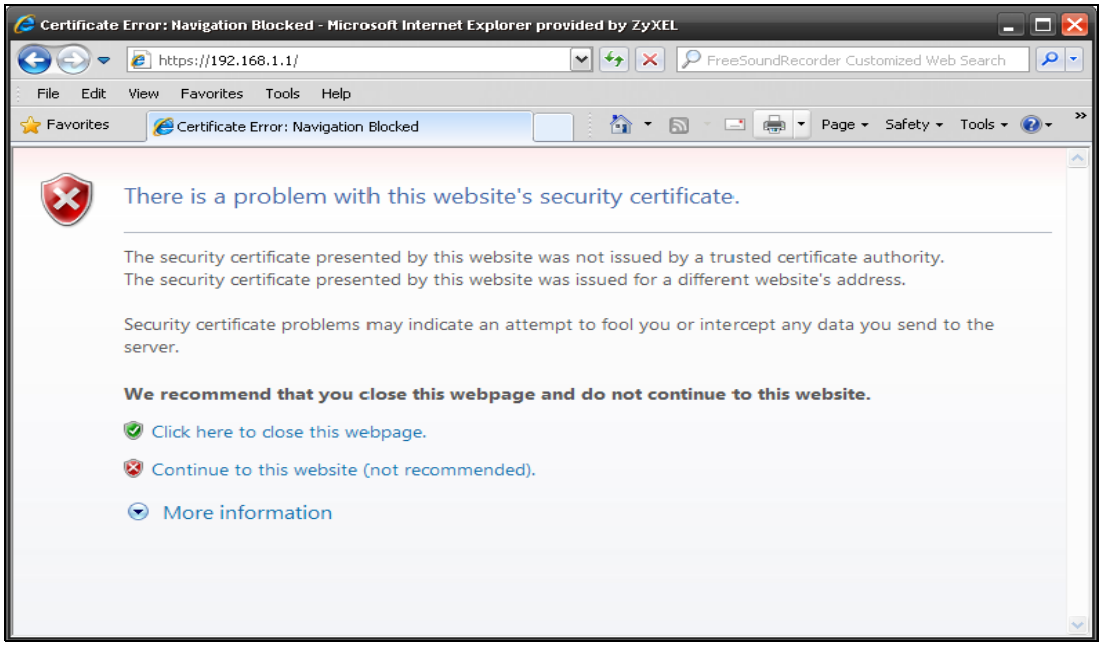
Многие изделия ZyXEL, такие, как устройство NXC, выпускают собственные сертификаты с открытым ключом. Веб-браузеры, работающие в локальной сети или сети WAN, могут использовать эти сертификаты для проверки того факта, что они подключаются к легитимному устройству, а не к устройству, выдающему себя за таковое. Следует учесть, однако, что эти сертификаты выпущены оборудованием ZyXEL, а не одним из центров сертификации, официально признанных большинством наиболее распространенных веб-браузеров, поэтому необходимо импортировать такой сертификат в веб-браузер и пометить его как сертификат доверенного центра сертификации.

Примечание: Если просматривается защищенный веб-сайт, то ссылка в строке адреса веб-браузера начинается с `https://`, еще один признак – пиктограмма запертого замка где-нибудь в основном окне браузера  (расположение отличается в зависимости от браузера).

Internet Explorer

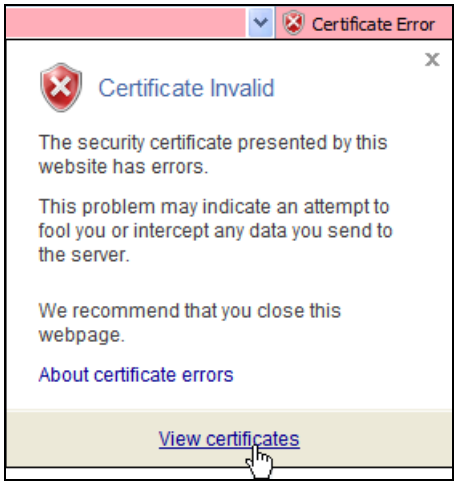
В примере ниже рассматривается процедура импорта сертификата для браузера Microsoft Internet Explorer 7 в операционной системе Windows XP Professional; тем не менее, этот пример пригоден и для работы с браузером Internet Explorer в операционной системе Windows Vista.

1 Если на Web-конфигураторе устройства включена проверка сертификатов SSL, то при первом заходе на страницу устройства появится сообщение об ошибке проверки сертификата.

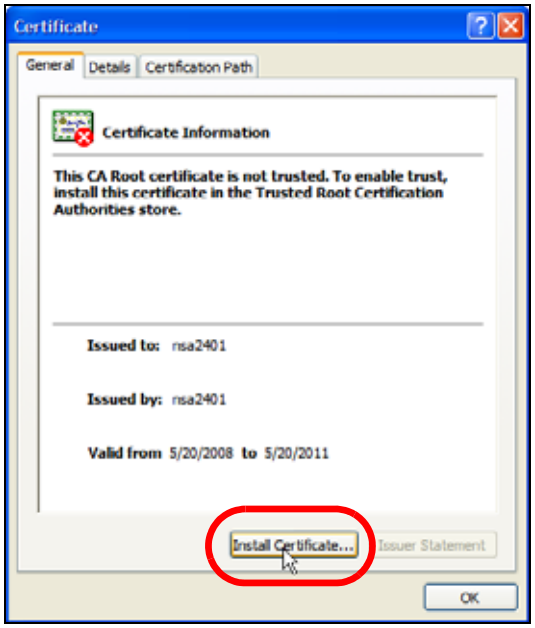


2 Выберите **Continue to this website (not recommended)**.

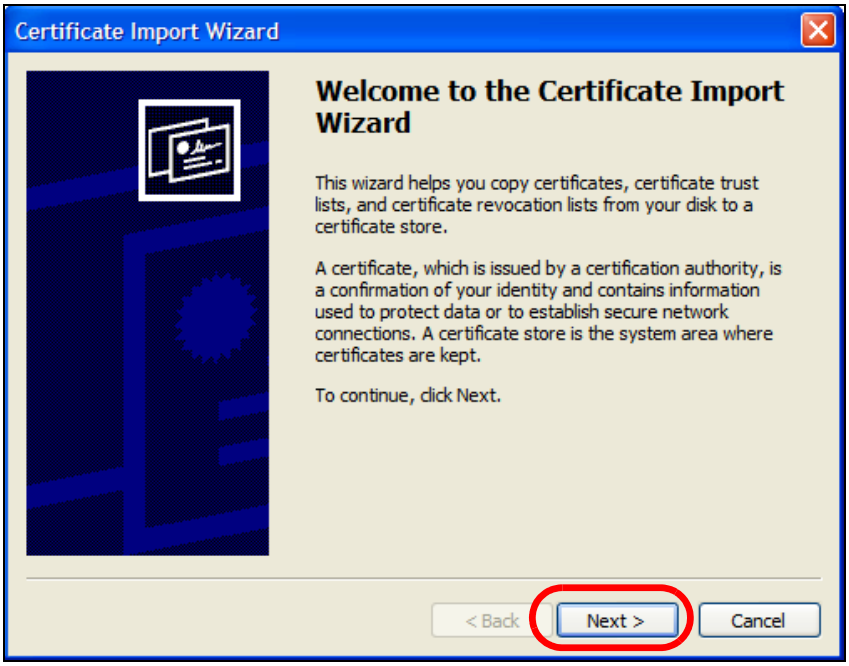
3 В адресной строке выберите **Certificate Error** > **View certificates**.



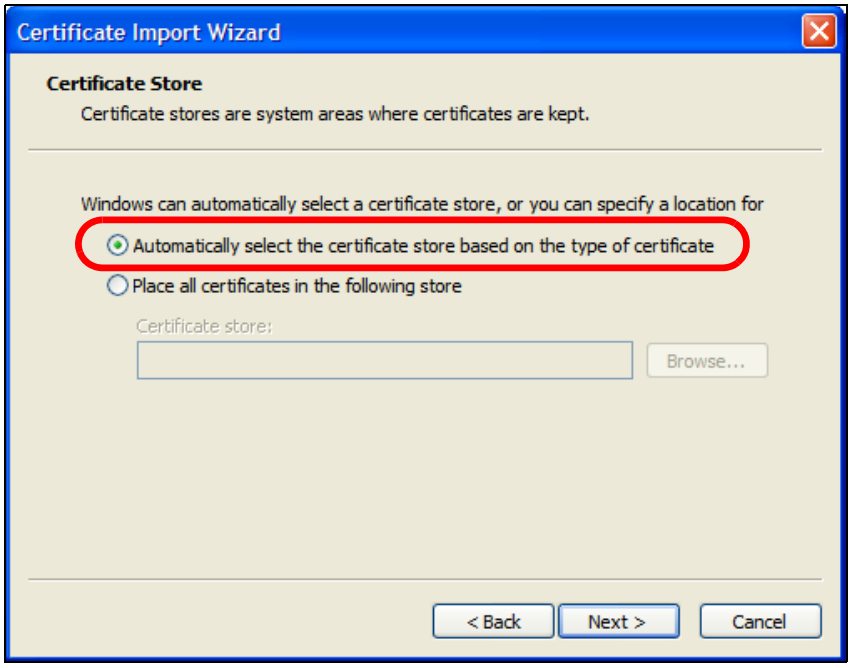
4 В диалоговом окне **Certificate** нажмите кнопку **Install Certificate**.



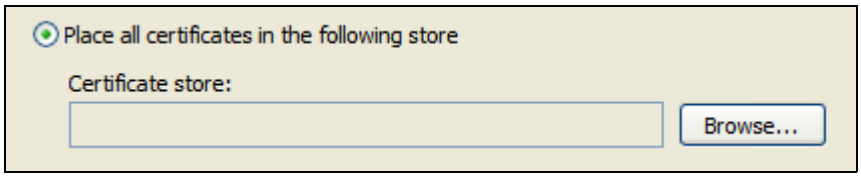
5 В окне **Certificate Import Wizard** нажмите кнопку **Next**.



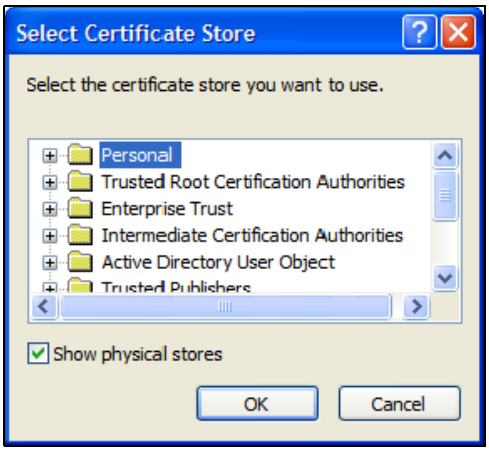
6 Чтобы браузер самостоятельно выбрал хранилище для сертификата исходя из его типа, выберите опцию **Automatically select certificate store based on the type of certificate**, еще раз нажмите кнопку **Next** и перейдите к шагу 9.



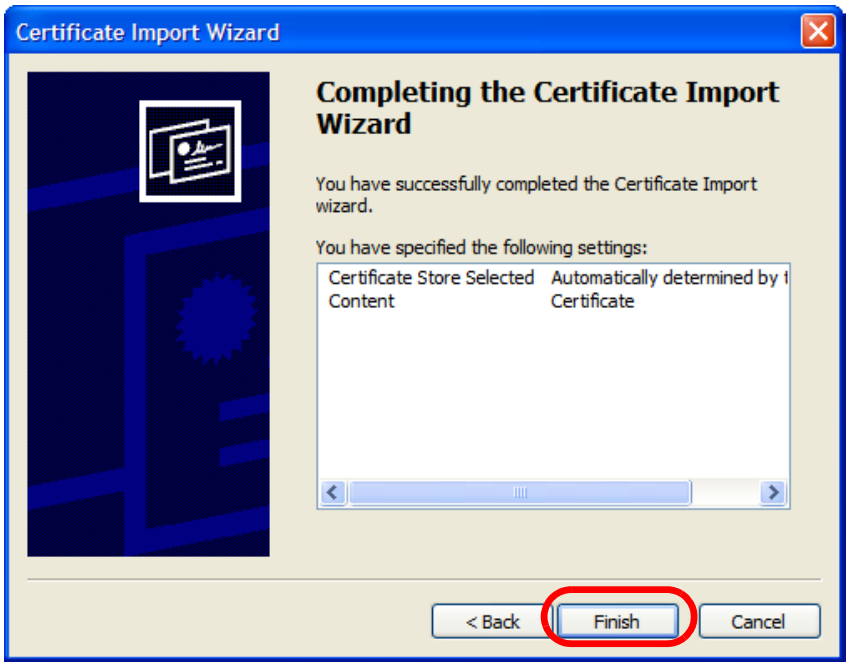
7 В противном случае выберите опцию **Place all certificates in the following store** и нажмите кнопку **Browse**.



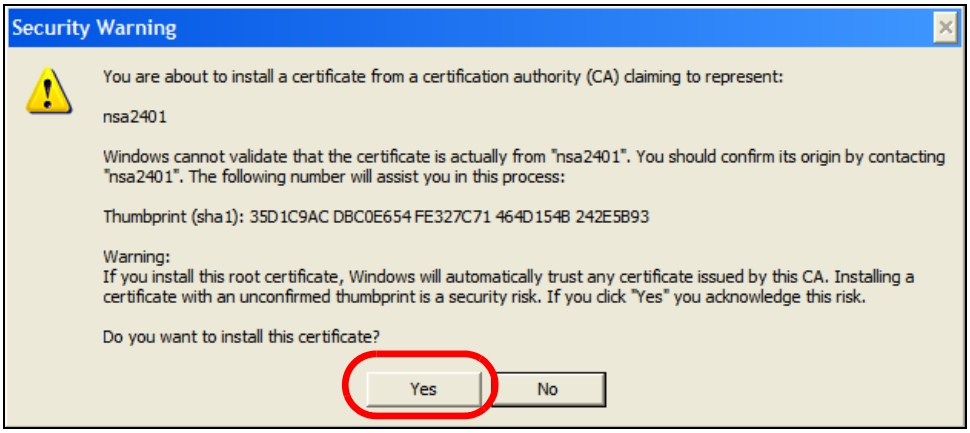
8 В диалоговом окне **Select Certificate Store** выберите папку, в которой необходимо сохранить сертификат, и нажмите кнопку **OK**.



9 На экране **Completing the Certificate Import Wizard** нажмите кнопку **Finish**.

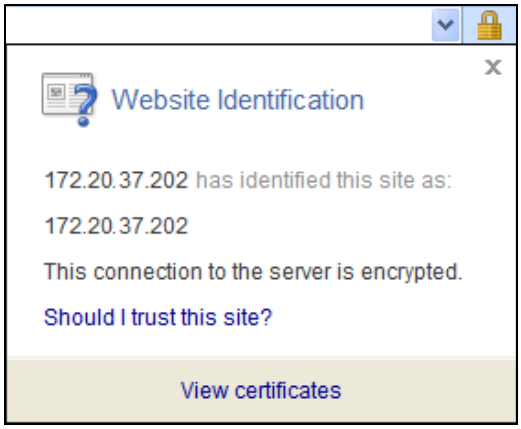


10 Если на экране появится еще одно предупреждение системы безопасности (**Security Warning**), нажмите кнопку **Yes**.



11 Появится сообщение об успешной установке сертификата. Нажмите кнопку **OK**.

12 Теперь при следующем запуске Internet Explorer и переходе на страницу Web-конфигуратора ZyXEL в адресной строке появится пиктограмма запертого замка. Щелкните по ней, чтобы ознакомиться с идентификационной информацией об этой странице веб-сайта.

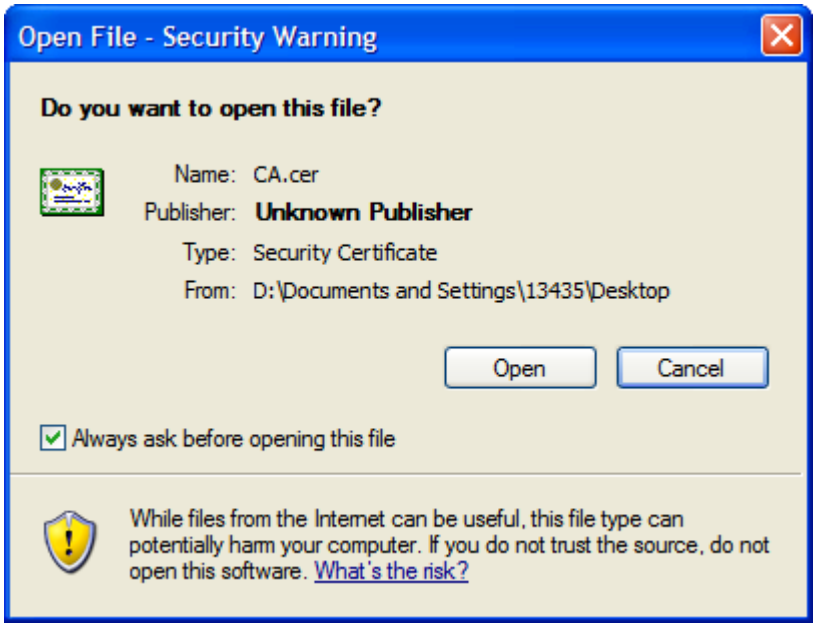


Установка автономного файла сертификата в Internet Explorer

Вместо того, чтобы заходить на страницу ZyXEL Web-конфигуратора и устанавливать открытый ключ, воспользовавшись соответствующим предложением, можно установить автономный файл сертификата, если он был выпущен.

1 Дважды щелкните по файлу сертификата с открытым ключом.

2 В диалоговом окне с предупреждением системы безопасности нажмите кнопку **Open**.

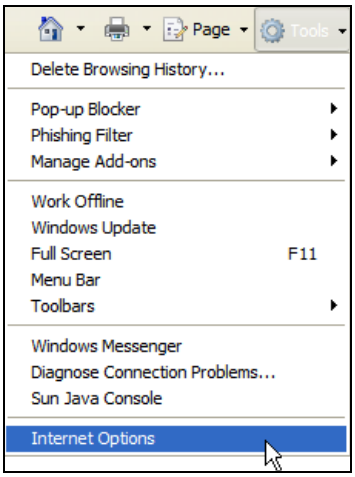


3 Повторите шаги с 4 по 12 процедуры для Internet Explorer, описание которой начинается на стр. 451, чтобы завершить процесс установки.

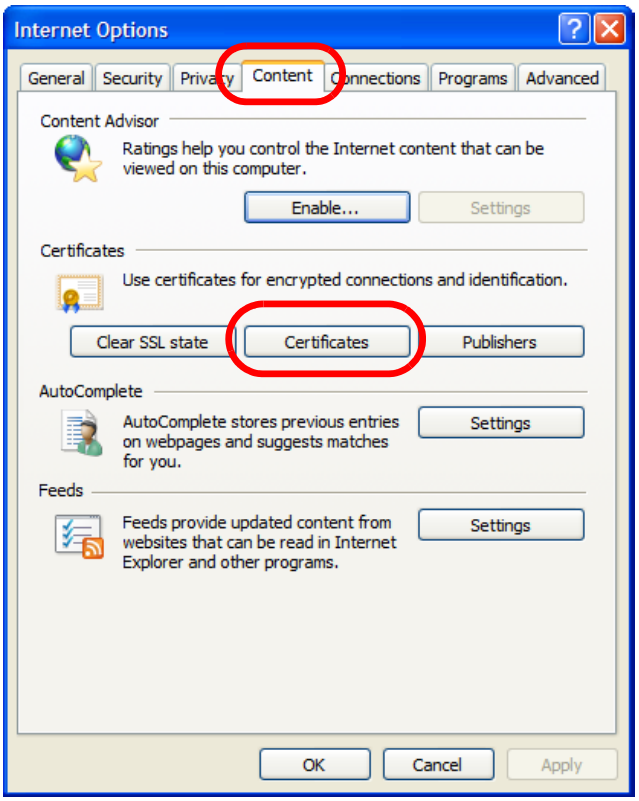
Удаление сертификата в Internet Explorer

В этом разделе описана процедура удаления сертификата с открытым ключом в браузере Internet Explorer 7 в операционной системе Windows XP.

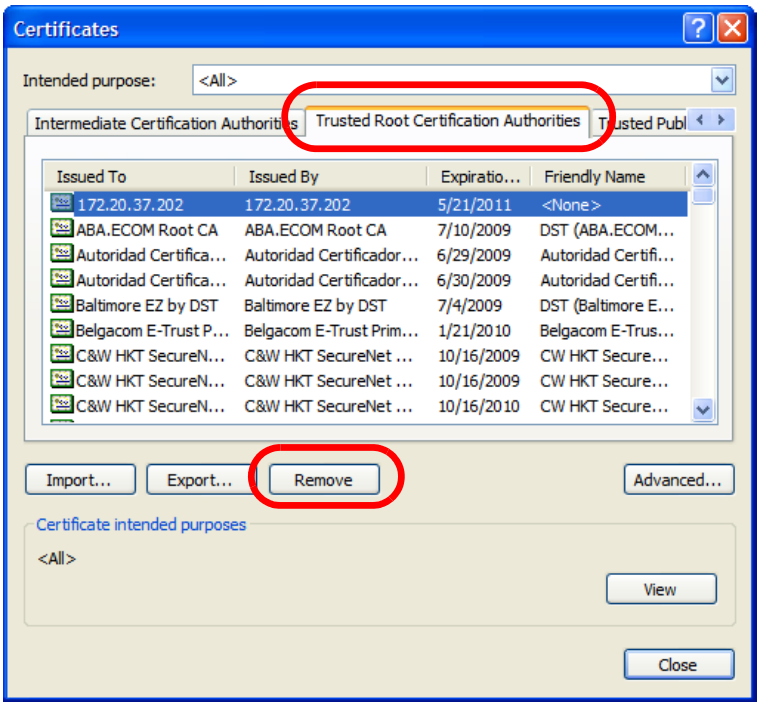
1 Запустите **Internet Explorer** и выберите в меню **Tools > Internet Options**.



2 В диалоговом окне **Internet Options** выберите **Content** > **Certificates**.

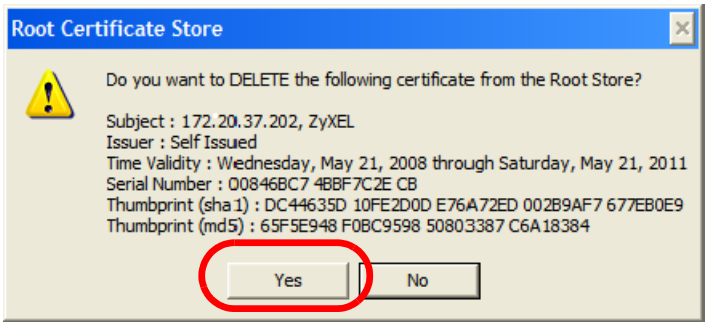


3 В диалоговом окне **Certificates** dialog box перейдите на вкладку **Trusted Root Certificates Authorities**, выберите сертификат, который необходимо удалить, и нажмите кнопку **Remove**.



4 В окне **Certificates** confirmation нажмите кнопку **Yes**.

5 В диалоговом окне **Root Certificate Store** нажмите кнопку **Yes**.



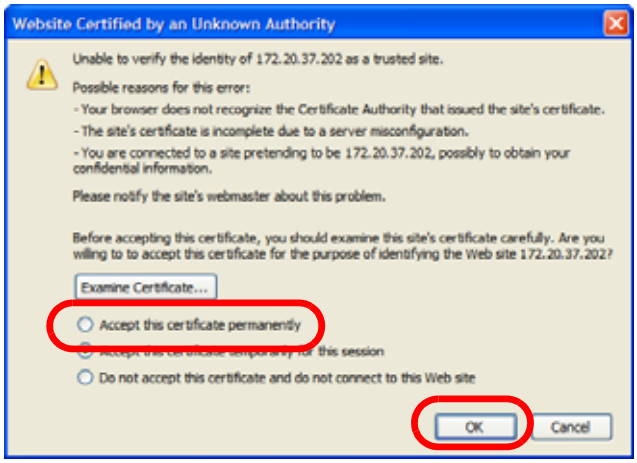
6 Теперь, при следующем переходе на веб-сайт, который выпустил только что удаленный сертификат с открытым ключом, появится сообщение об ошибке проверки сертификата.

Firefox

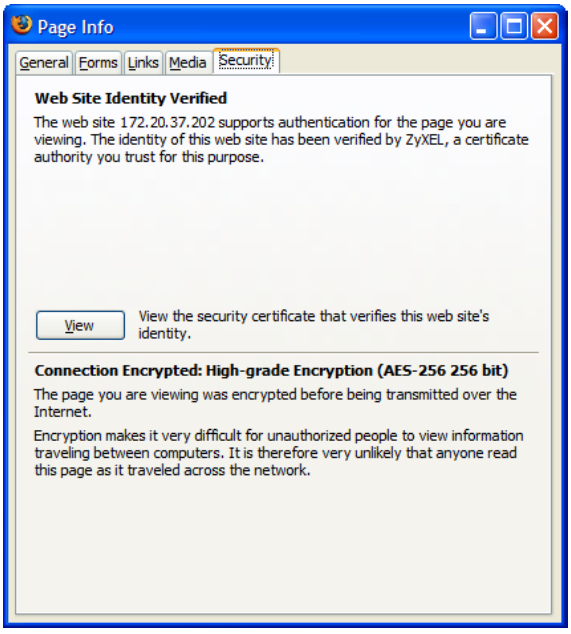
В примере ниже рассматривается процедура импорта сертификата для браузера Mozilla Firefox 2 в операционной системе Windows XP Professional; экраны, приведенные ниже, однако, применимы к работе с браузером Firefox 2 на всех платформах.

1 Если на Web-конфигураторе устройства включена проверка сертификатов SSL, то при первом заходе на страницу устройства появится сообщение об ошибке проверки сертификата.

2 Выберите опцию **Accept this certificate permanently** и нажмите кнопку **OK.**



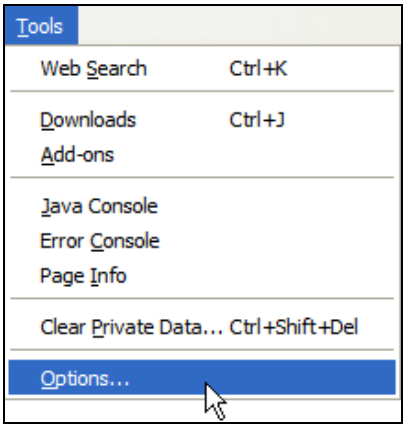
3 Сертификат будет сохранен, и теперь можно работать с Web-конфигуратором в защищенном режиме. В строке адреса появится пиктограмма запертого замка, щелкнув по которой, можно открыть окно **Page Info > Security** и ознакомиться с информацией о безопасности данной веб-страницы.



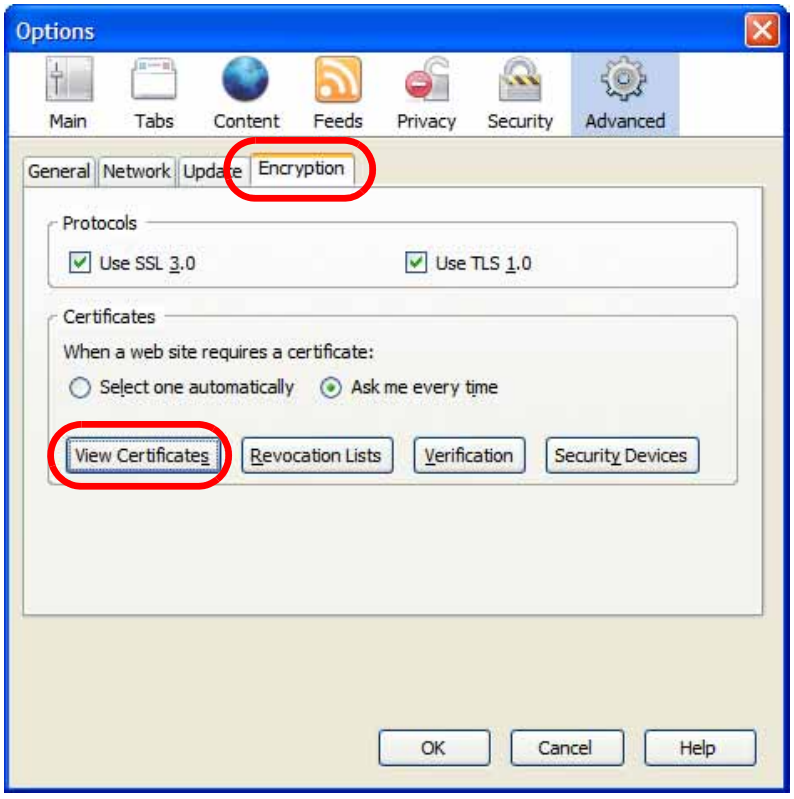
Установка автономного файла сертификата в Firefox

Вместо того, чтобы заходить на страницу ZyXEL Web-конфигуратора и устанавливать открытый ключ, воспользовавшись соответствующим предложением, можно установить автономный файл сертификата, если он был выпущен.

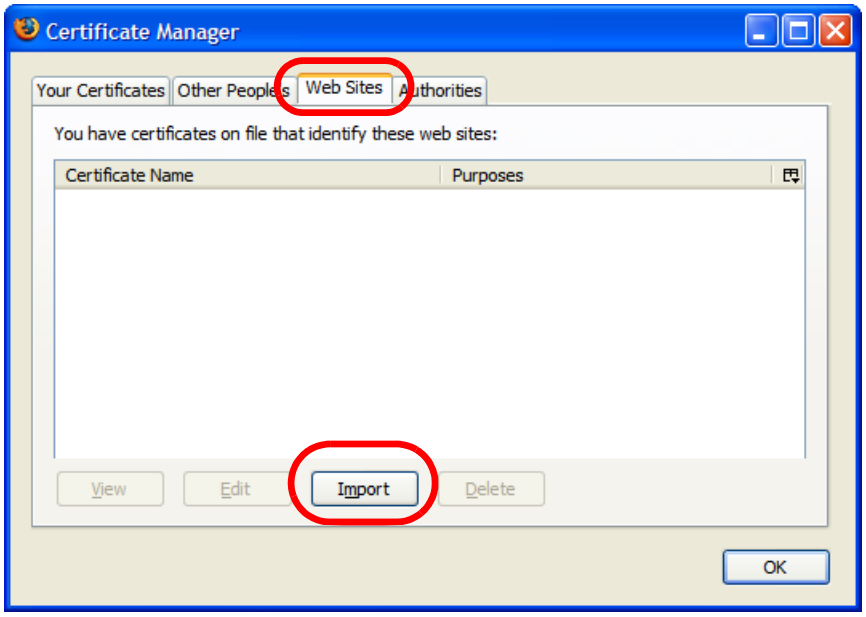
1 Запустите **Firefox** и выберите в меню **Tools > Options**.



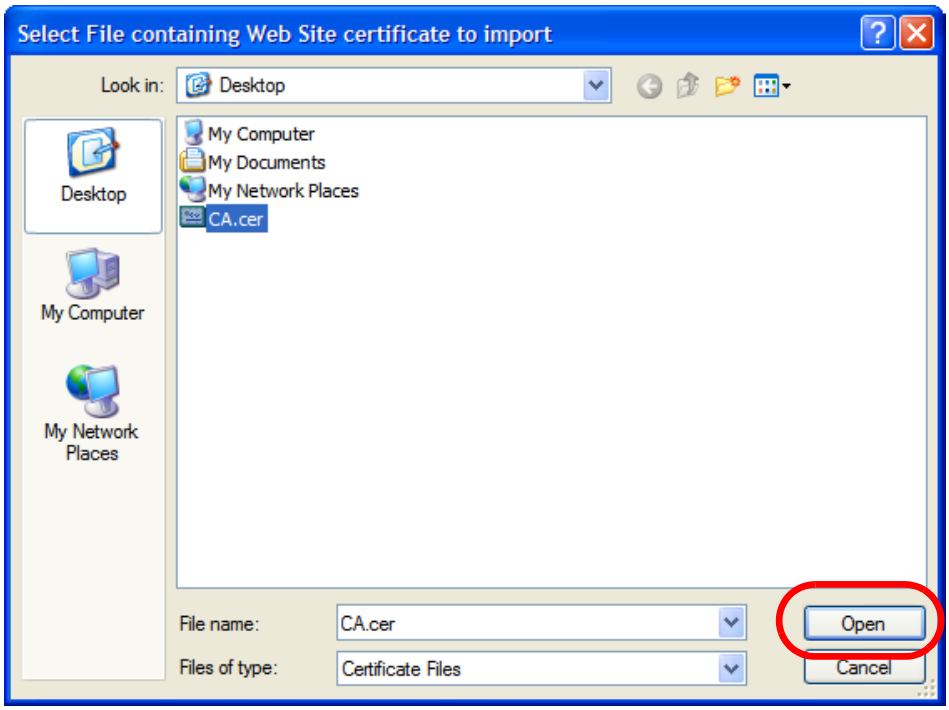
2 В диалоговом окне **Options** выберите **Advanced** > **Encryption** > **View Certificates**.



3 В диалоговом окне **Certificate Manager** выберите **Web Sites** > **Import**.



4 Найдите нужный сертификат с помощью диалогового окна **Select File** и нажмите кнопку **Open**.

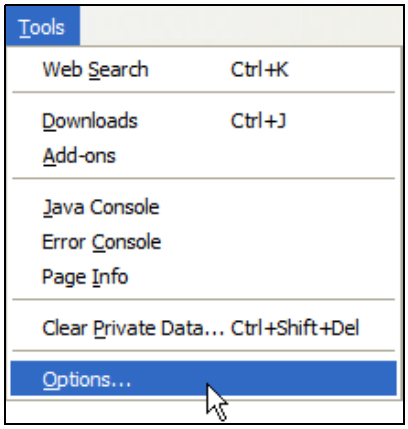


5 Теперь, при следующем переходе на этот веб-сайт в строке адреса появится пиктограмма запертого замка. Щелкнув по ней, можно открыть окно **Page Info > Security** и ознакомиться с информацией о безопасности данной страницы.

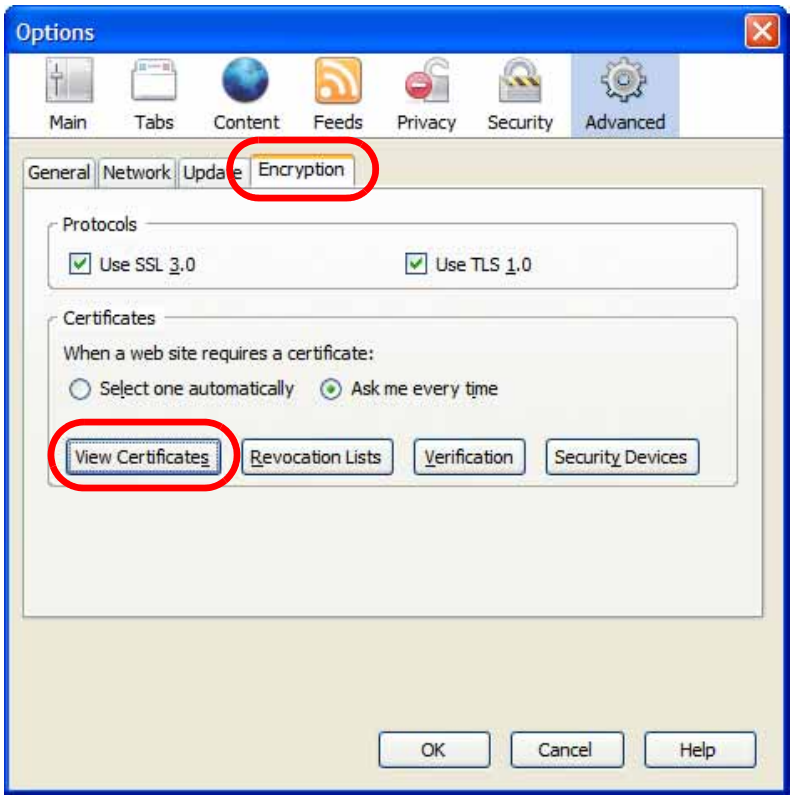
Удаление сертификата в Firefox

В этом разделе описана процедура удаления сертификата с открытым ключом в браузере Firefox 2.

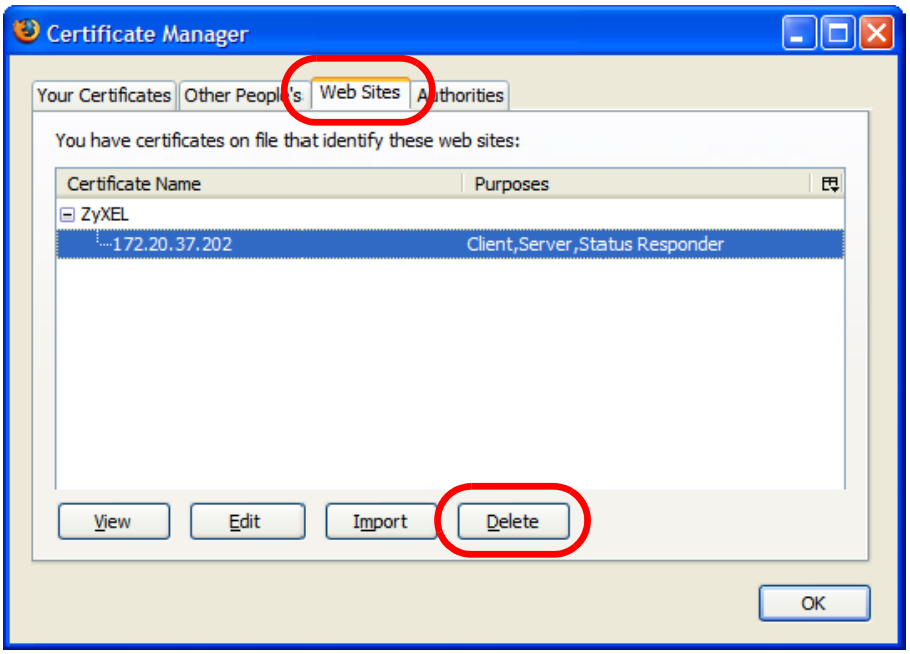
1 Запустите **Firefox** и выберите в меню **Tools** > **Options**.



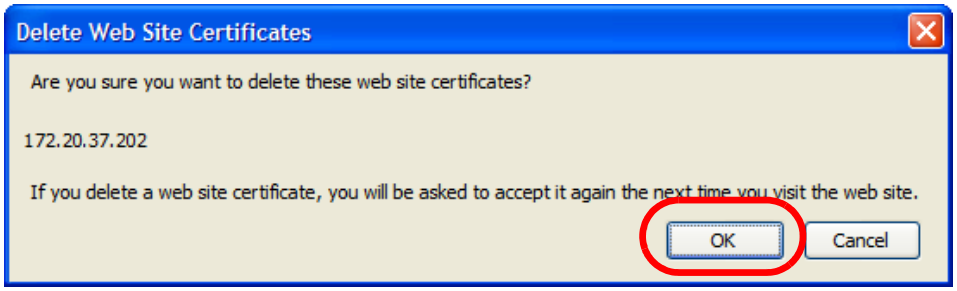
2 В диалоговом окне **Options** выберите **Advanced** > **Encryption** > **View Certificates**.



3 В диалоговом окне **Certificate Manager** перейдите на вкладку **Web Sites**, выберите сертификат, который необходимо удалить, и нажмите кнопку **Delete**.



4 В диалоговом окне **Delete Web Site Certificates** нажмите кнопку **OK**.



5 Теперь, при следующем переходе на веб-сайт, который выпустил только что удаленный сертификат с открытым ключом, появится сообщение об ошибке проверки сертификата.

D

Беспроводные сети

Варианты топологии беспроводных сетей

В этом разделе рассматриваются два варианта топологии беспроводных сетей – независимые (ad-hoc) и инфраструктурные (infrastructure) сети.

Динамическая (ad-hoc) конфигурация беспроводной сети

Наиболее простым вариантом конфигурации беспроводной сети является независимая (Ad-hoc) беспроводная сеть, которая связывает между собой компьютеры с беспроводными адаптерами (A, B, C). В любой момент времени, когда два и более беспроводных адаптеров находятся в зоне досягаемости друг у друга, они могут образовать независимую сеть, которую еще часто называют сетью ad-hoc network или независимым базовым набором служб (Independent Basic Service Set, IBSS). В примере на схеме, приведенной ниже, ноутбуки с беспроводными адаптерами образуют независимую беспроводную сеть.

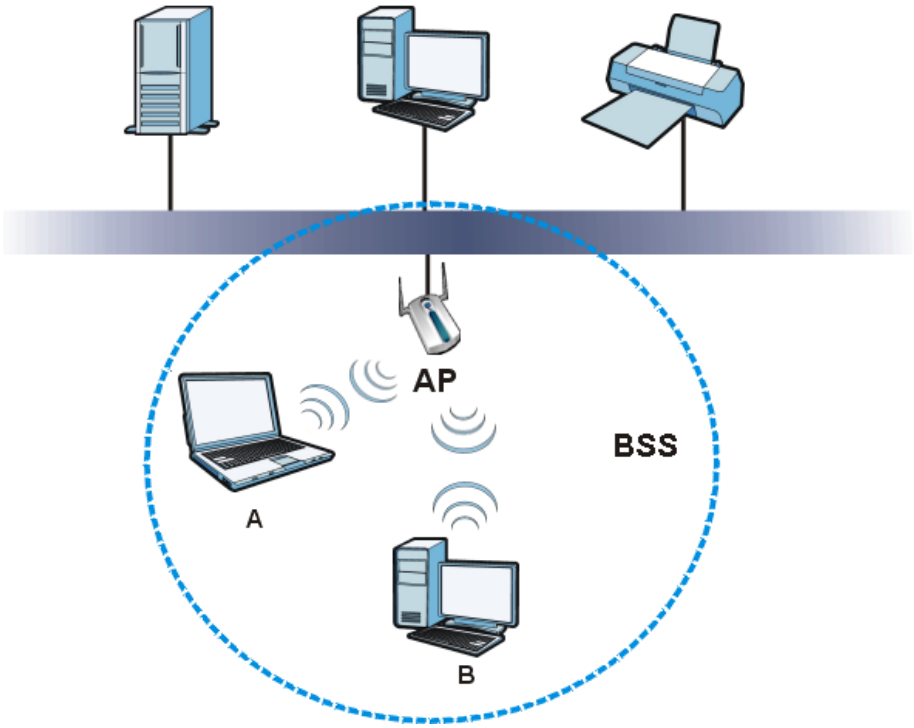
Рисунок 232 Одноранговая связь в независимой сети

BSS

Базовый набор служб (Basic Service Set, BSS) существует в том случае, когда все виды коммуникаций между беспроводными клиентами или между беспроводным клиентом и клиентом, подключенным к беспроводной сети, осуществляются через одну точку доступа (AP).

Внутренним трафиком BSS называется трафик между беспроводными клиентами в сети BSS. Если внутренний трафик BSS разрешен, беспроводные клиенты **A** и **B** получают доступ к проводной сети и могут установить связь друг с другом. Если внутренний трафик BSS запрещен, беспроводные клиенты **A** и **B** сохраняют возможность доступа к проводной сети, но не могут установить связь друг с другом.

Рисунок 233 Базовый набор служб



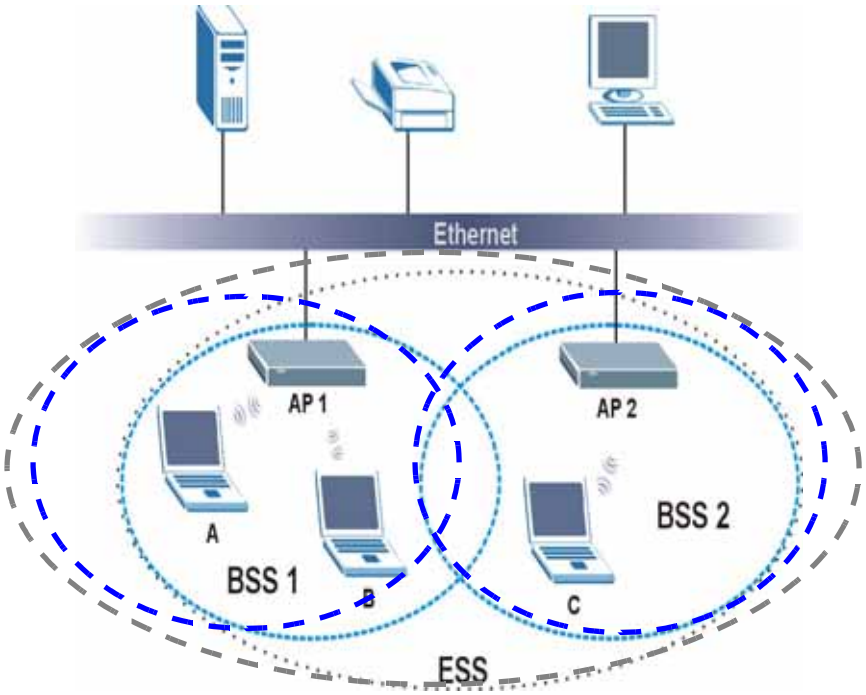
ESS

Расширенный набор служб (Extended Service Set, ESS) включает в себя серии пересекающихся сетей BSS, каждая из которых включает в себя точку доступа. Точки доступа соединены друг с другом через проводную сеть. Беспроводные соединения между точками доступа образуют распределительную систему (Distribution System, DS).

Этот вариант топологии беспроводных сетей называется инфраструктурной беспроводной сетью (Infrastructure WLAN). Точки доступа не только обеспечивают связь с проводной сетью, но и являются посредниками для беспроводного сетевого трафика в ближней зоне.

Идентификатор ESSID (ESS IDentification) уникальным образом идентифицирует каждую сеть ESS. Все точки доступа и ассоциированные с ними беспроводные клиенты в пределах одной сети ESS должны иметь одинаковый идентификатор ESSID для связи друг с другом.

Рисунок 234 Инфраструктурная беспроводная сеть



Канал

Канал – это одна или несколько радиочастот, используемых беспроводными устройствами для передачи и приема данных. Перечень доступных каналов зависит от географического региона. Доступных каналов в конкретном регионе может быть несколько, поэтому следует выбирать канал, отличный от канала, используемого соседней точкой доступа, чтобы снизить уровень помех. Помехи возникают при наложении радиосигналов от соседних точек доступа, что в конечном счете приводит к ухудшению производительности.

Соседние каналы, однако, частично накладываются друг на друга. Чтобы избежать помех, связанных с наложением каналов, точка доступа должна использовать канал, который отстоит как минимум на пять каналов от канала, используемого соседней точкой доступа. Например, если в данной местности всего доступно 11 каналов, и соседняя точка доступа использует канал 1, то необходимо выбрать канал в диапазоне от 6 до 11.

RTS/CTS

Скрытый узел возникает в том случае, если две станции находятся в диапазоне одной точки доступа, но при этом их диапазоны не пересекаются. На рисунке, приведенном ниже, изображен пример скрытого узла. Обе станции (STA) находятся в диапазоне точки доступа или беспроводного шлюза, но вне диапазона друг друга, то есть они не могут «слышать» друг друга и соответственно не могут знать, используется ли в настоящее время определенный канал. Такие станции считаются скрытыми друг от друга.

Рисунок 235 RTS/CTS

Когда станция **A** отправляет данные точке доступа, она может не «знать», что станция **B** уже использует тот же самый канал. Если две станции будут отправлять данные одновременно, то при одновременном поступлении данных на точку доступа может возникнуть коллизия, которая приведет к потере сообщений обоих станций.

Механизм **RTS/CTS** призван предотвратить коллизии, причиной которых являются скрытые узлы. Значение **RTS/CTS** определяет максимальный размер кадра данных, который можно отправить без согласования с использованием RTS (Request To Send)/CTS (Clear to Send).

Если размер кадра данных превышает установленное значение **RTS/CTS** (число из диапазона от 0 до 2432 байт), то станция, которая собирается передать этот кадр, должна вначале отправить сообщение RTS (готовность к передаче) точке доступа и получить разрешение на отправку. После этого точка доступа отправляет сообщение CTS (готовность к приему) всем остальным станциям в ее диапазоне, уведомляя их о необходимости отложить передачу. Кроме того, она резервирует и подтверждает запрашивающей станции временной интервал для запрашиваемой передачи.

Станции могут отправлять кадры, чей размер меньше указанного значения **RTS/CTS**, непосредственно точке доступа без согласования по процедуре RTS/CTS.

Включать опцию **RTS/CTS** следует только в том случае, если в сети существует вероятность появления скрытых узлов, и «цена» повторной отправки кадров большого размера оказывается больше, чем дополнительный служебный сетевой трафик, связанный с согласованием по процедуре RTS/CTS.

Если значение параметра **RTS/CTS** больше **порога фрагментации** (см. далее), то согласование по процедуре RTS/CTS не будет происходить вообще, поскольку система будет фрагментировать кадры данных, и они не смогут достичь размера, определенного в параметре **RTS/CTS**.

Примечание: Установка порога фрагментации приводит к появлению дополнительного служебного трафика, который вместо ожидаемого положительного эффекта может повлечь уменьшение пропускной способности.

Порог фрагментации

Порог фрагментации **Fragmentation Threshold** – это максимальный размер фрагмента данных (в диапазоне от 256 до 2432 байт), который можно отправить в беспроводной сети без разбиения его точкой доступа на более мелкие фрагменты.

Более высокий **порог фрагментации** рекомендуется устанавливать в сетях с малой вероятностью помех, меньший порог фрагментации – в сетях, подверженных частым перегрузкам, и сетях с высокой вероятностью помех.

Если **порог фрагментации** меньше, чем установленное значение параметра **RTS/CTS** (см. выше), то согласование по процедуре RTS/CTS не будет происходить вообще, поскольку система будет фрагментировать кадры данных, и они не смогут достичь размера, определенного в параметре **RTS/CTS**.

Тип преамбулы (Preamble Type)

Преамбула служит для индикации того, что данные приходят к принимающей стороне. Определения «короткая» и «длинная» относятся к длине поля синхронизации в пакете.

Короткая преамбула способствует повышению производительности, поскольку чем меньше времени тратится на отправку преамбулы, тем больше времени остается на отправку данных. Все беспроводные адаптеры с поддержкой стандарта IEEE 802.11 поддерживают длинную преамбулу, но не все поддерживают короткую.

Длинную преамбулу стоит использовать в тех случаях, когда неизвестно наверняка, какой режим преамбулы поддерживают другие устройства в сети, а также когда необходимо обеспечить более надежную связь в беспроводной сети с высокой нагрузкой.

Короткую преамбулу стоит использовать при наличии уверенности в том, что ее поддерживают все беспроводные устройства в сети, а также когда необходимо обеспечить более быструю связь.

Можно также воспользоваться режимом динамической настройки на устройстве NXC, которая позволяет автоматически использовать короткую преамбулу, если все беспроводные устройства в сети ее поддерживают, а в противном случае использовать длинную преамбулу.

Примечание: Для связи друг с другом беспроводные устройства ДОЛЖНЫ использовать одинаковый режим преамбулы.

Беспроводная сеть IEEE 802.11g

Стандарт IEEE 802.11g обладает полной совместимостью со стандартом IEEE 802.11b. Это означает, что адаптер IEEE 802.11b может напрямую подключаться к точке доступа IEEE 802.11g (и наоборот) на скорости 11 Мбит/с или меньше, в зависимости от диапазона. IEEE 802.11g предусматривает несколько промежуточных скоростей между максимальной и

минимальной скоростями передачи данных. Стандарт IEEE 802.11g поддерживает следующие скорости передачи данных и модуляции:

Таблица 220 IEEE 802.11g

СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (МБИТ/С)	МОДУЛЯЦИЯ
1	DBPSK (Differential Binary Phase Shift Keyed, дифференциальное двоичное переключение со сдвигом фазы)
2	DQPSK (Differential Quadrature Phase Shift Keying, дифференциальное четвертичное переключение со сдвигом фазы)
5.5 / 11	CCK (Complementary Code Keying, кодирование с использованием дополняющих кодов)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing, мультиплексирование с ортогональным частотным разделением)

Обзор средств безопасности в беспроводных сетях

Средства безопасности имеют первостепенное значение для защиты каналов связи между беспроводными клиентами, точками доступа и проводной сетью.

Устройство NXC поддерживает следующие методы обеспечения безопасности в беспроводной сети: шифрование данных, аутентификация беспроводных клиентов, ограничение доступа по MAC-адресу устройства и скрытие идентичности устройства NXC.

На рисунке, приведенном ниже, показана относительная эффективность перечисленных методов обеспечения безопасности беспроводной сети, поддерживаемых устройством NXC.

Таблица 221 Уровни безопасности в беспроводной сети

УРОВЕНЬ БЕЗОПАСНОСТИ	ТИП БЕЗОПАСНОСТИ
Менеебезопасные	Уникальный SSID (по умолчанию)
	Уникальный SSID с включенной опцией сокрытия SSID
	Фильтрация по MAC-адресам
	Шифрование по стандарту WEP
	Протокол EAP IEEE802.1x с аутентификацией на сервере RADIUS
	Поддержка стандарта WPA (Wi-Fi Protected Access, защищенный доступ к сети Wi-Fi)
Более безопасные	WPA2

Примечание: Необходимо установить одинаковые настройки безопасности беспроводной сети на устройстве NXC и на всех беспроводных клиентах, которые необходимо с ним ассоциировать.

IEEE 802.1x

В июне 2001 года был разработан стандарт IEEE 802.1x, расширяющий возможности стандарта IEEE 802.11 в части поддержки расширенной аутентификации и дополнительных функций

учета и контроля. Этот стандарт поддерживает операционная система Windows XP и большое количество сетевых устройств. Перечислим некоторые из преимуществ IEEE 802.1x:

- Идентификация по имени пользователя, обеспечивающая возможность роуминга.
- Поддержка протокола RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139), обеспечивающая централизованное хранение профилей пользователей и управление учетом на сетевом сервере RADIUS.
- Поддержка протокола EAP (Extensible Authentication Protocol, RFC 2486), позволяющая использовать дополнительные методы аутентификации без изменения конфигурации точек доступа и беспроводных клиентов.

RADIUS

В основе протокола RADIUS лежит клиент-серверная модель, которая поддерживает аутентификацию, авторизацию и учет. Точка доступа выступает в качестве клиента, а сервер RADIUS – в качестве сервера. Сервер RADIUS решает следующие задачи:

- Authentication

  Выполняет идентификацию пользователей.
- Авторизация

  Определяет перечень сетевых служб, доступных аутентифицированным пользователям после подключения к сети.
- Учет

  Отслеживает действия клиентов в сети.

RADIUS – это простой обмен пакетами, в рамках которого точка доступа действует как ретранслятор сообщений между беспроводным клиентом и сетевым сервером RADIUS.

Типы сообщений RADIUS

В процессе аутентификации пользователей точка доступа и сервер RADIUS обмениваются сообщениями RADIUS следующих типов:

- Доступ-Запрос (Access-Request)

  Инициируется точкой доступа, запрашивающей аутентификацию.
- Доступ-Отказ (Access-Reject)

  Инициируется сервером RADIUS, отказывающим в доступе.
- Доступ-Согласие (Access-Accept)

  Инициируется сервером RADIUS, разрешающим доступ.
- Доступ-Дополнительный запрос (Access-Challenge)

  Инициируется сервером RADIUS, запрашивающим дополнительную информацию для принятия решения о доступе. Точка доступа отправляет соответствующий ответ от пользователя, а затем отправляет еще одно сообщение типа «доступ-запрос».

При выполнении функций учета пользователей точка доступа и сервер RADIUS обмениваются сообщениями RADIUS следующих типов:

- Учет-Запрос (Accounting-Request)

  Инициируется точкой доступа, запрашивающей операцию учета.

- Учет-Ответ (Accounting-Response)

  Инициируется сервером RADIUS для индикации начала или остановки операции учета.

Для обеспечения безопасности сети точка доступа и сервер RADIUS используют общий секретный ключ, то есть пароль, который известен им обоим. Этот ключ не пересылается по сети. Помимо использования секретного ключа производится шифрование информации о пароле, которой обмениваются стороны, чтобы защитить сеть от несанкционированного доступа.

Типы аутентификации EAP

В этом разделе рассматриваются некоторые популярные типы аутентификации: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP и LEAP. Беспроводное устройство, возможно, поддерживает не все из перечисленных типов аутентификации.

EAP (Extensible Authentication Protocol) – это протокол аутентификации, который действует поверх транспортного механизма IEEE 802.1x, обеспечивая поддержку различных типов аутентификации пользователей. Используя протокол EAP для взаимодействия с EAP-совместимым сервером RADIUS, точка доступа помогает беспроводной станции и серверу RADIUS выполнить аутентификацию.

Используемый тип аутентификации зависит от сервера RADIUS и промежуточной точки (или точек) доступа, которая поддерживает стандарт IEEE 802.1x. .

При использовании аутентификации типа EAP-TLS необходимо вначале подключиться к сети по проводному соединению и получить сертификат (или сертификаты) от центра сертификации. Сертификат (именуемый также цифровым идентификатором) может использоваться для аутентификации пользователей. Центр сертификации выпускает сертификаты и гарантирует подлинность владельца каждого сертификата.

EAP-MD5 (Message-Digest Algorithm 5)

Аутентификация MD5 – это простейший односторонний метод аутентификации. Сервер аутентификации отправляет запрос (challenge) беспроводному клиенту. Беспроводной клиент «подтверждает», что ему известен пароль, – он шифрует пароль вместе с запросом и отправляет результирующую информацию обратно. Пароль не пересылается в обычном текстовом виде.

Однако у аутентификации MD5 есть некоторые недостатки. Серверу аутентификации необходимо получать пароли в виде обычного текста, поэтому пароли необходимо хранить. Соответственно, доступ к файлу пароля может получить кто-то еще, кроме сервера аутентификации. Кроме того, злоумышленник может изобразить сервер аутентификации, поскольку метод аутентификации MD5 не предусматривает взаимной аутентификации. Наконец, метод аутентификации MD5 не поддерживает шифрование данных с помощью динамического сессионного ключа. Для шифрования данных необходимо настроить ключи шифрования WEP.

EAP-TLS (Transport Layer Security, безопасность транспортного уровня)

При использовании аутентификации типа EAP-TLS и серверу, и беспроводным клиентам необходимы цифровые сертификаты для взаимной аутентификации. Сервер предоставляет сертификат клиенту. После проверки подлинности сервера клиент отправляет серверу другой сертификат. Обмен сертификатами происходит в открытом режиме, до создания защищенного

туннеля. Это делает идентификационные данные пользователей уязвимыми для пассивных атак. Цифровой сертификат – это электронная идентификационная карта, которая удостоверяет подлинность отправителя. Для реализации аутентификации типа EAP-TLS нужен центр сертификации для обработки сертификатов, который создает дополнительный служебный трафик.

EAP-TTLS (Tunneled Transport Layer Service, служба туннелированного транспортного уровня)

EAP-TTLS – это расширение типа аутентификации EAP-TLS, которое использует сертификаты только для аутентификации на стороне сервера для организации защищенного соединения. Аутентификация клиента осуществляется путем отправки имени пользователя и пароля по защищенному соединению, таким образом обеспечивается защита идентификационных данных клиента. При аутентификации клиентов EAP-TTLS поддерживает как методы EAP, так и унаследованные методы аутентификации, такие, как PAP, CHAP, MS-CHAP и MS-CHAP v2.

PEAP (Protected EAP, защищенный EAP)

Как и в случае EAP-TTLS, для установки защищенного соединения здесь применяется аутентификация на стороне сервера с использованием сертификата, затем по защищенному соединению с помощью простых методов передаются имя пользователя и пароль для аутентификации клиентов, обеспечивая конфиденциальность идентификационных данных клиента. PEAP, однако, поддерживает для аутентификации клиентов только методы EAP, такие, как EAP-MD5, EAP-MSCHAPv2 и EAP-GTC (EAP-Generic Token Card). Тип аутентификации EAP-GTC реализует только компания Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) – это реализация стандарта IEEE 802.1x, выполненная компанией Cisco.

Обмен динамическими ключами WEP

Данный протокол аутентификации использует соответствие уникального ключа, который генерирует сервер RADIUS. Срок действия ключа заканчивается при разрыве беспроводного соединения по тайм-ауту, при отключении или при запросе повторной аутентификации. При выполнении повторной аутентификации каждый раз генерируется новый ключ WEP.

Если эта функция включена, то необходимости создавать ключ шифрования по умолчанию на экране настройки безопасности беспроводной сети нет. Можно точно так же создавать и хранить ключи, но, если включена функция динамического обмена ключами WEP, они не будут использоваться.

Примечание: Использовать тип аутентификации EAP-MD5 одновременно с обменом динамическими ключами WEP нельзя

С целью повышения безопасности процедуры аутентификации на основе сертификатов (EAP-TLS, EAP-TTLS и PEAP) используют динамические ключи для шифрования данных. Их часто используют в корпоративной инфраструктуре, но при развертывании в общественных помещениях простая пара «имя пользователя – пароль» является более практичной.

Сравнительный анализ возможностей различных типов аутентификации приведен в следующей таблице.

Таблица 222 Сравнительный анализ типов аутентификации EAP

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Взаимная аутентификация	Нет	Да	Да	Да	Да
Сертификат – Клиент	Нет	Да	Опционально	Опционально	Нет
Сертификат – Сервер	Нет	Да	Да	Да	Нет
Обмен динамическими ключами	Нет	Да	Да	Да	Да
Целостность учетных данных	Нет	Высокая	Высокая	Высокая	Умеренная
Сложность внедрения	Низкая	Высокая	Умеренная	Умеренная	Умеренная
Защита учетных данных клиента	Нет	Нет	Да	Да	Нет

WPA и WPA2

Wi-Fi Protected Access (WPA) – это подраздел стандарта IEEE 802.11i. WPA2 (IEEE 802.11i) – это стандарт безопасности для беспроводной связи, который описывает более строгие методы шифрования, аутентификации и управления ключами по сравнению с WPA.

В первую очередь WPA/WPA2 отличаются от WEP более мощным методом шифрования данных и более строгими правилами аутентификации пользователей.

Если и точка доступа, и беспроводные клиенты поддерживают WPA2, и имеется внешний сервер RADIUS, используйте стандарт WPA2 для более мощного шифрования данных. Если внешнего сервера RADIUS не имеется, необходимо использовать WPA2-PSK (WPA2-Pre-Shared Key), который требует ввода одного (идентичного) пароля на любой точке доступа, беспроводном шлюзе и беспроводном клиенте. Если пароли совпадают, беспроводному клиенту будет предоставлен доступ к беспроводной сети.

Если точка доступа или беспроводные клиенты не поддерживают WPA2, используйте WPA или WPA-PSK в зависимости от наличия внешнего сервера RADIUS.

Используйте WEP только в том случае, если точка доступа и/или беспроводные клиенты не поддерживают WPA или WPA2. Стандарт WEP менее безопасен, чем WPA или WPA2.

Шифрование

Обе технологии – и WPA, и WPA2 – повышают качество шифрования данных за счет использования протокола TKIP (Temporal Key Integrity Protocol, протокол обеспечения целостности с помощью временного ключа), функции MIC (Message Integrity Check, проверка целостности сообщений) и поддержки стандарта IEEE 802.1x. WPA и WPA2 используют стандарт шифрования AES (Advanced Encryption Standard) в сочетании с протоколом CCMP (Counter mode with Cipher block chaining Message authentication code Protocol, протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика), чтобы обеспечить более мощное шифрование по сравнению с протоколом TKIP.

TKIP использует 128-разрядные ключи, которые динамически генерирует и распространяет сервер аутентификации. AES (Advanced Encryption Standard) – это блочный шифр, который

использует 256-разрядный математический алгоритм под названием Рэндал (Rijndael). Оба алгоритма включают в себя функцию смешивания ключей на уровне пакетов, функцию MIC (Message Integrity Check, проверка целостности сообщений) под названием Майкл (Michael), расширенный вектор инициализации (IV) с правилами определения последовательностей и механизм повторной генерации ключей (re-keying).

WPA и WPA2 регулярно меняют и ротируют ключи шифрования, поэтому один и тот же ключ шифрования никогда не используется дважды.

Сервер RADIUS передает ключ PMK (Pairwise Master Key, парный главный ключ) точке доступа, которая формирует иерархию ключей и систему управления ими. Точка доступа использует ключ PMK для динамической генерации уникальных ключей шифрования данных для шифрования каждого пакета данных, которым обмениваются в беспроводной сети точка доступа и беспроводные клиенты. Все это происходит автоматически, в фоновом режиме.

Функция MIC (Message Integrity Check, проверка целостности сообщений) призвана защитить пакеты данных от попыток записи их злоумышленником. С этой целью функция MIC изменяет и пересылает пакеты повторно. MIC использует мощную математическую функцию, пользуясь которой приемник и передатчик рассчитывают, а затем сравнивают полученные значения MIC. Если они не совпадают, то предполагается, что данные были искажены, и такой пакет отбрасывается.

Благодаря генерации уникальных ключей шифрования данных для каждого пакета данных и созданию механизма проверки целостности (MIC) использование протоколов TKIP и AES усложняет процесс дешифрации данных в сети Wi-Fi по сравнению с технологией WEP и уменьшает вероятность проникновения в сеть злоумышленников.

WPA(2) и WPA(2)-PSK используют одинаковые механизмы шифрования. Единственная разница между ними состоит в том, что WPA(2)-PSK использует простой общий пароль вместо учетных данных конкретного пользователя. Подход на основе общего пароля делает алгоритм WPA(2)-PSK уязвимым к атакам путем перебора ключей, но все равно этот алгоритм является более совершенным по сравнению с алгоритмом WEP, поскольку он предусматривает целостный, единый, алфавитно-цифровой пароль для создания ключа PMK, который используется для генерации уникальных временных ключей шифрования. Это исключает ситуацию, при которой все беспроводные устройства используют одинаковые ключи шифрования. (недостаток WEP)

Аутентификация пользователей

WPA и WPA2 используют стандарт IEEE 802.1x и протокол EAP (Extensible Authentication Protocol) для аутентификации беспроводных клиентов с использованием базы данных внешнего сервера RADIUS. WPA2 уменьшает число сообщений об обмене ключами с шести до четырех (4-стороннее согласование CCMP) и сокращает время, необходимое для подключения к сети. WPA2 включает в себя еще две функции, которых нет в WPA – кэширование ключей и предварительную аутентификацию. Обе названные функции являются опциональными, и не все беспроводные устройства могут их поддерживать.

Кэширование ключей позволяет беспроводному клиенту хранить ключ PMK, созданный в результате успешной аутентификации на точке доступа. Беспроводной клиент использует этот ключ PMK при попытке подключения к той же точке доступа, при этом клиент не должен проходить процесс аутентификации повторно.

Предварительная аутентификация (pre-authentication) создает условия для быстрого роуминга за счет того, что беспроводной клиент (уже подключающийся к одной точке доступа) может

пройти аутентификацию по стандарту IEEE 802.1x с другой точкой доступа перед подключением к ней.

Модули предоставления данных для аутентификации беспроводных клиентов (WPA)

Модуль предоставления данных для аутентификации беспроводного клиента – это программное обеспечение, которое работает под управлением определенной операционной системы и информирует беспроводного клиента о том, как использовать WPA. На момент написания данного документа наиболее распространенным модулем предоставления данных для аутентификации являлось обновление WPA для Windows XP, клиент Odyssey от Funk Software.

Обновление для Windows XP – это бесплатно загружаемое дополнение, которое добавляет поддержку WPA для встроенного беспроводного клиента Windows XP, не требующего настройки. Использовать обновление можно только в операционной системе Windows XP.

Пример использования WPA(2) с сервером RADIUS

Чтобы организовать работу с использованием технологии WPA(2), необходимо знать IP-адрес сервера RADIUS, номер его порта (по умолчанию – 1812) и общий секретный код RADIUS. Пример использования WPA(2) с внешним сервером RADIUS выглядит следующим образом. «A» – это сервер RADIUS. «DS» – это система распространения.

1. Точка доступа передает запрос на аутентификацию беспроводного клиента серверу RADIUS.
2. Сервер RADIUS сверяет полученные идентификационные данные пользователя со своей базой данных и в зависимости от результатов сверки либо разрешает, либо запрещает доступ к сети.
3. В процессе аутентификации между сервером RADIUS и клиентом создается 256-разрядный парный главный ключ (Pairwise Master Key, PMK).
4. Сервер RADIUS передает этот ключ PMK точке доступа. Затем точка доступа создает иерархию ключей и систему управления ими, используя ключ PMK для динамической генерации уникальных ключей шифрования данных. Эти ключи используются для шифрования всех пакетов данных, которыми точка доступа и беспроводные клиенты обмениваются по беспроводной сети.

Рисунок 236 Пример использования WPA(2) с сервером RADIUS

Пример использования WPA(2)-PSK

Пример использования WPA(2)-PSK выглядит следующим образом.

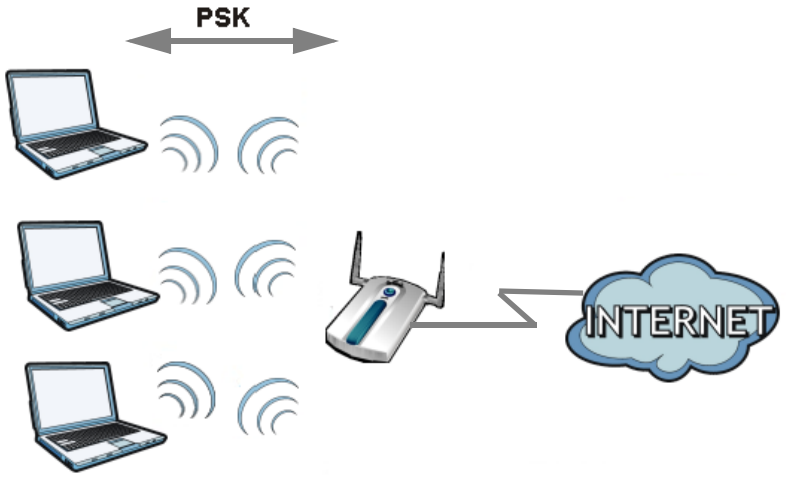
1. Вначале необходимо ввести одинаковый пароль на точке доступа и на всех беспроводных клиентах. Предварительно выданный ключ (Pre-Shared Key, PSK) должен включать в себя от 8 до 63 символов ASCII или 64 шестнадцатеричных символа (включая пробелы и специальные символы).

2. Точка доступа проверяет пароль каждого беспроводного клиента и разрешает ему доступ к сети только в том случае, если этот пароль совпадает с паролем, введенным на точке доступа.

3. Точка доступа и беспроводные клиенты генерируют общий парный главный ключ (PMK, Pairwise Master Key). Сам по себе ключ не пересылается по сети, он создается на основе ключа PSK и идентификатора SSID.

4. Точка доступа и беспроводные клиенты используют процесс шифрования TKIP или AES. В процессе согласования происходит обмен ключом PMK и дополнительной информацией для создания временных ключей шифрования. Впоследствии они используют эти ключи шифрования для шифрования данных, циркулирующих между ними.

Рисунок 237 Аутентификация WPA(2)-PSK



Сводная информация о параметрах безопасности

Эта таблица содержит информацию о том, какие еще параметры безопасности необходимо настроить для каждого метода аутентификации или типа протокола управления ключами. Фильтры по MAC-адресам не зависят от того, каким образом будут настроены эти параметры безопасности.

Таблица 223 Относительная матрица параметров безопасности в беспроводных сетях

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	ВВОД КЛЮЧА ВРУЧНУЮ	IEEE 802.1X
Открытая система	Нет	Нет	Отключено
			Включен без динамического ключа WEP
Открытая система	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен без динамического ключа WEP
		Да	Отключено
Общий ключ	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен без динамического ключа WEP
		Да	Отключено
WPA	TKIP/AES	Нет	Enable
WPA-PSK	TKIP/AES	Да	Отключено
WPA2	TKIP/AES	Нет	Enable
WPA2-PSK	TKIP/AES	Да	Отключено

E

IPv6

Обзор

IPv6 (версия 6 протокола IP, Internet Protocol) была разработана с целью увеличения размера и функциональности IP-адресов. Увеличение размера адреса IPv6 до 128 битов (по сравнению с 32-битными адресами IPv4) позволяет увеличить количество доступных IP-адресов до 3,4 x 10^{38}.

Адресация IPv6

128-разрядный адрес IPv6 записывается в виде восьми 16-битных шестнадцатеричных блоков, разделенных двоеточием (:). Вот пример адреса IPv6:
`2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

Адреса IPv6 можно сокращать двумя способами:

- Ведущие нули в блоках можно опускать. Например, адрес `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` можно записать в виде `2001:db8:1a2b:15:0:0:1a2f:0`.
- Любое число последовательных блоков, состоящих из нулей, можно заменить двойным двоеточием. Двойное двоеточие можно использовать при написании адреса IPv6 только один раз. Соответственно, адрес `2001:0db8:0000:0000:1a2f:0000:0000:0015` можно записать как `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` или `2001:db8:0:0:1a2f::15`.

Префикс и его длина

По аналогии с маской подсети для IPv4 протокол IPv6 использует адресный префикс для указания на адрес сети. Длина префикс IPv6 говорит о том, сколько наиболее значимых битов адреса, если отсчитывать слева, составляют адрес сети. Длина префикса записывается в формате «/x», где x – это число. Например,

```
запись 2001:db8:1a2b:15::1a2f:0/32
```

означает, что первые 32 бита (`2001:db8`) являются адресом подсети.

Адрес Link-local

Адрес link-local уникальным образом идентифицирует устройство в локальной сети. Он аналогичен «частному IP-адресу» протокола IPv4. Один и тот же адрес link-local может быть назначен двум и более интерфейсам одного устройства. Однонаправленный адрес link-local имеет предопределенный префикс fe80::/10. Формат однонаправленного адреса link-local выглядит следующим образом.

Таблица 224 Формат однонаправленного адреса link-local

1111 1110 10	0	Идентификатор интерфейса
10 битов	54 бита	64 бита

Глобальный адрес

Глобальный адрес уникальным образом идентифицирует устройство в сети Интернет. Он аналогичен «внешнему IP-адресу» протокола IPv4. Глобальный однонаправленный адрес начинается с 2 или 3.

Неуказанный адрес

Неуказанный адрес (0:0:0:0:0:0:0:0 или ::) используется в качестве адреса источника в том случае, если устройство не имеет собственного адреса. Он аналогичен адресу «0.0.0.0» протокола IPv4.

Адрес обратной петли

Адрес обратной петли (0:0:0:0:0:0:0:1 или ::1) дает хосту возможность отправлять пакеты самому себе. Этот тип адреса аналогичен адресу «127.0.0.1» протокола IPv4.

Адрес для многоадресной рассылки

Адреса для многоадресной рассылки протокола IPv6 выполняют ту же функцию, что и широковещательные адреса протокола IPv4. Протокол IPv6 не поддерживает широковещательные рассылки. Адрес для многоадресной рассылки позволяет хосту рассылать пакеты всем хостам, входящим в группу многоадресной рассылки.

Масштаб многоадресной рассылки позволяет определять размер группы многоадресной рассылки. Адрес для многоадресной рассылки имеет предопределенный префикс ff00::/8. В таблице ниже приведено описание некоторых предопределенных адресов для многоадресной рассылки.

Таблица 225 Предопределенные адреса для многоадресной рассылки

АДРЕС ДЛЯ МНОГОАДРЕСНОЙ РАССЫЛКИ	ОПИСАНИЕ
FF01:0:0:0:0:0:0:1	Все хосты на локальном узле.
FF01:0:0:0:0:0:0:2	Все маршрутизаторы на локальном узле.
FF02:0:0:0:0:0:0:1	Все хосты на локально подключенном соединении.
FF02:0:0:0:0:0:0:2	Все маршрутизаторы на локально подключенном соединении.
FF05:0:0:0:0:0:0:2	Все маршрутизаторы на локальной площадке.
FF05:0:0:0:0:0:1:3	Все DHCP-серверы на локальной площадке.

В таблице ниже приведен список зарезервированных адресов для многоадресной рассылки, которые нельзя назначить группе многоадресной рассылки.

Таблица 226 Зарезервированные адреса для многоадресной рассылки

АДРЕС ДЛЯ МНОГОАДРЕСНОЙ РАССЫЛКИ
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Маски подсети

И адрес IPv6, и маска подсети IPv6 состоят из 128-битных цифр, которые разбиты на восемь 16-битных блоков и записаны в шестнадцатеричной нотации. Шестнадцатеричная нотация использует четыре бита под каждый символ (1 ~ 10, A ~ F). 16 битов каждого блока затем представляются в виде четырех шестнадцатеричных символов. Например, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Идентификатор интерфейса

В протоколе IPv6 идентификатор интерфейса – это 64-битное число. Он идентифицирует физический интерфейс (например, порт Ethernet) или виртуальный интерфейс (например, IP-адрес управления для сети VLAN). Каждый интерфейс должен иметь уникальный идентификатор.

EUI-64

Расширенный уникальный идентификатор EUI-64 (Extended Unique Identifier), разработанный институтом IEEE (Institute of Electrical and Electronics Engineers), – это формат идентификатора интерфейса, адаптированный для протокола IPv6. Как показано ниже, он является производным от 48-битного (6-байтового) MAC-адреса Ethernet. EUI-64 вставляет шестнадцатеричные цифры fffe между третьим и четвертым байтами MAC-адреса и дополняет седьмой бит первого байта MAC-адреса.

Пример приводится ниже.

Таблица 227

MAC	00	:	13	:	49	: 12	:	34	:	56	

Таблица 228

EUI-64	02	:	13	:	49	:	FF	:	FE	: 12	:	34	:	56

Автоматическая настройка без сохранения состояния

Функция автоматической настройки без сохранения состояния для IPv6 позволяет автоматически генерировать уникальные адреса. В отличие от DHCPv6 (Dynamic Host Configuration Protocol версии шесть), который используется для автоматической настройки IPv6 с сохранением состояния, в данном случае DHCP-сервер не должен хранить сведения о владельце и состоянии адресов. Каждое устройство IPv6 может сгенерировать собственный, уникальный IP-адрес автоматически, если на данном интерфейсе включена поддержка IPv6. Полный адрес IPv6 формируется из префикса и идентификатора интерфейса (сгенерированного на основе собственного MAC-адреса Ethernet, см. Идентификатор интерфейса и EUI-64).

Если на устройстве включена поддержка IPv6, то его интерфейс автоматически генерирует адрес link-local (начинающийся с префикса fe80).

Если этот интерфейс подключен к сети с маршрутизатором, а настройки NXC предусматривают автоматическое получение сетевого префикса IPv6 для данного интерфейса с маршрутизатора, то он генерирует еще один адрес, сочетающий в себе идентификатор интерфейса, информацию о глобальной сети и информацию о подсети, полученную от маршрутизатора[2]. Это будет маршрутизируемый, глобальный IP-адрес.

DHCPv6

Протокол DHCPv6 (Dynamic Host Configuration Protocol for IPv6, протокол динамической конфигурации хостов для IPv6, RFC 3315) – это клиент-серверный протокол, который позволяет DHCP-серверу назначать и передавать сетевые адреса, префиксы и другие сведения о конфигурации IPv6 DHCP-клиентам. Серверы и клиенты DHCPv6 обмениваются сообщениями DHCP с использованием протокола UDP.

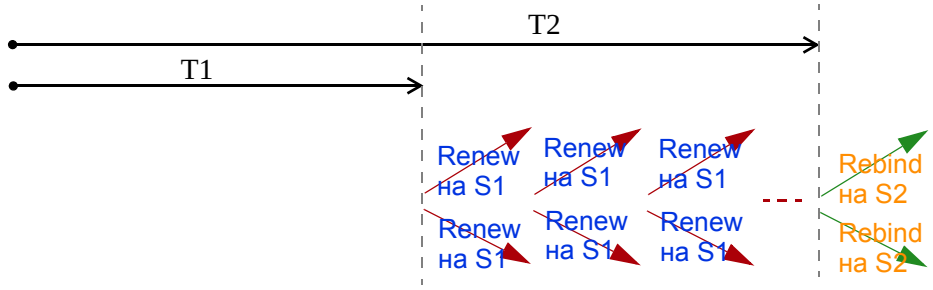
Каждый DHCP-клиент и DHCP-сервер имеет уникальный идентификатор DHCP (DHCP Unique IDentifier, DUID), который используется для идентификации при обмене сообщениями DHCPv6. DUID генерируется на основе MAC-адреса, времен, идентификатора, назначенного поставщиком, и/или частного корпоративного номера поставщика, зарегистрированного в IANA. DUID не должен меняться со временем, даже после перезагрузки устройства.

Ассоциация идентификаторов

Ассоциация идентификаторов (Identity Association, IA) – это коллекция адресов, назначенных DHCP-клиенту, посредством которой сервер и клиент могут управлять группой связанных IP-адресов. Каждая ассоциация IA должна быть ассоциирована только с одним интерфейсом. DHCP-клиент использует ассоциацию IA, назначенную данному интерфейсу, для получения настроек для данного интерфейса с DHCP-сервера. Каждая ассоциация IA включает в себя уникальный идентификатор IAID и связанную с ним информацию протокола IP.

2. Протокол IPv6 допускает привязку двух и более адресов к любому сетевому интерфейсу.

Тип IA – это тип адреса в IA. Каждая ассоциация IA хранит адреса одного типа. IA_NA означает ассоциацию идентификаторов для постоянных адресов, а IA_TA – ассоциацию идентификаторов для временных адресов. Опция IA_NA содержит поля T1 и T2, а опция IA_TA – нет. Сервер DHCPv6 использует поля T1 и T2 для управления временем обращения клиента к серверу с целью заблаговременного продления сроков жизни любых адресов, входящих в ассоциацию IA_NA. При наступлении момента времени T1 клиент отправляет серверу (**S1**), от которого были получены адреса, содержащиеся в ассоциации IA_NA, сообщение Renew. Если уже наступил момент времени T2, а сервер не отвечает, то клиент отправляет сообщение Rebind любому доступному серверу (**S2**). В случае ассоциации IA_TA клиент может посылать сообщения Renew или Rebind по собственному усмотрению.



Агент ретрансляции DHCP

Агент ретрансляции DHCP находится в одной сети с DHCP-клиентами и помогает пересылать сообщения между DHCP-сервером и DHCP-клиентами. Если клиент не может использовать собственный адрес link-local и хорошо известный адрес для многоадресной рассылки для поиска DHCP-сервера в своей сети, то ему нужен агент ретрансляции DHCP для отправки сообщения DHCP-серверу, находящемуся в другой сети.

Агент ретрансляции DHCP может добавлять опцию удаленной идентификации (remote-ID) и опцию идентификации интерфейса (interface-ID) в сообщения Relay-Forward протокола DHCPv6. Опция remote-ID содержит строку, заданную пользователем, например, имя системы. Опция interface-ID передает серверу DHCPv6 сведения о номере слота, информация о портах и идентификатор VLAN. Опция remote-ID (если она есть) удаляется из сообщений Relay-Reply до момента отправки пакетов агентом ретрансляции клиентам. DHCP-сервер копирует опцию interface-ID из сообщения Relay-Forward в сообщение Relay-Reply и отправляет его агенту ретрансляции. Значение interface-ID не должно меняться даже после перезапуска агента ретрансляции.

Делегирование префикса

Функция делегирования префикса позволяет маршрутизатору IPv6 использовать префикс IPv6 (сетевой адрес), полученный от провайдера услуг Интернет (или агрегирующего маршрутизатора), для локальной сети. Устройство NXC использует полученный префикс IPv6 (например, 2001:db2::/48) для генерации собственного IP-адреса в локальной сети. Устройство NXC передает информацию о префиксе IPv6 хостам в локальной сети посредством регулярной многоадресной рассылки анонсов маршрутизатора (Router Advertisements, RA). После получения сведений о префиксе хосты могут использовать его для генерации собственных адресов IPv6.

ICMPv6

Протокол ICMPv6 (Internet Control Message Protocol for IPv6 или ICMP for IPv6) описан в документе RFC 4443. Для ICMPv6 значение поля Next Header равно 58 – это отличается от значения, используемого для идентификации ICMP for IPv4. ICMPv6 является неотъемлемой частью IPv6. Узлы IPv6 используют ICMPv6 для информирования об ошибках, которые встретились при обработке пакетов, и выполнения других диагностических функций, таких, как «ping».

Протокол Neighbor Discovery Protocol (NDP)

Протокол NDP (Neighbor Discovery Protocol, протокол обнаружения соседей) – это протокол, используемый для обнаружения других устройств IPv6 и отслеживания их досягаемости в сети. Устройство IPv6 использует следующие типы сообщений ICMPv6:

- Запрос доступных соседей (Neighbor solicitation): Запрос от хоста с целью узнать адрес канального уровня (MAC-адрес) соседнего устройства и определить, остается ли оно досягаемым. Соседнее устройство считается «досягаемым», если оно отвечает на сообщение типа «Запрос доступных соседей», поступившее от хоста, сообщением типа «Ответ соседа».
- Ответ соседа (Neighbor advertisement): Ответ от узла с целью анонса его адреса канального уровня.
- Запрос на доступность маршрутизаторов (Router solicitation): Запрос от хоста с целью поиска маршрутизатора, который может выступать в качестве маршрутизатора по умолчанию и пересылать пакеты.
- Ответ маршрутизатора (Router advertisement): Ответ на сообщение типа «Запрос на доступность маршрутизаторов» или периодический широковещательный анонс от маршрутизатора, информирующий о его присутствии и содержащий сведения о ряде его параметров.

Кэш IPv6

Хост IPv6 обязательно должен иметь кэш соседских узлов, кэш узлов назначения, список префиксов и список маршрутизаторов по умолчанию. Устройство NXC постоянно обслуживает и обновляет кэши IPv6 на основе информации, получаемой в сообщениях-ответах. В соответствии с протоколом IPv6 устройство NXC автоматически выполняет настройку адреса link-local, а затем отправляет сообщение типа «Запрос доступных соседей» для проверки уникальности адреса. При наличии адреса, который надо разрешить или верифицировать, устройство NXC также отправляет сообщение типа «Запрос доступных соседей». При получении сообщения типа «Ответ соседа» устройство NXC сохраняет адрес канального уровня соседнего устройства в кэше соседних узлов. При получении в ответ на сообщение типа «Запрос на доступность маршрутизаторов» сообщения типа «Ответ маршрутизатора» устройство NXC добавляет сведения о маршрутизаторе в кэш соседних узлов, список префиксов и кэш узлов назначения. Если данный маршрутизатор можно использовать в качестве маршрутизатора по умолчанию, то устройство NXC создает запись в списке маршрутизаторов по умолчанию.

Если устройству NXC необходимо отправить пакет, то оно вначале обращается к кэшу узлов назначения, чтобы определить следующий переход. Если соответствующей записи в кэше узлов назначения нет, устройство NXC с помощью списка префиксов определяет, доступен ли данный адрес назначения, и можно ли связаться с ним напрямую, в обход маршрутизатора. В случае доступности этот адрес выбирается в качестве следующего перехода. В противном случае устройство NXC выбирает следующий переход из списка маршрутизаторов по

умолчанию или из таблицы маршрутизации. Если IP-адрес следующего перехода известен, устройство NXC ищет в кэше соседних узлов соответствующий адрес канального уровня и отправляет пакет, когда соседний узел становится досягаемым. Если устройство NXC не может найти нужной записи в кэше соседних узлов, или соседний узел недоступен, то оно начинает процесс разрешения адреса. Это помогает уменьшить число IPv6-сообщений типа «Запрос...» и «Ответ...».

Протокол Multicast Listener Discovery

Протокол MLD (Multicast Listener Discovery, протокол обнаружения получателей запросов на многоадресную рассылку), описанный в RFC 2710, является производной от протокола IGMPv2 (IPv4's Internet Group Management Protocol version 2). MLD использует типы сообщений ICMPv6 вместо типов сообщений IGMP. MLDv1 является эквивалентом IGMPv2, а MLDv2 – эквивалентом IGMPv3.

MLD позволяет коммутатору или маршрутизатору IPv6 находить получателей запросов MLD, которые желают получить многоадресные пакеты, и IP-адреса групп многоадресной рассылки, к которым хотят присоединиться хосты в их сети.

Функции отслеживания и фильтрации многоадресного трафика и проксирования MLD аналогичны соответствующим функциям IGMP для протокола IPv4.

Фильтрация MLD контролирует перечень групп многоадресной рассылки, к которым может присоединиться порт.

Сообщения MLD

Маршрутизатор или коммутатор многоадресной рассылки периодически отправляет общие запросы хостам MLD для актуализации таблицы многоадресной рассылки. Если хост MLD хочет присоединиться к группе многоадресной рассылки, он отправляет сообщение MLD Report для данного адреса.

Сообщение MLD Done является эквивалентом сообщения IGMP Leave. Если хост MLD хочет выйти из группы многоадресной рассылки, он может отправить сообщение Done маршрутизатору или коммутатору. Затем маршрутизатор или коммутатор отправляет сообщение, адресованное определенной группе, на тот порт, на котором было получено сообщение Done, чтобы определить, должны ли другие устройства, подключенные к этому порту, оставаться в этой группе.

Пример – Включение поддержки протокола IPv6 в операционных системах Windows XP/2003/Vista

По умолчанию операционные системы Windows XP и Windows 2003 поддерживают протокол IPv6. Этот пример иллюстрирует процесс включения поддержки протокола IPv6 в операционных системах Windows XP/2003 с помощью команды `ipv6 install`. Кроме того,

здесь рассматривается применение команды `ipconfig` для просмотра автоматически сгенерированных IP-адресов.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . :255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . :10.1.1.254
```

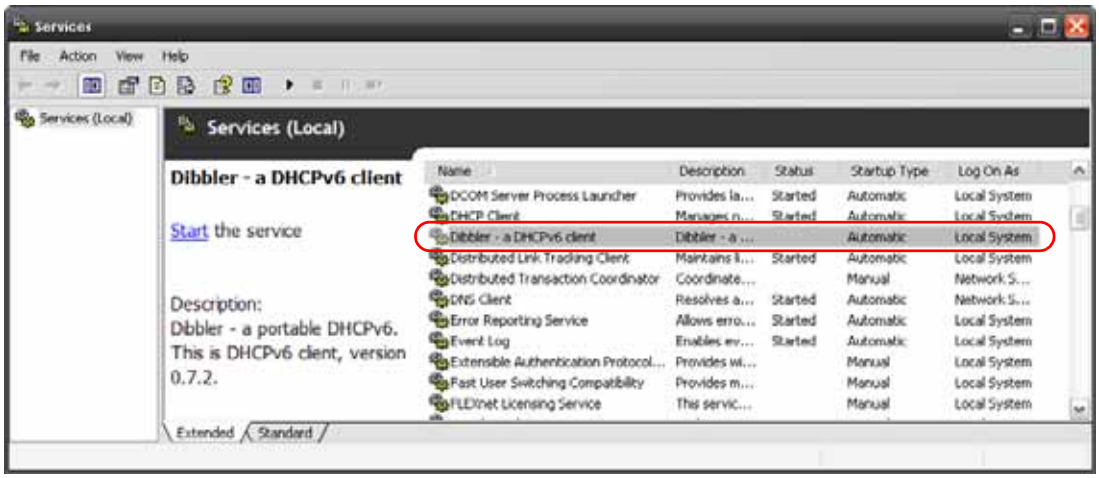
Протокол IPv6 установлен и включен по умолчанию в операционной системе Windows Vista. Воспользуйтесь командой `ipconfig` для просмотра автоматически назначенного адреса IPv6. Для данного интерфейса на компьютере должен отображаться как минимум один доступный адрес IPv6.

Пример – Включение поддержки DHCPv6 в операционной системе Windows XP

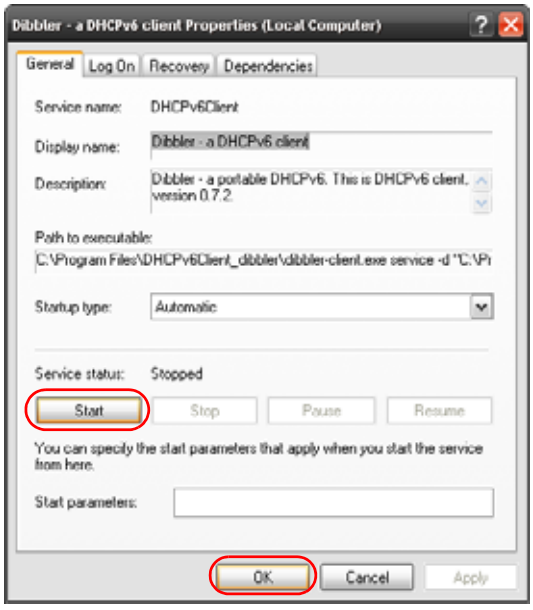
Windows XP не поддерживает DHCPv6. Если в сети для назначения IP-адресов используется протокол DHCPv6, необходимо установить клиентское программное обеспечение DHCPv6 в операционной системе Windows XP. (Примечание: Если для назначения адресов IPv6 в сети используются статические IP-адреса или анонсы маршрутизаторов (Router Advertisement), этот раздел можно пропустить).

В этом примере в качестве клиента DHCPv6 используется Dibbler. Чтобы включить клиент DHCPv6 на компьютере:

1. Установите на компьютер Dibbler и выберите опцию «клиент DHCPv6».
2. После завершения установки выберите в меню **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Выберите **Start** > **Control Panel** > **Administrative Tools** > **Services**.
4. Дважды щелкните мышью по строке **Dibbler – a DHCPv6 client**.



5 Нажмите кнопку **Start**, затем кнопку **OK**.



6 Теперь компьютер сможет получать адрес IPv6 от сервера DHCPv6.

Пример – Включение поддержки IPv6 в операционной системе Windows 7

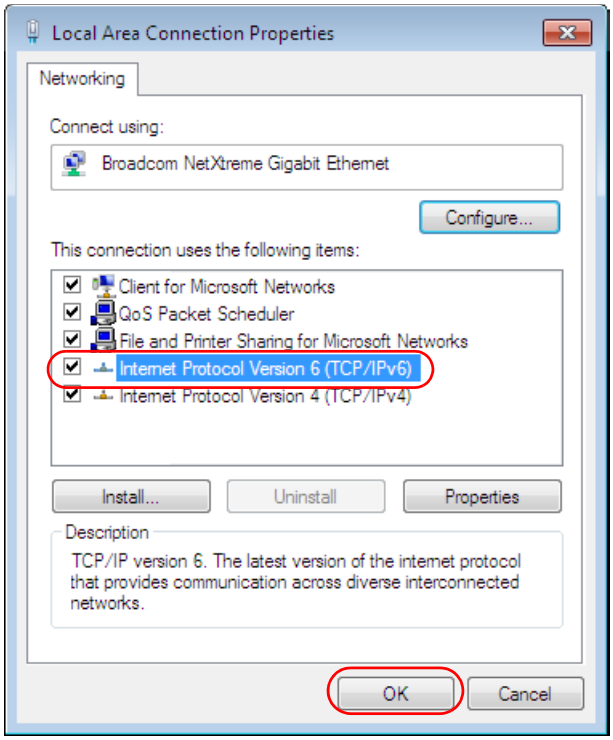
По умолчанию операционная система Windows 7 поддерживает IPv6. Включение поддержки IPv6 на компьютере, работающем под управлением Windows 7, автоматически включает поддержку DHCPv6.

Чтобы включить поддержку IPv6 в операционной системе Windows 7:

1 Выберите в меню **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Установите переключатель **Internet Protocol Version 6 (TCP/IPv6)**, чтобы включить поддержку протокола IPv6.

3 Нажмите кнопку **OK**, чтобы сохранить изменения.



4 Нажмите кнопку **Close**, чтобы закрыть экран **Local Area Connection Status**.

5 Выберите в меню **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Воспользуйтесь командой `ipconfig` для просмотра динамического адреса IPv6. В этом примере показан глобальный адрес (2001:b021:2d::1000), полученный от DHCP-сервера.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . :172.16.100.61
   Subnet Mask . . . . . . . . . . . :255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

F

Поддержка пользователей

В случаях, когда настоящего руководства оказывается недостаточно для решения проблем, следует обращаться к своему поставщику. При невозможности связаться со своим поставщиком обратитесь в представительство ZyXEL в регионе, где было приобретено устройство. Перечень региональных веб-сайтов приведен ниже (его также можно найти здесь http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml). При обращении в представительство ZyXEL может понадобиться следующая информация.

Требуемая информация

- Модель продукта и серийный номер.
- Информация о гарантии.
- Дата получения устройства.
- Краткое описание проблемы и шагов, которые были предприняты для ее решения.

Штаб-квартира компании (всемирная)

Тайвань

- ZyXEL Communications Corporation
- http://www.zyxel.com

Азия

Китай

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

Индия

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Казахстан

- ZyXEL Казахстан
- http://www.zyxel.kz

Корея

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Малайзия

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Пакистан

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Филиппины

- ZyXEL Philippines
- http://www.zyxel.com.ph

Сингапур

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Тайвань

- ZyXEL Communications Corporation
- http://www.zyxel.com

Таиланд

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Вьетнам

- ZyXEL Communications Corporation-Вьетнамское отделение
- http://www.zyxel.com/vn/vi

Европа

Австрия

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Беларусь

- ZyXEL BY
- http://www.zyxel.by

Бельгия

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/

Болгария

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Чехия

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Дания

- ZyXEL Communications A/S
- http://www.zyxel.dk

Эстония

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Финляндия

- ZyXEL Communications
- http://www.zyxel.fi

Франция

- ZyXEL Франция
- http://www.zyxel.fr

Германия

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Венгрия

- ZyXEL Венгрия, Восточная и Южная Европа
- http://www.zyxel.hu

Латвия

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Литва

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Нидерланды

- ZyXEL Benelux
- http://www.zyxel.nl

Норвегия

- ZyXEL Communications
- http://www.zyxel.no

Польша

- ZyXEL Communications Poland
- http://www.zyxel.pl

Румыния

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Россия

- ZyXEL Россия
- http://www.zyxel.ru

Словакия

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Испания

- ZyXEL Испания
- http://www.zyxel.es

Швеция

- ZyXEL Communications
- http://www.zyxel.se

Швейцария

- Studerus AG
- http://www.zyxel.ch/

Турция

- ZyXEL Turkey
- http://www.zyxel.com.tr

Великобритания

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Украина

- ZyXEL Украина
- http://www.ua.zyxel.com

Латинская Америка

Аргентина

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Эквадор

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Ближний Восток

Египет

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

Ближний Восток

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

Северная Америка

США

- ZyXEL Communications, Inc. – Штаб-квартира в Северной Америке
- http://www.us.zyxel.com/

Океания

Австралия

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Африка

ЮАР

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

G

Правовая информация

Уведомление об авторских правах

Уведомление

ZyXEL снимает с себя любую ответственность за последствия использования любых продуктов или программного обеспечения, описанных в настоящем документе. Кроме того, ZyXEL не передает никаких лицензий в отношении принадлежащих ZyXEL патентов или патентов третьих лиц. ZyXEL оставляет за собой право вносить изменения в описанные ниже продукты без какого-либо предварительного уведомления. Данная публикация может быть изменена без уведомления.

При использовании устройства NXC необходимо придерживаться условий и положений соответствующих провайдеров услуг.

Товарные знаки

ZyNOS (ZyXEL Network Operating System) является зарегистрированным товарным знаком ZyXEL Communications, Inc. Другие товарные знаки, упомянутые в данной публикации, используются только для идентификации и могут являться собственностью соответствующих правообладателей.

Сертификаты

Заявление о соответствии требованиям Федеральной комиссии связи США (FCC) в отношении помех

Данное устройство отвечает требованиям Части 15 правил FCC. При эксплуатации данного оборудования должны быть соблюдены два условия:

- Данное устройство не вызывает вредных помех.
- Данное устройство допускает работу в условиях любых помех, в том числе помех, которые могут вызвать нежелательные операции.

Данное устройство было испытано и признано отвечающим ограничениям для цифровых устройств Класса B в соответствии с Частью 15 правил FCC. Данные ограничения разработаны в целях обеспечения разумной степени защиты от вредных помех при эксплуатации оборудования в жилых помещениях. Данное устройство генерирует, использует и может излучать сигналы высокой частоты, в связи с чем при нарушении правил установки и эксплуатации, описанных в руководстве, оно может послужить причиной вредных помех для радиосвязи. Тем не менее, невозможно гарантировать отсутствие помех в конкретном помещении, где установлено устройство.

Если устройство действительно вызывает вредные помехи для теле/радиоприема, что можно установить включением и выключением устройства, пользователю рекомендуется попытаться устранить помехи одним или комбинацией из следующих способов:

1. Изменить ориентацию или расположение приемной антенны.
2. Увеличить расстояние между оборудованием и приемником.
3. Подключить оборудование к розетке, которая не относится к той же питающей цепи, что и розетка, к которой подключен приемник.
4. Обратиться за помощью к продавцу оборудования или специалисту по теле-/радиоприему.

Замечания

Изменения или модификации, внесенные без явно выраженного согласия стороны, ответственной за соблюдение требований, могут привести к аннулированию права пользователя на эксплуатацию данного оборудования.

Данное цифровое устройство Класса B соответствует требованиям Правил Канадского департамента связи для радиочастотных помех ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Просмотр сертификатов

Ознакомиться с документацией к продукту и имеющимися сертификатами можно по следующей ссылке: http://www.zyxel.com.

Ограниченная гарантия ZyXEL

Компания ZyXEL гарантирует конечному пользователю (покупателю) отсутствие любых дефектов, связанных с материалами или изготовлением данного продукта, в течение определенного срока (Гарантийного срока) с даты покупки. Гарантийный срок зависит от региона. Более подробную информацию о Гарантийном сроке для данного продукта можно получить у торгующей организации или местного авторизованного дистрибьютера ZyXEL. При обнаружении признаков неисправности продукта по причине некачественных материалов и/или качества изготовления в течение гарантийного срока, и при наличии подтверждения покупки, компания ZyXEL обязуется по своему усмотрению бесплатно отремонтировать или заменить неисправные продукты или

компоненты, насколько это необходимо, по мнению компании, для восстановления надлежащего рабочего состояния продукта или компонентов. Для замены будут использоваться новые или восстановленные функционально эквивалентные продукты аналогичной или более высокой стоимости, исключительно по усмотрению компании ZyXEL. Данная гарантия не имеет силы, если продукт был подвергнут изменениям или несанкционированному вмешательству, эксплуатировался с нарушением правил, был поврежден в результате форс-мажорных обстоятельств или в связи с нарушением условий эксплуатации.

Примечание

Ремонт или замена, предусмотренные данной гарантией, являются исключительным средством правовой защиты покупателя. Данная гарантия заменяет собой все прочие явно выраженные или подразумеваемые гарантии, включая подразумеваемые гарантии товарных качеств или пригодности для конкретной цели. Ни при каких обстоятельствах компания ZyXEL не несет ответственности за какой бы то ни было косвенный или побочный ущерб любого характера, причиненный покупателю.

Для получения гарантийного обслуживания необходимо обращаться к торгующей организации. Правила гарантийного обслуживания для региона, в котором было приобретено устройство, можно уточнить на сайте http://www.zyxel.com/web/support_warranty_info.php.

Регистрация

Чтобы получать по электронной почте уведомления об обновлениях встроенного программного обеспечения и дополнительную информацию, зарегистрируйте продукт в режиме онлайн на сайте www.zyxel.com (для поставляемых в различные страны мира продуктов) или на сайте www.us.zyxel.com (для продуктов, предназначенных для североамериканского рынка).

Лицензии на открытое программное обеспечение

Данное изделие включает в себя некоторые компоненты открытого программного обеспечения, распространяемого по лицензии GPL и/или аналогичным GPL лицензиям. Лицензии на открытое программное обеспечение предоставляются в составе пакета встроенного программного обеспечения. Самые свежие версии встроенного программного обеспечения доступны на сайте www.zyxel.com. Если не удалось нужное программное обеспечение на этом сайте, свяжитесь со своим поставщиком или обратитесь в Службу технической поддержки ZyXEL по адресу support@zyxel.com.tw.

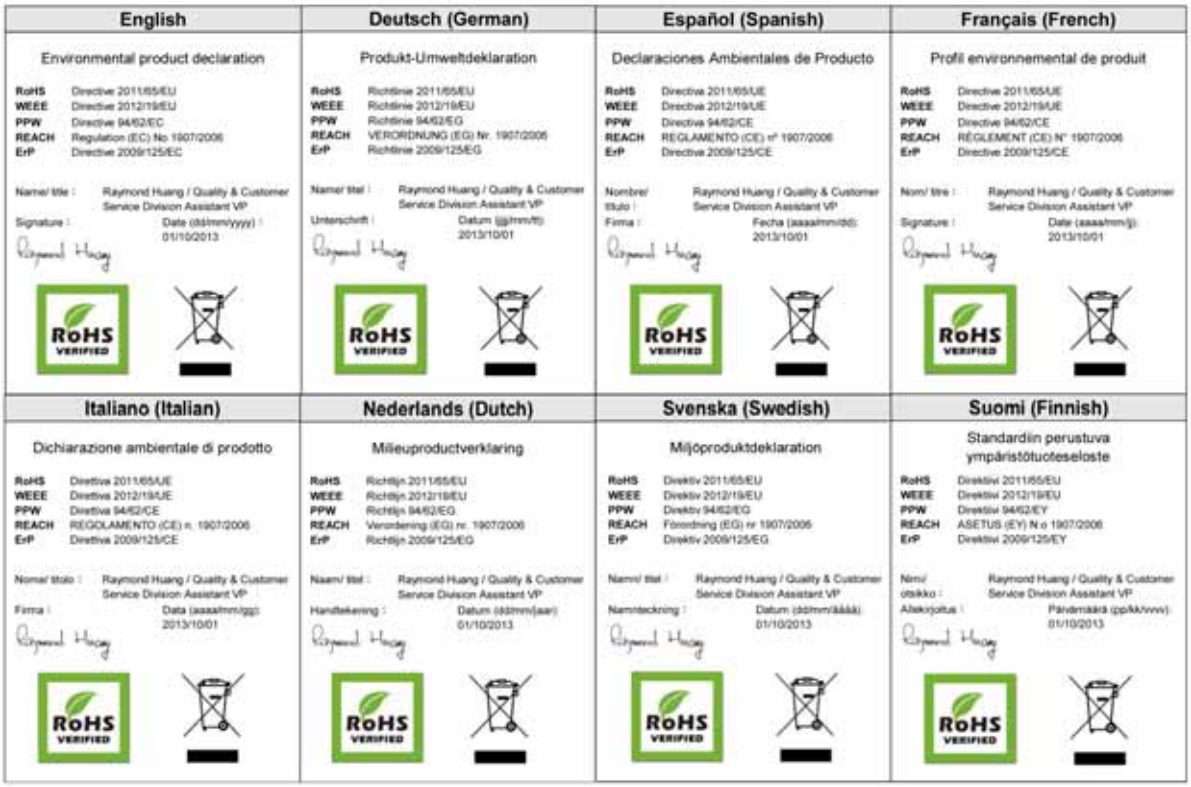
Для получения исходных текстов, на которые распространяются указанные лицензии, свяжитесь со своим поставщиком или обратитесь в Службу технической поддержки ZyXEL по адресу support@zyxel.com.tw.

Предупреждения по безопасности

- НЕ используйте данный продукт вблизи воды, например, в сыром подвале или неподалеку от плавательного бассейна.
- НЕ подвергайте устройство воздействию сырости, пыли или агрессивных жидкостей.
- НЕ кладите ничего поверх устройства.
- НЕ занимайтесь установкой, обслуживанием и не эксплуатируйте устройство во время грозы. Существует опасность поражения электрическим током в результате удара молнии.
- К устройству разрешается подключать ТОЛЬКО подходящие дополнительные модули.
- НЕ открывайте устройство. В результате вскрытия или снятия защитных кожухов вы подвергаете себя опасности прикосновения к оголенным токоведущим участкам с опасным высоким напряжением и иным рискам. Обслуживать или разбирать данное устройство разрешается ТОЛЬКО квалифицированному сервисному персоналу. Для получения дополнительной информации свяжитесь с поставщиком.
- Убедитесь, что кабели подключены к нужным портам.
- Аккуратно расположите соединительные кабели так, чтобы никто не мог наступить или споткнуться о них.
- Перед обслуживанием или разборкой обязательно отсоедините все кабели от устройства.
- Используйте с устройством ТОЛЬКО подходящий адаптер питания или шнур питания. Подключайте его к источнику питания с требуемым номиналом напряжения (например, 110 В перем. тока в Северной Америке или 230 В перем. тока в Европе).
- НЕ кладите ничего на адаптер питания или шнур питания и НЕ располагайте продукт в таком месте, где кто-нибудь может наступить на адаптер питания или шнур питания.
- НЕ используйте устройство, если адаптер питания или шнур повреждены, так как в этом случае существует опасность поражения электрическим током.
- Если адаптер питания или шнур питания повреждены, отсоедините их от устройства и от сети питания.
- НЕ пытайтесь отремонтировать адаптер питания или шнур питания. Обратитесь к местному поставщику и закажите новый.
- Не используйте устройство вне помещений; все соединения также должны проходить внутри помещений. Существует опасность поражения электрическим током в результате удара молнии.
- Устройства, поддерживающие подачу или получение питания по витой паре (PoE), а также подключенные к ним кабели Ethernet должны располагаться целиком внутри помещений.
- Это изделие предназначено для использования только внутри помещений (utilisation intérieure exclusivement).

Изделие промаркировано показанным символом, известным также как маркировка WEEE. WEEE является сокращением от Waste Electronics and Electrical Equipment (отходы электрического и электронного оборудования). Это означает, что отслужившее свой срок электрическое и электронное оборудование не должно утилизироваться вместе с обычными бытовыми отходами. Отслужившее свой срок электрическое и электронное оборудование должно утилизироваться отдельно.

Экологическая декларация для изделия



English

Environmental product declaration

RoHS	Directive 2011/65/EU
WEEE	Directive 2012/19/EU
PPW	Directive 94/62/EC
REACH	Regulation (EC) No 1907/2006
ErP	Directive 2009/125/EC

Name/ title : Raymond Huang / Quality & Customer Service Division Assistant VP

Signature : Date (dd/mm/yyyy) : 01/10/2013

Deutsch (German)

Produkt-Umweltdeklaration

RoHS	Richtlinie 2011/65/EU
WEEE	Richtlinie 2012/19/EU
PPW	Richtlinie 94/62/EG
REACH	VERORDNUNG (EG) Nr. 1907/2006
ErP	Richtlinie 2009/125/EG

Name/ titel : Raymond Huang / Quality & Customer Service Division Assistant VP

Unterschrift : Datum (tt/mm/jj): 2013/10/01

Español (Spanish)

Declaraciones Ambientales de Producto

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	REGLAMENTO (CE) nº 1907/2006
ErP	Directiva 2009/125/CE

Nombre/ título : Raymond Huang / Quality & Customer Service Division Assistant VP

Firma : Fecha (aaaa/mm/dd): 2013/10/01

Français (French)

Profil environnemental de produit

RoHS	Directive 2011/65/UE
WEEE	Directive 2012/19/UE
PPW	Directive 94/62/CE
REACH	RÈGLEMENT (CE) N° 1907/2006
ErP	Directive 2009/125/CE

Nom/ titre : Raymond Huang / Quality & Customer Service Division Assistant VP

Signature : Date (aaaa/mm/jj): 2013/10/01

Italiano (Italian)

Dichiarazione ambientale di prodotto

RoHS	Direttiva 2011/65/UE
WEEE	Direttiva 2012/19/UE
PPW	Direttiva 94/62/CE
REACH	REGOLAMENTO (CE) n. 1907/2006
ErP	Direttiva 2009/125/CE

Nome/ titolo : Raymond Huang / Quality & Customer Service Division Assistant VP

Firma : Data (aaaa/mm/gg): 2013/10/01

Nederlands (Dutch)

Milieuproductverklaring

RoHS	Richtlijn 2011/65/EU
WEEE	Richtlijn 2012/19/EU
PPW	Richtlijn 94/62/EG
REACH	Verordening (EG) nr. 1907/2006
ErP	Richtlijn 2009/125/EG

Naam/ titel : Raymond Huang / Quality & Customer Service Division Assistant VP

Handtekening : Datum (dd/mm/jaar) 01/10/2013

Svenska (Swedish)

Miljöproduktdeklaration

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EG
REACH	Förordning (EG) nr 1907/2006
ErP	Direktiv 2009/125/EG

Namn/ titel : Raymond Huang / Quality & Customer Service Division Assistant VP

Namnteckning : Datum (dd/mm/åååå) 01/10/2013

Suomi (Finnish)

Standardiin perustuva ympäristötuoteseloste

RoHS	Direktiivi 2011/65/EU
WEEE	Direktiivi 2012/19/EU
PPW	Direktiivi 94/62/EY
REACH	ASETUS (EY) N:o 1907/2006
ErP	Direktiivi 2009/125/EY

Nimi/ otsikko : Raymond Huang / Quality & Customer Service Division Assistant VP

Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2013

Указатель

G

H

I

L

M

N

O

P

Q

R

S (C)

T

U

V

W

Z