

ZyXEL NDMS v2.00 Command Line Interface Guide

Draft 1.0

Введение	4
Вход в систему	4
Ввод команд	4
Вход в группу	4
Автодополнение и подсказка	5
Префикс po	6
Влияние команд на настройки	6
Команды с многократным вводом	7
Сохранение настроек	7
Отложенная перезагрузка	7
Системные команды общего назначения	7
system	7
system reboot	8
system set	8
system hostname	9
copy	9
more	10
show running-config	10
Базовые настройки IP	10
Сетевые интерфейсы	10
Классы интерфейсов	10
Статические и динамические сетевые интерфейсы	11
Базовые функции интерфейса	11
Функции MAC	11
Функции IP	11
Функции Ethernet	11
Описание команд	12
interface	12
interface description	13
interface up	13
interface down	13
interface mac address	13
interface ip address	14
interface ip alias	14
interface ip dhcp	15
interface ip mtu	15
interface ip tcp adjust-mss	15
ip route	16
global	16
Firewall и NAT	17
Описание команд	17
ip nat	17
ip static	17
interface security-level	18
access-list	18
access-list deny	19
access-list permit	20
interface ip access-group	20
Switch и VLAN	21
Интерфейс Switch	21
Интерфейс VLAN	21
Пример	21
Описание команд	22
interface port	22
interface port mode	22
interface port mode access	23
interface port mode trunk	23

interface port access.....	23
interface port trunk	24
Мосты	24
Интерфейс Bridge	24
Пример	25
Описание команд	25
interface include	25
interface inherit	26
PPP	26
Функции PPP	26
Функции Secure	26
Интерфейс PPPoE.....	26
Интерфейс PPTP	26
Интерфейс L2TP.....	27
Порядок настройки	27
Дополнительные параметры	28
LCP Echo.....	28
IPCP	28
Описание команд	28
interface peer.....	28
interface discovery	28
interface authentication pap	29
interface authentication chap	29
interface authentication mschap.....	29
interface authentication mschap-v2.....	30
interface authentication identity.....	30
interface authentication password.....	30
interface encryption mppe.....	31
interface lcp echo	31
interface ipcp default-route	31
interface ipcp name-servers	32
interface ip mru.....	32
interface connect	32
Модемы 3G.....	33
Базовые функции сетевых интерфейсов USB.....	33
Идентификаторы производителя и модели	33
Описание	33
USB-модемы	34
Описание команд	34
interface usb device-id.....	34
interface modem init	35
interface modem connect.....	35
interface modem pin-code.....	36
interface ip apn.....	36
Беспроводная сеть 802.11.....	36
Точки Доступа.....	36
Беспроводные станции.....	37
Команды настройки сети.....	37
interface ssid.....	37
interface channel	37
interface compatibility.....	38
interface power.....	38
Команды настройки безопасности.....	38
interface authentication wpa-psk.....	38
interface authentication shared.....	39
interface encryption enable	39
interface encryption key.....	39
interface encryption wpa.....	40
interface encryption wpa2.....	40
Настройка DNS	41
Описание команд	41

ip name-server.....	41
service dns-proxy	41
Сервер DHCP	42
Описание команд	42
ip dhcp pool.....	42
Аргументы	42
ip dhcp pool range	42
ip dhcp pool default-router	43
ip dhcp pool dns-server.....	43
ip dhcp pool lease	44
ip dhcp host.....	44
service dhcp.....	44
Управление доступом к устройству	45
Описание команд	45
service http.....	45
service ftp	45
service telnet.....	45
user password.....	46
Диагностика.....	46
Описание команд	46
show version.....	46
show interface.....	46
show ip route.....	47
show ip arp	47
show ip name-server	48
show log	48
tools ping	49
Примеры настроек	49
Тестирование пропускной способности	49
Маршрутизация с включенной трансляцией адресов.....	50
DHCP-сервер и DHCP-клиент.....	51
Беспроводная точка доступа и станция в режиме моста	52
Подключение к провайдеру по PPPoE.....	53
Подключение к провайдеру по PPTP.....	54
Подключение к провайдеру по L2TP	55
Несколько беспроводных сетей и VLAN с тегом	56

Введение

В NDMS-микропрограммах v2.00 (второго поколения) для интернет-центров Keenetic вводится новое мощное средство управления — это интерфейс командной строки (Command Line Interface, CLI). Настройки системы полностью описываются в виде последовательности команд, которые нужно выполнить, чтобы привести устройство в заданное состояние.

В NDMS v2.00 существует три вида настроек:

Текущие настройки (running config) — это набор команд, которые требуется выполнить, чтобы привести систему в текущее состояние. Текущие настройки хранятся в оперативной памяти (RAM) и отражают все изменения настроек системы. Однако, содержимое оперативной памяти теряется при выключении устройства. Для того чтобы настройки восстановились при перезагрузке устройства, требуется сохранить их в энергонезависимой памяти.

Стартовые настройки (startup config) — это последовательность команд, которая хранится в специальном секторе энергонезависимой памяти и используется для инициализации системы непосредственно после загрузки.

Настройки по умолчанию (default config) — это заводские настройки, которые записываются на устройство при производстве. Кнопка **RESET** на корпусе позволяет сбросить стартовые настройки на заводские.

Вход в систему

При подключении к маршрутизатору NDMS v2.00 через telnet пользователю предлагается ввести пароль администратора. В настройках по умолчанию пароль установлен в значение **1234**.

```
$ telnet 172.16.1.1
Trying 172.16.1.1...
Connected to 172.16.1.1.
Escape character is '^]'.

Password: ****
(config)>
```

Ввод команд

Командный интерпретатор NDMS v2.00 разработан таким образом, чтобы им мог пользоваться как начинающий, так и опытный оператор. Все команды и параметры имеют ясные и легко запоминающиеся названия.

Команды разбиты на группы и выстроены в иерархию. Таким образом, для выполнения какой-либо настройки оператору потребуется последовательно ввести названия вложенных групп команд (*узловых* команд), и затем конечную команду с параметрами.

Например, IP-адрес сетевого интерфейса *Switch0/VLAN2* задается командой *address*, которая находится в группе *interface* → *ip*:

```
(config)> interface Switch0/VLAN2 ip address 192.168.15.43/24
Network address saved.
```

Вход в группу

Некоторые узловые команды, содержащие группу дочерних команд, позволяют оператору выполнить «вход» в группу, чтобы вводить дочерние команды непосредственно, не тратя время на ввод имени узловой команды. В этом случае меняется текст приглашения командной строки, чтобы оператор видел, в какой группе он находится.

Выход из группы выполняется по команде *exit*, ! или по нажатию комбинации клавиш <Ctrl-D>.

Например, при входе в группу *interface* приглашение командной строки меняется на *(config-if)*:

```
(config)> interface Switch0/VLAN2
(config-if)> ip address 192.168.15.43/24
Network address saved.
```

```
(config-if)> <Ctrl-D>
(config)>
```

Автодополнение и подсказка

Для того чтобы сделать процесс настройки максимально удобным, интерфейс командной строки имеет функцию автодополнения команд и параметров, подсказывая оператору, какие команды доступны на текущем уровне вложенности. Автодополнение работает по клавише <Tab>. Например:

```
(config)> in<Tab>

interface - network interface configuration
(config)> interface Sw<Tab>

Usage template:
interface {name}

Variants:
Switch0
Switch0/VLAN1
Switch0/VLAN2
(config)> interface Switch0<Tab>

Usage template:
interface {name}

Variants:
Switch0/VLAN1
Switch0/VLAN2
(config)> interface Switch0/VLAN2<Enter>
(config-if)> ip<Tab>

address - set interface IP address
alias - add interface IP alias
dhcp - enable dhcp client
mtu - set Maximum Transmit Unit size
mru - set Maximum Receive Unit size
access-group - bind access-control rules
apn - set 3G access point name
(config-if)> ip ad<Tab>

address - set interface IP address
(config-if)> ip address<Tab>

Usage template:
address {address} {mask}

(config-if)> ip address 192.168.15.43<Enter>
Configurator error[852002]: address: argument parse error.
(config-if)> ip address 192.168.15.43/24<Enter>
Network address saved.
(config-if)>
```

Подсказку по текущей команде всегда можно высветить, нажав клавишу <?>. Например:

```
(config)> interface Switch0/VLAN2 <?>

description - set interface description
alias - add interface name alias
discovery - set ethernet interface for PPPoE discovery
peer - specify remote peer identifier
```

```
service - specify PPPoE access service
mac-address - set interface MAC address
dyndns - DynDns updates
port - configure switch port
inherit - add Ethernet interface to a Bridge (with inheritance)
include - add Ethernet interface to a Bridge
usb - configure interface USB parameters
modem - Set modem parameters
lcp - set interface LCP parameters
ipcp - set interface IPCP parameters
security-level - assign security level
wps - enable WPS functionality
authentication - configure authentication
encryption - configure encryption parameters
ip - set interface IP parameters
igmp - set interface IGMP parameters
ssid - set wireless ESSID
channel - set radio channel
country-code - set country code
compatibility - set 802.11 compatibility (use parameters like BG or ABGN)
power - set transmission power level
connect - enable PPP connection
up - enable interface
down - disable interface

(config)> interface Switch0/VLAN2
```

Префикс no

Префикс `no` используется для отмены действия команды, перед которой он ставится.

Например, команда `interface` отвечает за создание сетевого интерфейса с заданным именем. Префикс `no`, используемый с этой командой, вызывает обратное действие — удаление интерфейса:

```
(config)> no interface PPPoE0
```

Если команда составная, `no` может ставиться перед любым ее членом. Например, `service dhcp` включает службу DHCP и состоит из двух частей: `service` — имени группы в иерархии команд, и `dhcp` — конечной команды. Префикс `no` можно ставить как в начале, так и в середине. Действие в обоих случаях будет одинаковым: остановка службы.

```
(config)> no service dhcp
(config)> service no dhcp
```

Влияние команд на настройки

Большая часть команд при вводе меняет состояние системы и записывает эти изменения в текущие настройки, которые можно отобразить с помощью команды `show running-config`. Например, при вводе команды `service http` запускается служба управления устройством через HTTP и в настройках появляется запись «`service http`»:

```
(config)> service http
HTTP server enabled.
(config)> show running-config
...
service http
```

При вводе команды с префиксом `no` строка «`service http`» удаляется из `running-config`. Поскольку по умолчанию служба HTTP не работает, такое поведение позволяет восстановить состояние службы при следующем старте системы, если текущие настройки сохранить в `startup-config`.

Практически все команды вносятся в настройки по принципу «есть команда — есть функция», так чтобы оператор при взгляде на `running-config` видел, что в системе включено.

Команды с многократным вводом

Многие команды обладают свойством *идемпотентности*, которое проявляется в том, что многократный ввод этих команд приводит к тем же изменениям, что и однократный. Например, команда `service http` добавляет строку «`service http`» в текущие настройки, и при повторном вводе ничего не меняет.

Однако, часть команд позволяет добавлять не одну, а несколько записей, если вводить их с разными аргументами. Например, статические записи в таблице маршрутизации `ip route` или фильтры `access-list` добавляются последовательно, и затем присутствуют в настройках в виде списка:

```
(config)> ip route 1.1.1.0/24 PTPR0
Route added.
(config)> ip route 1.1.2.0/24 PTPR0
Route added.
(config)> ip route 1.1.3.0/24 PTPR1
Route added.
(config)> show running-config
...
ip route 1.1.1.0 255.255.255.0 PTPR0
ip route 1.1.2.0 255.255.255.0 PTPR0
ip route 1.1.3.0 255.255.255.0 PTPR0
...
```

Записи из таких таблиц можно удалять по одной, используя префикс `no`, и указывая в аргументе команды, какую именно запись требуется удалить:

```
(config)> no ip route 1.1.2.0/24
Route deleted.
(config)> show running-config
...
ip route 1.1.1.0 255.255.255.0 PTPR0
ip route 1.1.3.0 255.255.255.0 PTPR0
...
```

Сохранение настроек

Текущие и стартовые настройки хранятся в файлах `running-config` и `startup-config`. Для того чтобы сохранить текущие настройки в энергонезависимую память, нужно ввести команду копирования:

```
(config)> copy running-config startup-config
Copied: running-config -> startup-config
```

Отложенная перезагрузка

Если устройство находится на значительном удалении от оператора и управляется по сети, возникает опасность потерять связь с ним по причине ошибочных действий оператора. В этом случае перезагрузка и возврат к сохраненным настройкам будет затруднена.

Команда `system reboot` позволяет установить таймер отложенной перезагрузки, выполнить «опасные» настройки, затем выключить таймер и сохранить изменения. Если в процессе настройки связь с устройством будет потеряна, оператору достаточно будет дождаться автоматической перезагрузки и подключиться к устройству снова.

Системные команды общего назначения

`system`

Вход в группу системных функций, в том числе команд для настройки глобальных параметров.

Свойства

Идентификатор	1
Префикс <code>no</code>	нет
Меняет настройки	нет
Многократный ввод	нет
Вход в группу	(<code>system</code>)

Команды

		Описание
1	<code>reboot</code>	Перезагрузка системы
2	<code>set</code>	Установка системных параметров
4	<code>hostname</code>	Установка имени хоста системы

`system reboot`

Выполняет перезагрузку системы. Если указан параметр, перезагрузка выполнится запланированно через заданный интервал в секундах. Префикс `no` отменяет запланированную перезагрузку. Использование команды при уже установленном таймере заменяет старое значение таймера новым.

Использование запланированной перезагрузки удобно в том случае, когда осуществляется удаленное управление устройством, и пользователю неизвестен эффект от применения каких-либо команд. Из опасения потерять контроль над устройством пользователь может включить запланированную перезагрузку, которая сработает через заданный интервал времени и вернет систему в первоначальное состояние, в котором она снова будет доступна по сети.

Свойства

Идентификатор	1.1
Префикс <code>no</code>	да
Меняет настройки	нет
Многократный ввод	нет

Аргументы

```
(system)>      reboot <interval>
(system)> no    reboot
```

	Тип	Описание
<code>interval</code>	Целое число	Интервал, через который выполнится запланированная перезагрузка

`system set`

Устанавливает значение указанного системного параметра и сохраняет изменения в текущих настройках. При использовании с префиксом `no` возвращает параметру значение, которое было установлено по умолчанию, до первого изменения.

Например:

```
(config)> system
(system)> set net.ipv4.ip_forward 1
(system)> set net.ipv4.tcp_fin_timeout 30
(system)> set net.ipv4.tcp_keepalive_time 120
(system)> set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
(system)> set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
(system)> set net.ipv4.netfilter.ip_conntrack_max 4096
(system)> exit
(config)> show running-config
system
set net.ipv4.ip_forward 1
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.netfilter.ip_conntrack_max 4096
!
...
(config)>
```

Свойства

Идентификатор	1.2
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	да

Аргументы

```
(system)>      set <name> <value>
(system)> no    set <name>
```

	Тип	Описание
<code>name</code>	Строка	Имя системного параметра
<code>value</code>	Строка	Значение системного параметра

`system hostname`

Команда задает имя хоста. Префикс `no` устанавливает пустое имя.

Свойства

Идентификатор	1.4
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	нет

Аргументы

```
(system)>      hostname <hostname>
(system)> no    hostname
```

	Тип	Описание
<code>hostname</code>	Строка	Имя хоста системы

`copy`

Копирует содержимое одного файла в другой. Используется для обновления микропрограммы, сохранения текущих настроек, сброса на заводские настройки и т. п.

Например, сохранение настроек делается так:

```
(config)> copy running-config startup-config
```

Названия файлов в примере — псевдонимы. Полные имена файлов настроек, соответственно, `system:running-config` и `flash:startup-config`.

Свойства

Идентификатор	502
Префикс <code>no</code>	нет
Меняет настройки	нет

Аргументы

```
(config)> copy <source> <destination>
```

	Тип	Описание
<code>source</code>	Имя файла	Откуда копировать
<code>destination</code>	Имя файла	Куда копировать

more

Выводит содержимое текстового файла построчно.

Свойства

Идентификатор	500
Префикс no	нет
Меняет настройки	нет

Аргументы

```
(config)> more <filename>
```

	Тип	Описание
filename	Имя файла	Полное имя файла или псевдоним

show running-config

Отображает текущие настройки, а именно содержимое файла `system:running-config` — точно так же, как это делает команда `more`.

Свойства

Идентификатор	600.60
Префикс no	нет
Меняет настройки	нет

Базовые настройки IP

Сетевые интерфейсы

Под *сетевым интерфейсом* в NDMS v2.00 понимается физический или виртуальный сетевой интерфейс — абстракция, описывающая соединение устройства с локальной сетью. Физический интерфейс соответствует сетевому адаптеру с физическим (проводным или беспроводным) подключением. Виртуальный интерфейс соответствует виртуальной сети, например VLAN IEEE 802.1Q или Multiple ESSID в беспроводной сети IEEE 802.11.

В общем случае, сетевых интерфейсов на устройстве несколько, что позволяет ему передавать пакеты из одной локальной сети в другую в режиме маршрутизатора или моста.

Каждый интерфейс имеет определенный тип, например, `FastEthernet` или `PPTP`. Интерфейсы каждого типа пронумерованы. Кроме того, между интерфейсами существуют отношения *вложенности*, когда *вложенный* интерфейс имеет смысл только при наличии другого, *родительского*. Таким образом, в NDMS v2.00 каждый сетевой интерфейс имеет уникальное имя, которое состоит из имени родительского интерфейса, типа и индекса, например:

FastEthernet0/VLAN100

Здесь `FastEthernet0` — родительский интерфейс, `VLAN` — тип, а `100` — индекс, уникальный в пределах родительского интерфейса.

Классы интерфейсов

Каждый сетевой интерфейс обладает некоторым набором функций и позволяет оператору менять настройки, соответствующие назначению интерфейса. Настройки подразделяются на группы. Можно выделить базовые настройки, настройки IP, PPP и т. д.

Если интерфейс поддерживает настройки определенной группы, то говорят, что интерфейс относится к *классу* интерфейсов с такими настройками. Например, интерфейсы `FastEthernet`, `PPTP`, `Bridge` и `VLAN` несмотря на существенные различия позволяют настроить IP-адрес, поэтому они относятся к одному базовому классу — IP.

Интерфейс может одновременно относиться к нескольким классам. В этом случае говорят, что интерфейс *агрегирует* функции нескольких классов.

Статические и динамические сетевые интерфейсы

Статические интерфейсы соответствуют аппаратной конфигурации устройства. Они определяются при старте системы, и существуют все время ее работы. Интерфейсы такого типа не могут быть созданы или удалены в процессе работы системы.

Динамические интерфейсы обычно соответствуют виртуальным сетевым подключениям. Они могут быть созданы или удалены в процессе работы системы. Динамическая конфигурация интерфейсов отображается в текущих настройках и может быть сохранена в энергонезависимой памяти. К динамическим относятся интерфейсы следующих классов: VLAN, PPP, USB, Bridge.

Базовые функции интерфейса

Базовые функции применимы ко всем интерфейсам. К ним относятся:

- включение/выключение интерфейса командами `interface up` и `interface down`;
- назначение произвольной строки описания командой `interface description`.

Функции MAC

Интерфейсы класса MAC могут работать в сетях с адресацией IEEE EUI-48. Функции MAC поддерживаются интерфейсами класса Ethernet, куда относится VLAN, SSID, Bridge и WiMAX. Интерфейсы класса MAC обладают MAC-адресом по умолчанию и позволяют задать его вручную командой `interface mac-address`.

Функции IP

На интерфейсах с поддержкой протокола IP можно настроить IP-адрес и подключить их к различным IP-подсетям. Такие сети называются *подключенными напрямую (непосредственно)* и автоматически добавляются в таблицу маршрутизации.

Таблица маршрутизации IP состоит из маршрутов. Каждый маршрут имеет сеть назначения, заданную IP-адресом и маской. В маршруте указан идентификатор интерфейса, через который можно попасть в сеть назначения. Если интерфейс подключен к сети с множественным доступом, то кроме идентификатора интерфейса в маршруте указывается транзитный IP-адрес соседнего транзитного узла, или *маршрутизатора*.

На основе сетевой информации, которая содержится в таблице маршрутизации IP, к узлу любой уникально идентифицируемой сети IP, не подключенной напрямую к одному из интерфейсов, можно добраться, направив пакет к следующему транзитному узлу сети, подключенной напрямую.

В таблице маршрутизации может быть один *маршрут по умолчанию* с адресом назначения `0.0.0.0/0`, по которому направляются все пакеты, для которых не нашлось более подходящего специального маршрута.

Записи в таблицу маршрутизации добавляются тремя способами:

- *Автоматически*, при настройке IP-адреса на интерфейсе вручную командой `interface ip address` или службой отвечающей за подключение по протоколу DHCP или PPP. Автоматические маршруты указывают на сети, подключенные напрямую.
- *Статически*, командой `ip route`. Статические маршруты отображаются в текущих настройках и присутствуют в системе в течение времени жизни сетевого интерфейса, через который они работают.
- *Динамически* службой, отвечающей за подключение по протоколу DHCP или PPP. Динамические маршруты обычно передаются провайдером вместе с настройками IP-адреса.

Функции Ethernet

Интерфейсы Ethernet представляют собой класс интерфейсов, агрегирующий базовые классы IP и MAC. Интерфейсы Ethernet обладают рядом специальных свойств, которые будут рассмотрены в последующих разделах, а именно:

- запуск DHCP-клиента;
- создание дочерних интерфейсов VLAN;
- включение в мосты в качестве портов;
- поддержка PPPoE.

Описание команд

interface

Вход в группу команд для настройки выбранного интерфейса. Если интерфейс не найден, команда пытается его создать. Префикс `no` удаляет интерфейс.

Каждая из команд данной группы применима к определенному типу интерфейса иерархии. Базовый тип интерфейса, к которому применима команда, указан в колонке «Тип интерфейса» таблицы команд ниже.

Свойства

Идентификатор	10
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	(<code>config-if</code>)

Аргументы

```
(config)>      interface <name>
(config)> no    interface <name>
```

	Тип	Описание
<code>name</code>	Строка	Полное имя интерфейса или псевдоним

Команды

		Тип интерфейса	Описание
1	<code>description</code>	Base	Описание интерфейса
2	<code>alias</code>	Base	Настройка псевдонимов
3	<code>discovery</code>	PPPoE	Привязка PPPoE к Ethernet-интерфейсу
4	<code>peer</code>	PPP	Идентификатор удаленного узла PPP
5	<code>service</code>	PPPoE	Идентификатор удаленного сервиса PPPoE
6	<code>mac</code>	MAC	Настройка MAC-адреса
8	<code>dyndns</code>	IP	Назначить профиль DynDns, ручное обновление dyndns
10	<code>port</code>	Switch	Настройка порта коммутатора
11	<code>inherit</code>	Bridge	Добавление интерфейса в мост с передачей настроек
12	<code>include</code>	Bridge	Добавление интерфейса в мост
30	<code>usb</code>	USB	Настройки USB
34	<code>modem</code>	USB Modem	Настройки модема, подключенного по асинхронному последовательному порту
40	<code>lcp</code>	PPP	Настройки параметров LCP
41	<code>ipcp</code>	PPP	Настройки параметров IPCP
50	<code>security-level</code>	IP	Настройка security level
97	<code>wps</code>	SSID	Управление WPS (Wi-Fi protected setup)
98	<code>authentication</code>	Secure/SSID	Настройка аутентификации
99	<code>encryption</code>	Secure/SSID	Настройка шифрования
100	<code>ip</code>	IP	Настройка параметров IP
103	<code>igmp</code>	IP	Настройка параметров IGMP
200	<code>ssid</code>	SSID	Настройка SSID
201	<code>channel</code>	Radio	Выбор канала Wifi
202	<code>country-code</code>	Radio	Установка кода региона Wifi
203	<code>compatibility</code>	Radio	Установка режима совместимости Wifi (A/B/G/N)

205	power	Radio	Установка мощности передатчика Wifi
499	connect	PPP	Подключение к удаленной точке
500	up	Base	Включение интерфейса
501	down	Base	Выключение интерфейса

interface description

Устанавливает произвольное описание сетевого интерфейса. Префикс `no` стирает описание.

Свойства

Идентификатор	10.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

Аргументы

```
(config-if)> description <description>
(config-if)> no description
```

	Тип	Описание
<code>description</code>	Строка	Произвольное описание интерфейса

interface up

Включает сетевой интерфейс и записывает в настройки состояние "`up`". Префикс `no` выключает сетевой интерфейс и удаляет "`up`" из настроек.

Свойства

Идентификатор	10.500
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

interface down

Выключает сетевой интерфейс и записывает в настройки состояние "`down`". Префикс `no` выключает сетевой интерфейс и удаляет "`down`" из настроек.

Свойства

Идентификатор	10.501
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

interface mac address

Устанавливает MAC-адрес на указанный сетевой интерфейс. Адрес задается в шестнадцатеричном формате, поддерживаются две формы записи: вида `0000.0000.0000` и `00:00:00:00:00:00`. Команда позволяет установить любой адрес, но предупреждает пользователя, если в новом адресе установлен бит «multicast» или сброшен бит «OUI enforced».

Команда с префиксом `no` возвращает интерфейсу исходный MAC-адрес.

Свойства

Идентификатор	10.6.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

Аргументы

```
(config-if)>      mac address <address>
(config-if)> no    mac address
```

	Тип	Описание
<code>address</code>	MAC-адрес	MAC-адрес интерфейса

`interface ip address`

Меняет IP-адрес и маску сетевого интерфейса. Позволяет либо установить параметры вручную, либо с помощью команды `interface ip dhcp` запустить DHCP-клиент для автоматической настройки. Префикс `no` сбрасывает адрес на 0.0.0.0.

Свойства

Идентификатор	10.100.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет
Тип интерфейса	IP

Аргументы

```
(config-if)>      ip address <address>
(config-if)> no    ip address
```

	Тип	Описание
<code>address</code>	IP-подсеть	Адрес и маска сетевого интерфейса.

`interface ip alias`

Устанавливает дополнительный IP-адрес и маску сетевого интерфейса (псевдоним). Префикс `no` сбрасывает указанный псевдоним на 0.0.0.0, тем самым удаляя его. Если при вводе с префиксом `no` аргументы не передаются, команда удаляет все псевдонимы.

Свойства

Идентификатор	10.100.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	нет

Аргументы

```
(config-if)>      ip alias <address>
(config-if)> no    ip alias [address]
```

	Тип	Описание
--	-----	----------

address	IP-подсеть	Адрес и маска сетевого интерфейса
---------	------------	-----------------------------------

interface ip dhcp

Запустить на интерфейсе DHCP-клиент для автоматической настройки сетевых параметров: IP-адреса, маски, серверов DNS и шлюза по умолчанию. Префикс `no` останавливает службу DHCP-клиента, удаляет динамически настроенные параметры и возвращает статические настройки.

Свойства

Идентификатор	10.100.3
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	нет
Тип интерфейса	Ethernet

Аргументы

```
(config-if)> ip dhcp
(config-if)> no ip dhcp
```

interface ip mtu

Меняет значение MTU на сетевом интерфейсе. Префикс `no` сбрасывает значение MTU на то, которое было до первого применения команды.

При установлении соединения по протоколу PPP (IPCP), удаленному узлу будут отправляться пакеты указанного размера MTU, даже если он указал MRU меньшего значения.

Свойства

Идентификатор	10.100.5
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	нет
Вход в группу	нет
Тип интерфейса	IP

Аргументы

```
(config-if)> ip mtu <mtu>
(config-if)> no ip mtu
```

	Тип	Описание
mtu	Целое число	Значение MTU

interface ip tcp adjust-mss

Устанавливает ограничение максимального размера сегмента исходящих сессий TCP, меняя значение в поле заголовка SYN-пакетов. Префикс `no` отменяет действие команды.

Свойства

Идентификатор	10.100.28.12
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	нет
Вход в группу	нет

Тип интерфейса	IP
----------------	----

Аргументы

```
(config-if)> ip tcp adjust-mss (pmtu | <mss>)
(config-if)> no ip tcp adjust-mss
```

	Тип	Описание
pmtu	Ключевое слово	Установить верхнюю границу MSS, равную минимальному MTU на пути к удаленному узлу, см. Path MTU Discovery
mss	Целое число	Верхняя граница MSS

ip route

Настройка статических маршрутов IP. Команда добавляет статический маршрут в таблицу маршрутизации. Маршрут задает правило передачи IP-пакетов через определенный шлюз или сетевой интерфейс. В качестве сети назначения можно указать ключевое слово `default`. Префикс `no` удаляет маршрут.

Свойства

Идентификатор	100.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	нет

Аргументы

```
(config)> ip route (<network> | <host> | default) (<interface> | <gateway>) [metric]
(config)> no ip route (<network> | <host> | default) [<interface> | <gateway>] [metric]
```

	Тип	Описание
network	IP-подсеть	Сеть назначения
host	IP-адрес	Узел назначения
default	Ключевое слово	Маршрут по умолчанию
interface	Строка	Полное имя интерфейса или псевдоним
metric	Целое число	Метрика маршрута
gateway	IP-адрес	Адрес шлюза

global

Устанавливает для интерфейса свойство «global». Это свойство необходимо для установки маршрута по умолчанию, работы DynDNS-клиента и NAT. Можно представлять global-интерфейсы, как ведущие в глобальную сеть (в интернет).

Свойства

Идентификатор	101
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да

Аргументы

```
(config-if)> global <interface>
(config-if)> no global <interface>
```

	Тип	Описание
--	-----	----------

<code>interface</code>	Строка	Полное имя интерфейса или псевдоним
------------------------	--------	-------------------------------------

Firewall и NAT

Описание команд

`ip nat`

Включает трансляцию «локальных» адресов сети `network` или сети за интерфейсом `interface`. Например, команда `ip nat _LAN` означает, что для всех пакетов из сети `_LAN`, проходящих через маршрутизатор, будет выполнена подмена адресов источника.

Свойства

Идентификатор	100.50
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	нет

Аргументы

```
(config-if)> ip nat (<interface>|<network>)
(config-if)> no ip nat (<interface>|<network>)
```

	Тип	Описание
<code>interface</code>	Строка	Имя интерфейса источника (полное имя интерфейса или псевдоним)
<code>network</code>	IP-подсеть	Диапазон IP-адресов источника, подлежащих трансляции

`ip static`

Задаёт статическую привязку локальных IP-адресов к глобальным. Если `interface` или `network` соответствует глобальному интерфейсу, то будет выполняться трансляция адреса источника (SNAT). Если `to-address` соответствует глобальному интерфейсу, то будет выполняться трансляция адреса назначения (DNAT). Номер порта TCP/UDP всегда рассматривается как порт назначения.

Если `network` соответствует одному адресу, и этот адрес равен `to-address`, то такое правило будет запрещать трансляцию указанного адреса, которая могла бы быть выполнена исходя из заданных правил `ip nat`.

Правила `ip static` имеют более высокий приоритет по сравнению с правилами `ip nat`.

Пример: Пусть имеется маршрутизатор между «локальной» сетью 172.16.1.0/24 и «глобальной» сетью 10.0.0.0/16. Требуется, чтобы все запросы, приходящие на «глобальный» интерфейс этого маршрутизатора на порт 80, транслировались на «локальный» сервер с адресом 172.16.1.33. Последовательность команд, реализующих такую схему, может выглядеть так:

```
interface _LAN
ip address 172.16.1.1/24
!
interface _WAN
ip address 10.0.0.1/16
!
global _WAN
ip nat _LAN
ip static tcp _WAN 80 172.16.1.33 80
```

Свойства

Идентификатор	100.51
Префикс <code>no</code>	да
Меняет настройки	да

Многократный ввод	да
Вход в группу	нет

Аргументы

```
(config-if)> ip static [protocol] (<interface>|<network>) [port] <to-address> [to-port]
(config-if)> no ip static [[protocol] (<interface>|<network>) [port] <to-address> [to-port]]
```

	Тип	Описание
protocol	Строка	IP-протокол: TCP или UDP. Используется совместно с port
interface	Строка	Имя интерфейса источника (полное имя интерфейса или псевдоним)
network	IP-подсеть	Диапазон адресов, подлежащих трансляции
port	Число	Номер порта TCP/UDP, подлежащего трансляции
to-address	IP-адрес	Адрес
to-port	Число	Номер порта TCP/UDP

interface security-level

Задаёт уровень безопасности для данного интерфейса.

Уровень безопасности определяет логику работы межсетевого экрана в отношении данного интерфейса: Соединения могут устанавливаться из сетей за интерфейсами `private` в сети за интерфейсами `public`, либо между двумя интерфейсами `private`. Соединения НЕ могут устанавливаться из сетей за интерфейсами `public` в сети за интерфейсами `private`, а также между двумя интерфейсами `public`. Само устройство принимает сетевые подключения (разрешает управление) только с интерфейсов `private`. По-умолчанию, всем интерфейсам присваивается уровень безопасности `public`.

Списки доступа имеют более высокий приоритет, чем уровни безопасности.

Свойства

Идентификатор	10.50
Префикс <code>no</code>	нет
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	IP

Аргументы

```
(config-if)> security-level (public|private)
```

access-list

Настройка правил фильтрации пакетов. Команда создает список правил с заданным именем, в который можно добавлять разрешающие и запрещающие правила командами `permit` и `deny` соответственно. Созданный таким образом список можно привязать к сетевому интерфейсу командой `interface ip access-group`.

Префикс `no` удаляет список правил.

Свойства

Идентификатор	100
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	(config-acl)

Аргументы

```
(config)>      access-list <acl>
(config)> no   access-list <acl>
```

	Тип	Описание
acl	Строка	Имя списка правил фильтрации (ACL)

Команды

		Описание
1	deny	Добавить запрещающее правило
2	permit	Добавить разрешающее правило

access-list deny

Команда задает правило фильтрации пакетов в заданном списке ACL. Префикс no удаляет правило.

Свойства

Идентификатор	100.1
Префикс no	да
Меняет настройки	да
Множественный ввод	да

Аргументы

```
(config-acl)>      deny  (tcp|udp)  <source> <source-mask> [port [lt|eq|gt] <source-port>]
                                     <destination> <destination-mask> [port [lt|eq|gt]
                                     <destination-port>]

(config-acl)>      deny  icmp        <source> <source-mask> <destination> <destination-
                                     mask>

(config-acl)> no   deny  (tcp|udp)  <source> <source-mask> [port [lt|eq|gt] <source-port>]
                                     <destination> <destination-mask> [port [lt|eq|gt]
                                     <destination-port>]

(config-acl)> no   deny  icmp        <source> <source-mask> <destination> <destination-
                                     mask>
```

	Тип	Описание
tcp	Ключевое слово	Протокол TCP
udp	Ключевое слово	Протокол UDP
icmp	Ключевое слово	Протокол ICMP
source	IP-адрес	Адрес источника в заголовке IP-пакета
source-mask	IP-маска	Маска, накладываемая на адрес источника в заголовке IP-пакета перед сравнением с source
source-port	Целое число	Порт источника в заголовке TCP или UDP
destination	IP-адрес	Адрес назначения в заголовке IP-пакета
destination-mask	IP-маска	Маска, накладываемая на адрес назначения в заголовке IP-пакета перед сравнением с destination
destination-port	Целое число	Порт назначения в заголовке TCP или UDP
port	Ключевое слово	
eq	Ключевое слово	Оператор равенства порта с указанным значением source-port или destination-port
lt	Ключевое слово	Оператор «меньше» при сравнении порта с указанным значением source-port или destination-port

gt	Ключевое слово	Оператор «больше» при сравнении порта с указанным значением <code>source-port</code> или <code>destination-port</code>
----	----------------	--

access-list permit

Команда задает правило разрешения передачи пакетов в заданном списке ACL. Префикс `no` удаляет правило.

Свойства

Идентификатор	100.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да

Аргументы

(config-acl)> permit (tcp udp) <source> <source-mask> [port [lt eq gt] <source-port>]		
		<destination> <destination-mask> [port [lt eq gt] <destination-port>]
(config-acl)> permit icmp <source> <source-mask> <destination> <destination-mask>		
(config-acl)> no permit (tcp udp) <source> <source-mask> [port [lt eq gt] <source-port>]		
		<destination> <destination-mask> [port [lt eq gt] <destination-port>]
(config-acl)> no permit icmp <source> <source-mask> <destination> <destination-mask>		
	Тип	Описание
tcp	Ключевое слово	Протокол TCP
udp	Ключевое слово	Протокол UDP
icmp	Ключевое слово	Протокол ICMP
source	IP-адрес	Адрес источника в заголовке IP-пакета
source-mask	IP-маска	Маска, накладываемая на адрес источника в заголовке IP-пакета перед сравнением с <code>source</code>
source-port	Целое число	Порт источника в заголовке TCP или UDP
destination	IP-адрес	Адрес назначения в заголовке IP-пакета
destination-mask	IP-маска	Маска, накладываемая на адрес назначения в заголовке IP-пакета перед сравнением с <code>destination</code>
destination-port	Целое число	Порт назначения в заголовке TCP или UDP
port	Ключевое слово	
eq	Ключевое слово	Оператор равенства порта с указанным значением <code>source-port</code> или <code>destination-port</code>
lt	Ключевое слово	Оператор «меньше» при сравнении порта с указанным значением <code>source-port</code> или <code>destination-port</code>
gt	Ключевое слово	Оператор «больше» при сравнении порта с указанным значением <code>source-port</code> или <code>destination-port</code>

interface ip access-group

Назначает именованный список правил фильтрации (ACL) на интерфейс. Второй параметр указывает направление трафика для которого будет применяться ACL. На один интерфейс может быть назначено несколько ACL. Префикс `no` отключает ACL для указанного интерфейса и направления трафика.

Свойства

Идентификатор	10.100.11
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	нет

Аргументы

```
(config-if)> ip access-group <name> (in|out)
(config-if)> no ip access-group <name> (in|out)
```

	Тип	Описание
<code>name</code>	Строка	Имя ACL

Switch и VLAN

Интерфейс Switch

Интерфейс типа `Switch` соответствует аппаратному коммутатору IEEE 802.1D, который имеет определенный набор портов — разъемов на корпусе устройства. `Switch` позволяет включить порты в различные виртуальные локальные сети VLAN IEEE 802.1Q.

Каждый порт коммутатора настраивается командами группы `interface port`, в которой можно задать режим работы `access` или `trunk`, и перечислить идентификаторы VLAN, в которые порт входит. В режиме `access` порт может входить только в один VLAN, при этом кадры Ethernet, передаваемые в сеть, не маркируются тегом 802.1Q. В режиме `trunk` порт может входить в несколько VLAN, и кадры передаются с тегом.

Интерфейс VLAN

Интерфейс типа `VLAN` позволяет работать с виртуальной сетью IEEE 802.1Q по протоколу IP. `VLAN` создается динамически, используя интерфейс класса Ethernet (сюда относится Bridge, SSID и пр.) или `Switch` в качестве родительского. Например:

```
(config)> interface Switch0/VLAN100
Created interface Switch0/VLAN100.
(config-if)>
```

При этом индекс `VLAN` (в примере — 100) задает идентификатор VLAN 802.1Q. Если `VLAN` создается поверх интерфейса Ethernet, то его исходящие кадры будут передаваться с маркером. Если `VLAN` создается поверх интерфейса Switch, то маркирование исходящих кадров зависит от настроек родительского интерфейса.

`VLAN` относится к классу Ethernet, т. е. агрегирует свойства классов IP и MAC. Таким образом, на интерфейсе `VLAN` можно настроить IP-адрес, MAC-адрес, включить его в мост и т. п. По умолчанию `VLAN` наследует MAC-адрес от родительского интерфейса.

Пример

На коммутаторе `Switch0` настроено два VLAN с идентификаторами 1 и 2 в режиме `access`. На первом VLAN создан интерфейс `Switch0/VLAN1` с IP-адресом 172.16.1.1/24, а на втором — интерфейс `Switch0/VLAN2`, на котором запущен DHCP-клиент:

```
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access
access vlan 1
!
port 3
```

```
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
ip address 172.16.1.1/24
up
!
interface Switch0/VLAN2
ip dhcp
up
!
```

Описание команд

interface port

Группа команд для настроек порта аппаратного коммутатора. В качестве аргумента указывается номер порта. Префикс `no` не применим.

Свойства

Идентификатор	10.10
Префикс <code>no</code>	нет
Меняет настройки	да
Многократный ввод	да
Тип интерфейса	Switch
Вход в группу	(<code>config-if-port</code>)

Аргументы

```
(config-if)> port <port>
```

	Тип	Описание
<code>port</code>	Целое число	Номер порта коммутатора

Команды

		Тип интерфейса	Описание
10	<code>mode</code>	Switch	Режим работы VLAN
11	<code>access</code>	Switch	Настройка VLAN в режиме доступа
12	<code>trunk</code>	Switch	Настройка VLAN в режиме мультиплексирования

interface port mode

Команда для выбора режима обработки тегов VLAN портом коммутатора. Две последующие вложенные команды включают либо режим *доступа*, либо режим *мультиплексирования*.

Свойства

Идентификатор	10.10.10
Префикс <code>no</code>	нет

Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Switch
Вход в группу	нет

Команды

		Тип интерфейса	Описание
1	<code>access</code>	Switch	Включить порт в режим доступа
2	<code>trunk</code>	Switch	Включить порт в режим мультиплексирования

`interface port mode access`

Команда включает порт в режим *доступа* в виртуальную локальную сеть VLAN, то есть в такой режим, когда через порт передаются только немаркированные кадры. На входящие кадры ставится маркер PVID, установленный командой `port access`. Порт является выходным только для VLAN с идентификатором PVID. При передаче кадров в порт, маркер VLAN с них снимается.

Префикс `no` выключает режим доступа.

В зависимости от аппаратной реализации коммутатора, порт может поддерживать или не поддерживать одновременную работу режима доступа и режима мультиплексирования. Если одновременная работа не поддерживается, то включение режима доступа автоматически отключает режим мультиплексирования.

Свойства

Идентификатор	10.10.10.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Switch

`interface port mode trunk`

Команда включает порт в режим *мультиплексирования* VLAN, то есть в такой режим, когда через порт передаются кадры, принадлежащие нескольким VLAN. При этом каждый кадр помечен маркером VLAN. Список идентификаторов сетей VLAN, в которые входит порт, устанавливается командой `port trunk`.

Префикс `no` выключает режим мультиплексирования.

В зависимости от аппаратной реализации коммутатора, порт может поддерживать или не поддерживать одновременную работу режима мультиплексирования и режима доступа. Если одновременная работа не поддерживается, то включение режима мультиплексирования автоматически отключает режим доступа.

Свойства

Идентификатор	10.10.10.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Switch

`interface port access`

Установка идентификатора VLAN на порту для работы в режиме доступа. Команда ставит идентификатор VLAN порта по умолчанию (PVID), разрешает передачу кадров указанного VLAN в порт и включает удаление маркера VLAN из передаваемых кадров. Префикс `no` удаляет настройку.

Свойства

Идентификатор	10.10.11
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Switch

Аргументы

```
(config-if-port)>      access vlan <vid>
(config-if-port)>no    access vlan
```

	Тип	Описание
<code>vlan</code>	Ключевое слово	
<code>vid</code>	Идентификатор VLAN	Идентификатор VLAN доступа

`interface port trunk`

Добавление порта в VLAN, разрешает прием и передачу кадров указанного VLAN в порт, причем маркер VLAN из передаваемых кадров не удаляется. В режиме trunk допускается добавление порта в несколько VLAN.

Команда с префиксом `no` удаляет порт из указанного VLAN либо из всех VLAN, если `vid` не указан.

Свойства

Идентификатор	10.10.12
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Тип интерфейса	Switch

Аргументы

```
(config-if-port)>      trunk vlan <vid>
(config-if-port)>no    trunk vlan [vid]
```

	Тип	Описание
<code>vlan</code>	Ключевое слово	
<code>vid</code>	Идентификатор VLAN	Идентификатор VLAN

Мосты

Интерфейс Bridge

Интерфейс типа `Bridge` представляет собой динамический интерфейс виртуального моста IEEE 802.1D, в который можно добавлять интерфейсы класса Ethernet (сюда относятся VLAN, SSID и пр.). `Bridge` реализуется программно, средствами операционной системы маршрутизатора.

`Bridge` относится к классу Ethernet, т. е. агрегирует свойства классов IP и MAC. Таким образом, на интерфейсе `Bridge` можно настроить IP-адрес, MAC-адрес и т. п. По умолчанию `Bridge` наследует MAC-адрес от первого добавленного интерфейса.

У добавляемого в мост интерфейса блокируются настройки IP, и теряется возможность непосредственно передавать IP-пакеты, поскольку он связывается с другими интерфейсами, добавленными в мост, на канальном уровне. Существует два способа добавить интерфейс в мост:

- `interface include` — с потерей настроек IP.

- `interface inherit` — с передачей настроек IP интерфейсу моста.

Второй способ удобен тем, что при настройке маршрутизатора по сети можно добавлять в мост даже тот интерфейс, через который осуществляется управление устройством. Сессия управления при этом не разорвется.

Пример

На коммутаторе `Switch0` настроено два VLAN с идентификаторами 10 и 20 в режиме `trunk`. На беспроводном адаптере `WifiMaster0` настроены две точки доступа: `WifiMaster0/AccessPoint0` и `WifiMaster0/AccessPoint1`. С помощью мостов `Bridge0` и `Bridge1` пакеты из беспроводных сетей передаются в порт 5 коммутатора `Switch0` с маркерами VLAN 10 и VLAN 20 соответственно:

```
interface Switch0
port 5
mode trunk
trunk vlan 10
trunk vlan 20
!
!
interface Switch0/VLAN10
up
!
interface Switch0/VLAN20
up
!
interface WifiMaster0/AccessPoint0
! здесь настраиваются параметры
! первой беспроводной сети
!
interface WifiMaster0/AccessPoint1
! здесь настраиваются параметры
! второй беспроводной сети
!
interface Bridge0
include Switch0/VLAN10
include WifiMaster0/AccessPoint0
up
!
interface Bridge1
include Switch0/VLAN20
include WifiMaster0/AccessPoint1
up
!
```

Описание команд

`interface include`

Задаёт имя Ethernet-интерфейса, который будет добавлен в программный мост в качестве порта. Префикс `no` удаляет интерфейс из моста.

См. также команду `inherit`, которая позволяет передать мосту некоторые настройки добавляемого интерфейса, такие как IP-адрес, маску и IP-псевдонимы, что позволяет добавить в мост интерфейс, через который осуществляется управление устройством, и не потерять управление.

Свойства

Идентификатор	10.12
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	да
Тип интерфейса	Bridge

Аргументы

```
(config-if)> include <interface>
(config-if)> no include <interface>
```

	Тип	Описание
interface	Интерфейс Ethernet	Полное имя Ethernet-интерфейса или псевдоним

interface inherit

Задаёт имя Ethernet-интерфейса, который будет добавлен в программный мост в качестве порта. В отличие от команды `include`, команда `inherit` передаёт мосту некоторые настройки добавляемого интерфейса, такие как IP-адрес, маску и IP-псевдонимы. При удалении либо самого моста, либо интерфейса из моста, эти настройки, даже если они были изменены, будут скопированы обратно на освободившийся интерфейс.

Команда с префиксом `no` удаляет интерфейс из моста, возвращает интерфейсу настройки, унаследованные ранее мостом, и сбрасывает эти настройки у моста.

Команда позволяет добавить в мост интерфейс, через который осуществляется управление устройством, и не потерять управление.

Свойства

Идентификатор	10.11
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	нет
Тип интерфейса	Bridge

Аргументы

```
(config-if)> inherit <interface>
(config-if)> no inherit <interface>
```

	Тип	Описание
interface	Интерфейс Ethernet	Полное имя Ethernet-интерфейса или псевдоним

PPP

Функции PPP

Интерфейсы класса PPP агрегируют функции Secure и IP, и добавляют к ним собственный набор настроек для поддержки протокола PPP. PPP используется для установления прямой связи между двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование и сжатие данных. В частности, PPP используется для подключения к интернету.

Функции Secure

Интерфейсы класса Secure предоставляют базовые настройки аутентификации, которые используются в интерфейсах класса PPP для подключения к удаленному узлу.

Интерфейс PPPoE

PPPoE — сетевой протокол канального уровня передачи кадров PPP через Ethernet.

Интерфейс PPTP

PPTP (Point-to-Point Tunneling Protocol) — это туннельный протокол, работающий в сетях IP и использующий PPP для реализации механизмов проверки подлинности, сжатия и шифрования.

Интерфейсы PPTP поддерживают шифрование MPPE, которое включается командой `interface encryption mppe`.

Интерфейс L2TP

L2TP (Layer 2 Tunneling Protocol) — протокол туннелирования, использующий PPP для установления виртуального соединения между двумя узлами сети с коммутацией пакетов аналогично PPTP.

Порядок настройки

NDMS v2.00 поддерживает несколько одновременных PPP-подключений по PPPoE, PPTP и L2TP. Каждому подключению соответствует сетевой интерфейс с индексом, например: PPPoE0. Настройка базовых параметров подключения выполняется следующим образом.

1. Создание сетевого интерфейса командой `interface`:

```
(config)> interface PPPoE0
System event, type = "INTERFACE"
name: PPPoE0
state: up

System event, type = "DEVICE"
ACTION: add
DEVPATH: /devices/virtual/net/ppp5
SUBSYSTEM: net
INTERFACE: ppp5
IFINDEX: 35
SEQNUM: 6804

(config-if)>
```

2. Ввод имени удаленного концентратора доступа командой `peer`:

```
(config-if)> peer tp.example.net
Using peer tp.example.net.
```

3. Для подключений по протоколу PPPoE, ввод имени интерфейса Ethernet, через который осуществляется подключение:

```
(config-if)> discovery Switch0/VLAN2
Using Switch0/VLAN2 for PPPoE discovery.
```

4. Ввод поддерживаемых протоколов аутентификации (PAP, CHAP, MS-CHAP, MS-CHAPv2):

```
(config-if)> authentication chap
CHAP authentication enabled.
(config-if)> authentication mschap
MSCHAP authentication enabled.
(config-if)> authentication mschap-v2
MSCHAPv2 authentication enabled.
```

5. Ввод имени пользователя и пароля для аутентификации на удаленном концентраторе доступа:

```
(config-if)> authentication identity 00889@example.net
Identity saved.
(config-if)> authentication password P@sSW0Rd
Password saved.
```

6. После того как базовые параметры PPP-интерфейса настроены, нужно запустить процесс подключения командой `connect`. NDMS будет пытаться выполнить подключение и автоматически восстанавливать его сразу после разрыва:

```
(config-if)> connect
PPP connection enabled.
```

Дополнительные параметры

LCP Echo

По умолчанию на интерфейсе PPP включена функция контроля соединения с помощью пакетов LCP Echo-Request и Echo-Reply. Команда `interface lcp echo` позволяет задать интервал отправки запросов Echo-Request и предельное количество непринятых ответов Echo-Reply, прежде чем считать соединение разорванным.

Можно отключить функцию LCP Echo, используя команду `interface lcp echo` с префиксом `no`:

```
(config-if)> no lcp echo
LCP echo disabled.
```

IPCP

В процессе согласования параметров IP маршрутизатор NDMS v2.00 получает от провайдера адрес шлюза по умолчанию и адреса DNS-серверов. Если соединение PPP используется для выхода в интернет, полученные адреса сохраняются в системе. Однако, в ряде случаев необходимо их проигнорировать. Для этого нужно при настройке соединения вызвать команды `interface ipcp default-route` и `interface ipcp name-servers` с префиксом `no`:

```
(config-if)> no ipcp default-route
Not using peer as a default gateway.
(config-if)> no ipcp name-servers
Not using remote name servers.
```

Описание команд

`interface peer`

Задаёт идентификатор удаленного узла к которому будет осуществляться подключение PPP. Более точный смысл настройки зависит от типа интерфейса. Например, для PPPoE команда `interface peer` задаёт имя концентратора доступа, а для PPTP — имя удаленного хоста или его IP-адрес. Префикс `no` отменяет настройку.

Свойства

Идентификатор	10.3
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	PPP

Аргументы

```
(config-if)> peer <peer>
(config-if)> no peer
```

	Тип	Описание
<code>peer</code>	Строка	Идентификатор удаленной точки подключения

`interface discovery`

Задаёт имя Ethernet-интерфейса, через который будет осуществляться соединение PPPoE. Префикс `no` отменяет настройку.

Свойства

Идентификатор	10.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

Тип интерфейса	PPPoE
----------------	-------

Аргументы

```
(config-if)>      discovery <interface>
(config-if)> no    discovery
```

	Тип	Описание
interface	Интерфейс Ethernet	Полное имя Ethernet-интерфейса или псевдоним

interface authentication pap

Включает поддержку аутентификации PAP. Префикс no отключает PAP.

Свойства

Идентификатор	10.98.20
Префикс no	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Secure

Аргументы

```
(config-if)>      authentication pap
(config-if)> no    authentication pap
```

interface authentication chap

Включает поддержку аутентификации CHAP. Префикс no отключает CHAP.

Свойства

Идентификатор	10.98.21
Префикс no	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Secure

Аргументы

```
(config-if)>      authentication chap
(config-if)> no    authentication chap
```

interface authentication mschap

Включает поддержку аутентификации MSCHAP. Префикс no отключает MSCHAP.

Свойства

Идентификатор	10.98.22
Префикс no	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Secure

Аргументы

```
(config-if)> authentication mschap
(config-if)> no authentication mschap
```

interface authentication mschap-v2

Включает поддержку аутентификации MSCHAPv2. Префикс `no` отключает MSCHAPv2.

Свойства

Идентификатор	10.98.23
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Secure

Аргументы

```
(config-if)> authentication mschap-v2
(config-if)> no authentication mschap-v2
```

interface authentication identity

Задает имя пользователя для аутентификации устройства на удаленной системе. Одинаково используется для подключений RPTP, PPPoE и L2TP.

Команда с префиксом `no` стирает заданное ранее имя пользователя.

Свойства

Идентификатор	10.98.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Secure

Аргументы

```
(config-if)> authentication identity<identity>
(config-if)> no authentication identity
```

	Тип	Описание
<code>identity</code>	Строка	Имя пользователя для аутентификации

interface authentication password

Задает пароль для аутентификации устройства на удаленной системе. Одинаково используется для подключений RPTP, PPPoE и L2TP.

Команда с префиксом `no` стирает значение пароля.

Свойства

Идентификатор	10.98.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Secure

Аргументы

```
(config-if)> authentication password <password>
(config-if)> no authentication password
```

	Тип	Описание
password	Строка	Пароль для аутентификации

```
interface encryption mppe
```

Включает поддержку шифрования MPPE. Префикс `no` отключает шифрование MPPE.

Свойства

Идентификатор	10.99.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	RPTP

Аргументы

```
(config-if)> encryption mppe
(config-if)> no encryption mppe
```

```
interface lcp echo
```

Задает правила тестирования соединения PPP средствами LCP echo. Префикс `no` отключает LCP echo.

Свойства

Идентификатор	10.40.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Тип интерфейса	PPP

Аргументы

```
(config-if)> lcp echo <interval> <count>
(config-if)> no lcp echo
```

	Тип	Описание
interval	Целое число	Интервал в секундах между отправками LCP echo. Если в течение указанного интервала времени от удаленной стороны не был получен запрос LCP echo, ей будет отправлен такой запрос с ожиданием ответа LCP reply.
count	Целое число	Количество отправленных подряд запросов LCP echo, на которые не был получен ответ LCP reply. Если <code>count</code> запросов LCP echo остались без ответа, соединение будет разорвано.

```
interface ipcp default-route
```

Использовать адрес удаленного узла как шлюз по умолчанию. Префикс `no` запрещает менять шлюз по умолчанию при подключении к удаленному узлу.

Свойства

Идентификатор	10.41.20
Префикс <code>no</code>	да

Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	PPP

Аргументы

```
(config-if)> ipcp default-route
(config-if)> no ipcp default-route
```

interface ipcp name-servers

Использовать адреса серверов DNS, полученные по IPCP. Префикс **no** запрещает менять настройки DNS при подключении к удаленному узлу.

Свойства

Идентификатор	10.41.21
Префикс no	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	PPP

Аргументы

```
(config-if)> ipcp name-servers
(config-if)> no ipcp name-servers
```

interface ip mru

Устанавливает значение MRU (Maximum Receive Unit), которое будет передано удаленному узлу при установлении соединения PPP (IPCP). Префикс **no** отменяет действие команды. Если значение MRU не задано, используется значение по умолчанию, равное 1460.

Свойства

Идентификатор	10.100.6
Префикс no	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет
Тип интерфейса	PPP

Аргументы

```
(config-if)> ip mru <mru>
(config-if)> no ip mru
```

	Тип	Описание
mru	Целое число	Значение MRU

interface connect

Иницирует процесс автоматического подключения к удаленной точке PPP. Попытки установить соединение продолжаются до тех пор, пока не увенчаются успехом. Префикс **no** разрывает соединение.

Свойства

Идентификатор	10.499
---------------	---------------

Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет

Модемы 3G

NDMS позволяет подключать различные устройства через USB и использовать их в качестве дополнительных сетевых интерфейсов. В том числе поддерживаются некоторые модели 3G-модемов для подключения к сетям GPRS/EDGE, HSDPA и EVDO.

Базовые функции сетевых интерфейсов USB

Основным свойством сетевых интерфейсов USB является возможность их присоединения к USB-устройству в момент «горячего подключения». Все сетевые интерфейсы USB могут быть созданы с помощью команды `interface` до того, как USB-устройство было физически подключено. Это позволяет заранее задать необходимые настройки и сохранить их в текущей конфигурации.

Сетевые интерфейсы USB обладают признаком `plugged`, который принимает значения `yes` или `no` в зависимости от того, подключено USB-устройство или нет.

При подключении USB-устройства выполняется его распознавание. Если в результате распознавания оно было отнесено к одному из типов сетевых интерфейсов, в системе выполняется поиск уже созданного интерфейса с признаком `plugged` в значении `no`. Если такого интерфейса не нашлось, автоматически создается новый.

Идентификаторы производителя и модели

Все поддерживаемые USB-устройства должны обладать 16-битными идентификаторами производителя и модели, которые считываются сразу после подключения. Как правило, отдельные типы сетевых интерфейсов USB поддерживают только одну пару значений этих идентификаторов. Однако, существуют и такие, которые поддерживают целую группу устройств, имеющих различные идентификаторы.

Для того чтобы не возникло путаницы с настройками при подключении нескольких USB-устройств одновременно, идентификаторы производителя и модели хранятся в текущих настройках в виде команды `interface usb device-id`. Таким образом, сопоставление сетевого интерфейса и физического устройства может быть выполнено более точно.

Описание

Многие USB-устройства содержат текстовые строки с названием фирмы-производителя и модели. Если при создании нового сетевого интерфейса удастся их считать, они автоматически сохраняются в строке описания.

Например, при подключении USB-адаптера последовательного порта RS-232 он определяется как сетевой интерфейс `UsbModem0`. Сначала пользователю приходит некоторое количество системных событий, связанных с распознаванием устройства. Затем можно вывести текущие настройки и убедиться в том, что появился новый сетевой интерфейс:

```
...
System event, type = "DEVICE"
ACTION: add
DEVPATH: /devices/pci0000:00/0000:00:1d.3/usb4/4-2/4-2:1.0/ttyUSB0/tty/ttyUSB0
SUBSYSTEM: tty
MAJOR: 188
MINOR: 0
SEQNUM: 2944
DEVICE: /proc/bus/usb/004/002
ID_BUS: usb
ID_VENDOR_ID: 0557
ID_MODEL_ID: 2008

System event, type = "INTERFACE"
name: UsbModem0
state: up
```

```

System event, type = "DEVICE"
ACTION: add
DEVPATH: /devices/virtual/net/ppp5
SUBSYSTEM: net
INTERFACE: ppp5
IFINDEX: 13
SEQNUM: 2945

System event, type = "DEVICE"
ACTION: add
DEVPATH: /bus/usb/drivers/pl2303
SUBSYSTEM: drivers
SEQNUM: 2946

(config)> show running-config
...
interface UsbModem0
description "Prolific Technology Inc. , USB-Serial Controller D"
usb device-id 0557 2008
!
...

```

USB-модемы

USB-модемы в NDMS v2.00 — это сетевые интерфейсы, агрегирующие свойства классов USB и PPP. Сюда относятся как обычные последовательные интерфейсы RS-232, к которым можно подключить внешний модем, так и специализированные устройства, предназначенные для подключения к мобильным сетям GPRS/EDGE, HSDPA и EVDO.

В дополнение к параметрам классов USB и PPP, на всех USB-модемах NDMS позволяет настроить следующее:

- строки инициализации;
- команду подключения;
- пин-код для активации SIM-карты;
- имя точки доступа APN для доступа к мобильной сети.

В зависимости от модели устройства и условий использования, не все настройки из этого списка могут понадобиться. В общем случае, сценарий работы USB-модема следующий:

7. После подключения и успешной инициализации базовых свойств USB проверяется необходимость проверки пин-кода.
8. Если необходимо, в SIM-карту вводится пин-код, а если он не настроен, то до момента настройки подключение к сотовой сети будет невозможно.
9. Если включен `interface connect` и настроены необходимые параметры PPP, на модем передаются строки инициализации, настройки `APN` и команда установки соединения.
10. В случае неуспешного подключения или разрыва соединения повторно выполняется предыдущий пункт.

Описание команд

`interface usb device-id`

Задаёт идентификатор производителя и модели USB-устройства. Префикс `no` удаляет настройку.

Свойства

Идентификатор	10.30.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	USB

Аргументы

```
(config-if)>      usb device-id <vendor> <model>
(config-if)> no    usb device-id
```

	Тип	Описание
vendor	Строка	Четырехзначный код 16-битного идентификатора производителя USB-устройства
model	Строка	Четырехзначный код 16-битного идентификатора модели USB-устройства

interface modem init

Задаёт последовательность команд инициализации модема в виде строки. Каждая новая строка добавляется либо в конец списка, либо на позицию с указанным индексом. Префикс `no` стирает либо все строки инициализации, либо строку с указанным индексом.

Свойства

Идентификатор	10.34.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Тип интерфейса	USB Modem

Аргументы

```
(config-if)>      modem init [index] <string>
(config-if)> no    modem init [index]
```

	Тип	Описание
index	Целое число	Номер строки, которую необходимо добавить или удалить. Если не указан, то новая строка добавляется в конец списка или, если используется префикс <code>no</code> , очищается весь список.
string	Строка	Строка инициализации, которую необходимо добавить.

interface modem connect

Задаёт последовательность команд, которые посылаются модему для выполнения исходящего звонка. Префикс `no` удаляет настройку.

Свойства

Идентификатор	10.34.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	USB Modem

Аргументы

```
(config-if)>      modem connect (dial <phone> | <string>)
(config-if)> no    modem connect
```

	Тип	Описание
string	Строка	Строка с командами, которая посылается модему для выполнения исходящего звонка.
phone	Строка	Номер телефона. Если задан, то для выполнения исходящего звонка модему посылается строка <code>ATD<phone></code> .

interface modem pin-code

Задает четырехзначный пин-код для инициализации модема. Префикс `no` удаляет настройку.

Свойства

Идентификатор	10.34.9
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	USB Modem

Аргументы

```
(config-if)> modem pin-code <code>
```

```
(config-if)> no modem pin-code
```

	Тип	Описание
<code>code</code>	Строка	Строка, содержащая четыре цифры пин-кода.

interface ip apn

Задает имя точки доступа (Access Point Name, APN) к мобильной сети для получения услуги передачи данных по протоколу IP. При заданном имени APN, модему посылается специальная строка инициализации вида `AT+CGDCONT=1,"IP","APN"` после строк, заданных командой `interface modem init`. Префикс `no` удаляет настройку.

Свойства

Идентификатор	10.100.22
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	USB Modem

Аргументы

```
(config-if)> ip apn <apn>
```

```
(config-if)> no ip apn
```

	Тип	Описание
<code>apn</code>	Строка	Имя APN. Если задано, то после инициализации и перед выполнением исходящего звонка модему посылается строка <code>AT+CGDCONT=1,"IP","<apn>"</code> .

Беспроводная сеть 802.11

Точки Доступа

Базовые станции для подключения клиентов к проводной сети через радио-канал описываются в NDMS v2.00 как интерфейсы беспроводных точек доступа (AccessPoint). Подобная функциональность требует наличия у маршрутизатора соответствующего аппаратного обеспечения - беспроводного адаптера. Каждому физическому адаптеру, способному принимать клиентские подключения, в NDMS v2.00 соответствует интерфейс WifiMaster, у которого имеется столько дочерних интерфейсов AccessPoint, сколько беспроводных сетей он способен обслуживать одновременно.

Интерфейс WifiMaster относится к классу Radio, то есть имеет настройки физического уровня: частота вещания, мощность передатчика и проч. Интерфейсы AccessPoint агрегируют функции классов Ethernet и SSID. То есть, у всех точек доступа на одном адаптере будут одни и те же «физические» настройки, однако могут отличаться имя

сети (SSID) и алгоритмы обеспечения безопасности. Интерфейсы точек доступа являются маршрутизируемыми интерфейсами.

Беспроводные станции

Клиентское подключение к сети другой беспроводной точки доступа соответствует интерфейсу WifiStation. Для беспроводных адаптеров, поддерживающих режим станции, в NDMS v2.00 автоматически создаются интерфейсы этого типа. В соответствии с аппаратными возможностями адаптера, допускается наличие нескольких интерфейсов WifiStation, а так же одновременная работа в режимах беспроводной точки доступа и станции. Если данный адаптер не поддерживает одновременную работу в двух режимах, то при попытке включения очередного интерфейса, будет выдано соответствующее предупреждение.

Интерфейсы WifiStation агрегируют функции классов Ethernet, Radio и SSID. Интерфейсы этого типа также являются маршрутизируемыми интерфейсами.

Команды настройки сети

interface ssid

Задаёт имя беспроводной сети (SSID) для интерфейсов «беспроводная станция» (WifiStation) и «точка доступа» (AccessPoint). Без заданного значения SSID точка доступа не будет работать, а станция будет пытаться подключиться к одной из доступных беспроводных сетей по своему усмотрению.

Префикс `no` отменяет настройку.

Свойства

Идентификатор	200
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	SSID

Аргументы

```
(config-if)>      ssid<ssid>
(config-if)> no  ssid
```

	Тип	Описание
<code>ssid</code>	Строка	Имя беспроводной сети (SSID)

interface channel

Задаёт радио-канал (частоту вещания) для беспроводных интерфейсов. Интерфейсы Wi-Fi принимают в качестве номера канала целые числа от 1 до 14 (диапазон частот от 2.412ГГц до 2.484ГГц) и от 36 до 165 (диапазон частот от 5.180ГГц до 5.825ГГц)

Свойства

Идентификатор	201
Префикс <code>no</code>	нет
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Radio

Аргументы

```
(config-if)>  channel<channel>
```

	Тип	Описание
--	-----	----------

channel	Число	Номер радио-канала
---------	-------	--------------------

interface compatibility

Задаёт стандарты беспроводной связи, с которыми должен быть совместим данный беспроводной адаптер (интерфейс). Для интерфейсов Wi-Fi совместимость задается строкой из латинских букв A, B, G, N, обозначающих дополнения к стандарту IEEE 802.11. К примеру, наличие в строке совместимости буквы A будет означать, что данный адаптер сможет взаимодействовать с 802.11a-совместимыми устройствами через радио-канал. Набор допустимых строк совместимости определяется аппаратными возможностями конкретного адаптера и требованиями соответствующих дополнений к стандарту IEEE 802.11.

Свойства

Идентификатор	203
Префикс no	нет
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Radio

Аргументы

```
(config-if) > compatibility <compatibility>
```

	Тип	Описание
compatibility	Строка	Строка совместимости

interface power

Задаёт мощность передатчика для радио-интерфейсов. Максимальная мощность передатчика ограничена его аппаратными возможностями и государственными законами о радиосвязи. Данная команда позволяет лишь уменьшить мощность передающего устройства относительно его максимальной мощности, с целью возможного снижения помех для других устройств в этом диапазоне.

Свойства

Идентификатор	205
Префикс no	нет
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	Radio

Аргументы

```
(config-if) > power <power>
```

	Тип	Описание
power	Число	Мощность передатчика в процентах от максимальной мощности (1-100)

Команды настройки безопасности

interface authentication wpa-psk

Задаёт предварительно согласованный ключ для аутентификации по протоколу WPA-PSK. Возможно задание ключа в виде 256-битного шестнадцатеричного числа, либо в виде строки ASCII-символов длиной от 8 до 63 символов.

Команда с префиксом no отменяет настройку.

Свойства

Идентификатор	10.98.201
---------------	------------------

Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	SSID

Аргументы

```
(config-if)> wpa-psk <psk>
(config-if)> no wpa-psk
```

	Тип	Описание
<code>psk</code>	Строка	Предварительно согласованный ключ

interface authentication shared

Включает режим аутентификации с разделяемым ключом. Этот режим используется только в сочетании с шифрованием WEP. Разделяемые ключи задаются командой `interface encryption key`. Префикс `no` отменяет действие команды, т. е. переводит аутентификацию в режим `open`.

Свойства

Идентификатор	10.98.200
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	SSID

Аргументы

```
(config-if)> authentication shared
(config-if)> no authentication shared
```

interface encryption enable

Включает шифрование на беспроводном интерфейсе. По умолчанию используется шифрование WEP. Команды `wpa` и `wpa2` позволяют указать, что нужно использовать иной алгоритм шифрования.

Вызов команды с префиксом `no` отключает шифрование данных на беспроводном интерфейсе.

Свойства

Идентификатор	10.99.201
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	SSID

Аргументы

```
(config-if)> encryption enable
(config-if)> no encryption enable
```

interface encryption key

Задает ключи шифрования WEP. В зависимости от разрядности, ключ может быть задан 10 шестнадцатиричными цифрами (5 символами ASCII) — 40-битный ключ, или 26 шестнадцатиричными цифрами (13 символами ASCII) — 104-битный ключ. Всего может быть задано от 1 до 4 ключей шифрования, и один из них должен быть назначен ключом по-умолчанию.

Свойства

Идентификатор	10.99.200
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Тип интерфейса	SSID

Аргументы

```
(config-if)> encryption key <id> (<hex> [default]) | default
(config-if)> no encryption key <id>
```

	Тип	Описание
<code>id</code>	Число	Номер ключа. Всего можно задать до 4-х ключей
<code>hex</code>	Строка	Ключ в виде шестнадцатиричного числа
<code>default</code>	Ключевое слово	Указывает, что данный ключ будет использован по умолчанию

interface encryption wpa

Включает алгоритмы обеспечения безопасности WPA на беспроводном интерфейсе. Беспроводной интерфейс может разрешать совместное использование WPA и WPA2, однако поддержка WEP автоматически отключается при включении любого из WPA.

Вызов с префиксом `no` отключает WPA.

Свойства

Идентификатор	10.99.202
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	SSID

Аргументы

```
(config-if)> encryption wpa
(config-if)> no encryption wpa
```

interface encryption wpa2

Включает алгоритмы обеспечения безопасности WPA2 (IEEE 802.11i, RSN) на беспроводном интерфейсе. Беспроводной интерфейс может разрешать совместное использование WPA и WPA2, однако поддержка WEP автоматически отключается при включении любого из WPA.

Вызов с префиксом `no` отключает WPA2.

Свойства

Идентификатор	10.99.203
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Тип интерфейса	SSID

Аргументы

```
(config-if)> encryption wpa2
(config-if)> no encryption wpa2
```

Настройка DNS

Адреса DNS-серверов настраиваются командой `ip name-server`. Они также могут быть получены динамически при подключении по PPP или DHCP.

Адреса DNS-серверов нужны для разрешения имен хостов в IP-адреса при работе в режиме DNS-прокси, а также при взаимодействии маршрутизатора NDMS v2.00 с удаленными хостами, заданными по имени.

Описание команд

`ip name-server`

Настройка IP-адресов серверов DNS. В команде указывается от одного до трех адресов в порядке их приоритета. Сохраненные таким образом адреса называются *статическими* в противоположность *динамическим* — зарегистрированным службами PPP или DHCP.

Активными, то есть используемыми в данный момент адресами, являются те, которые были зарегистрированы позже остальных. Обычно система использует адреса, полученные последней успешно подключившейся службой PPP или DHCP. Если ни одна из служб не регистрирует адреса DNS, активными будут статические настройки. Однако, если после регистрации динамических адресов пользователем были изменены статические настройки, они становятся активными, пока не будут зарегистрированы новые динамические адреса.

Префикс `no` удаляет указанные адреса серверов DNS из статического и активного списка, если команда дается с аргументами, либо очищает список статических адресов, если команда дается без аргументов.

Свойства

Идентификатор	100.9
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет

Аргументы

```
(config-if)> ip name-server <address> [address2] [address3]
(config-if)> no ip name-server
```

	Тип	Описание
address	IP-адрес	IP-адрес сервера DNS
address2	IP-адрес	IP-адрес сервера DNS
address3	IP-адрес	IP-адрес сервера DNS

`service dns-proxy`

Команда запуска прокси-сервера DNS. Если в системе не настроены статические адреса серверов DNS, либо если они не были получены по DHCP или PPP, служба не будет видна в списке процессов `show services`. Как только для работы службы станет достаточно настроек, она включится автоматически. Префикс `no` останавливает службу.

Свойства

Идентификатор	101.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

Сервер DHCP

На маршрутизаторе NDMS v2.00 может быть запущен сервер DHCP, который может выдавать адреса из заданных пулов на одном или нескольких сетевых интерфейсах. Сервер включается командой `CommandServiceDhcp`. Пулы настраиваются командой `ip dhcp pool`.

Есть возможность сделать статические привязки IP-адресов к MAC-адресам хостов с помощью команды `ip dhcp host`.

Описание команд

`ip dhcp pool`

Вход в группу команд для настройки DHCP-пула. Если пул не найден, команда пытается его создать. Префикс `no` удаляет пул. Для пула задается список DNS-серверов (команда `dns-server`), шлюз по умолчанию (команда `default-router`) и время аренды (команда `lease`), а также диапазон динамических IP-адресов (команда `range`).

Внимание: В текущей версии системы реализована поддержка не более одного пула на интерфейс. Для корректной работы DHCP-сервера требуется, чтобы диапазон IP-адресов, установленный командой `range`, принадлежал сети, настроенной на одном из Ethernet-интерфейсов устройства.

После настройки пулов необходимо включить службу DHCP с помощью команды `service dhcp`.

Свойства

Идентификатор	100.2.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да
Вход в группу	(<code>config-dhcp</code>)

Аргументы

```
(config)> ip dhcp pool <name>
(config)> no ip dhcp pool <name>
```

	Тип	Описание
<code>name</code>	Строка	Имя пула

Команды

		Описание
3	<code>range</code>	Настройка диапазона адресов пула <code>network</code>
5	<code>default-router</code>	Настройка шлюза по умолчанию
6	<code>dns-server</code>	Настройка адресов DNS
7	<code>lease</code>	Настройка времени аренды

`ip dhcp pool range`

Настройка диапазона динамических адресов, выдаваемых DHCP-клиентам некоторой подсети. Диапазон задается начальным и конечным IP-адресом, либо начальным адресом и размером. Сетевой интерфейс, к которому будут применены настройки, выбирается автоматически. Адрес выбранного интерфейса используется в качестве шлюза по умолчанию и DNS-сервера, если не заданы другие адреса командами `ip dhcp pool default-router` и `ip dhcp pool dns-server`.

Префикс `no` удаляет диапазон.

Свойства

Идентификатор	100.2.1.3
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет

Аргументы

```
(config)> range <begin> (<end> | <size>)  
(config)> no range
```

	Тип	Описание
<code>begin</code>	IP-адрес	Начальный адрес пула
<code>end</code>	IP-адрес	Конечный адрес пула
<code>size</code>	Целое число	Размер пула

`ip dhcp pool default-router`

Настройка IP-адреса шлюза по умолчанию. Если не указан, то будет использоваться адрес, настроенный на ethernet-интерфейсе, определенном автоматически для заданного диапазона. Префикс `no` отменяет настройку.

Свойства

Идентификатор	100.2.1.5
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет

Аргументы

```
(config-dhcp)> default-router <address>  
(config-dhcp)> no default-router
```

	Тип	Описание
<code>address</code>	IP-адрес	Адрес шлюза по умолчанию

`ip dhcp pool dns-server`

Настройка IP-адресов серверов DNS. Если ничего не указано, то будет использоваться адрес, настроенный на ethernet-интерфейсе, определенном автоматически для заданного диапазона. Префикс `no` отменяет настройку.

Свойства

Идентификатор	100.2.1.6
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет

Аргументы

```
(config-dhcp)> dns-server <address1> [address2]  
(config-dhcp)> no dns-server
```

	Тип	Описание
--	-----	----------

address1	IP-адрес	Адрес первичного DNS-сервера
address2	IP-адрес	Адрес вторичного DNS-сервера

ip dhcp pool lease

Настройка времени аренды IP-адресов пула DHCP. Префикс `no` устанавливает значение по умолчанию, равное 86400 секунд.

Свойства

Идентификатор	100.2.1.7
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет
Вход в группу	нет

Аргументы

```
(config-dhcp)> lease <lease>
(config-dhcp)> no lease
```

	Тип	Описание
lease	Целое число	Время аренды в секундах

ip dhcp host

Настройка статической привязки IP-адреса к MAC-адресу хоста. Если хост с указанным именем не найден, команда пытается его создать. Префикс `no` удаляет хост. Если указанный IP-адрес не входит в диапазон ни одного пула, команда не будет влиять на работу DHCP-сервера.

Команда позволяет поменять MAC-адрес, оставив прежнее значение IP-адреса, и наоборот — поменять IP-адрес, оставив прежнее значение MAC-адреса.

Свойства

Идентификатор	100.2.2
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	да

Аргументы

```
(config)> ip dhcp host <name> [mac] [ip]
(config)> no ip dhcp host <name>
```

	Тип	Описание
name	Строка	Имя хоста
mac	MAC-адрес	MAC-адрес хоста для статической привязки IP-адреса. Если не указан, значение берется из предыдущей настройки.
ip	IP-адрес	IP-адрес хоста. Если не указан, значение берется из предыдущей настройки.

service dhcp

Команда запуска DHCP-сервера. Если для запуска службы недостаточно настроек (см. команды `ip dhcp pool`), служба не будет видна в списке процессов `show services`. Как только настроек станет достаточно, служба включится автоматически. Префикс `no` останавливает службу.

Свойства

Идентификатор	101.1
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

Управление доступом к устройству

Доступ к настройкам маршрутизатора NDMS v2.00 осуществляется через командную строку (`telnet`), web-интерфейс (`HTTP`) и `FTP`. Соответствующие службы должны быть запущены. При входе будет запрошен пароль администратора, который можно поменять с помощью команды `user password`.

Маршрутизатор позволяет подключаться к службам настроек через сетевые интерфейсы, на которых установлен уровень безопасности `private` (см. команду `interface security-level`) и не позволяет подключаться к интерфейсам с уровнем безопасности `public`. Кроме этого, доступ можно контролировать с помощью дополнительных разрешающих и запрещающих правил (см. команды `access-list` и `interface ip access-group`).

Описание команд

`service http`

Команда запуска HTTP-сервера, который предоставляет пользователю Web-интерфейс для настройки устройства. Префикс `no` останавливает службу.

Свойства

Идентификатор	101.20
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

`service ftp`

Команда запуска FTP-сервера, который предоставляет пользователю доступ к подключенным USB-носителям, файлам с настройками и файлу для записи новой версии микропрограммы. Префикс `no` останавливает службу.

Свойства

Идентификатор	101.17
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

`service telnet`

Команда запуска сервера telnet, который предоставляет пользователю интерфейс командной строки для настройки устройства. Префикс `no` останавливает службу.

Свойства

Идентификатор	101.21
Префикс <code>no</code>	да
Меняет настройки	да
Многократный ввод	нет

user password

Задает пароль пользователя. Пароль хранится в виде MD5-хеша, вычисленного из строки "пользователь:ndm:пароль".

Команда принимает аргумент в виде открытой строки или значения хеш-функции. Сохраненный пароль используется для аутентификации пользователя. Префикс `no` сбрасывает значение пароля таким образом, что пользователь теряет доступ к устройству. Для пользователя `admin` префикс `no` сбрасывает значение пароля на заводские настройки — "1234".

Свойства

Идентификатор	180.9
Префикс <code>no</code>	да
Меняет настройки	да
Множественный ввод	нет

Аргументы

```
(config-user)> password (md5 <hash> | <password>)  
(config-user)> no password
```

	Тип	Описание
<code>hash</code>	Строка	Значение MD5-хеша.
<code>password</code>	Строка	Открытое значение пароля, из которого автоматически вычисляется значение хеша.

Диагностика

Описание команд

show version

Выводит версию установленной микропрограммы.

```
(config)> show version  
ZyXEL Keenetic  
NDM OS version v2.00(BFW.1235)D0, Jul 28 2010, mips  
Copyright (c) 2010 ZyXEL Communications Corp.
```

Свойства

Идентификатор	600.1
Префикс <code>no</code>	нет
Меняет настройки	нет

show interface

Группа команд, предназначенная для отображения текущих настроек интерфейсов различных типов.

Каждая из команд данной группы применима к определенному типу интерфейса иерархии. Базовый тип интерфейса, к которому применима команда, указан в колонке «Тип интерфейса» таблицы команд ниже.

Если вводить саму команду `show interface`, не указывая дочерних команд, то будет показана таблица всех сетевых интерфейсов или информация по конкретному интерфейсу `name`:

```
(config)> show interface Bridge0  
  
type: Bridge  
description:  
state: up  
link: up  
address: 172.16.1.1
```

```
mask: 255.255.255.0
mtu: 1500
```

Свойства

Идентификатор	600.20
Префикс <code>no</code>	нет
Меняет настройки	нет
Множественный ввод	нет
Вход в группу	<code>(show-interface)</code>

Аргументы

```
(show)> interface [name]
```

	Тип	Описание
<code>name</code>	Строка	Полное имя интерфейса или псевдоним

Команды

		Тип интерфейса	Описание
2	<code>mac</code>	Switch	Отобразить таблицу MAC-адресов коммутатора
3	<code>stat</code>	Base	Отобразить статистику сетевого интерфейса
97	<code>wps</code>	SSID	Отобразить текущее состояние WPS на заданном SSID или значение PIN для радиointерфейса

`show ip route`

Выводит текущую таблицу маршрутизации.

```
(config)> show ip route
```

```
=====
Destination Gateway Interface Metric
=====
172.16.1.0/24 0.0.0.0 Bridge0 0
73.61.0.0/16 0.0.0.0 Bridge1 0
0.0.0.0/0 73.61.0.1 Bridge1 0
```

Свойства

Идентификатор	600.100.1
Префикс <code>no</code>	нет
Меняет настройки	нет

`show ip arp`

Выводит содержимое кеша ARP.

```
(config)> show ip arp
```

```
=====
IP MAC Interface
=====
172.16.1.23 00:14:c2:d8:8b:3e Bridge0
73.61.0.1 00:16:9c:6c:f6:81 Bridge1
```

Свойства

Идентификатор	600.100.10
Префикс <code>no</code>	нет
Меняет настройки	нет

show ip name-server

Выводит список текущих адресов DNS-серверов в порядке убывания приоритета. Отображает, включен ли DNS-прокси.

```
(config)> show ip name-server
status:
server: 8.8.8.8
server: 8.8.4.4
proxy: yes
```

Свойства

Идентификатор	600.100.9
Префикс no	нет
Меняет настройки	нет

show log

Выводит содержимое системного журнала, а именно записи, которые сохранились в циклическом буфере, а также новые записи по мере их поступления. Команда работает в фоновом режиме, то есть до принудительной остановки пользователем.

```
(config)> show log
=====
Time Message
=====
I [Jan 1 00:00:05] ndm: Command::LogResponse: Interface WiMax0 is set as
global.
I [Jan 1 00:00:05] ndm: Command::LogResponse: Interface UsbQualcommEvdo0 is
set as global.
I [Jan 1 00:00:05] ndm: Core::Authenticator: password has been changed for
user admin
I [Jan 1 00:00:05] pppd[719]: Plugin pppol2tp.so loaded.
I [Jan 1 00:00:05] pppd[719]: pppd 2.4.4 started by root, uid 0
I [Jan 1 00:00:05] l2tp_plugin[719]: l2tp version xl2tpd-1.1.11-plugin-0.1
started on (none) PID:719

I [Jan 1 00:00:05] l2tp_plugin[719]: Connecting to host 0.0.0.0, port 1701

I [Jan 1 00:00:05] ndm: ExecThread: "DHCP::Pool::Controller" started.
I [Jan 1 00:00:05] ndm: DHCP::Server: enabled
I [Jan 1 00:00:05] ndm: Command::LogResponse: DNS proxy enabled.
I [Jan 1 00:00:05] ndm: ExecThread: "FTP::Server" started.
I [Jan 1 00:00:05] ndm: FTP::Server: Starting service sucessfull
I [Jan 1 00:00:05] ndm: Command::LogResponse: FTP server enabled.
I [Jan 1 00:00:05] ndm: ExecThread: "HTTP::Server" started.
I [Jan 1 00:00:05] ndm: Command::LogResponse: HTTP server enabled.
I [Jan 1 00:00:05] ndm: ExecThread: "Telnet::Server" started.
I [Jan 1 00:00:05] ndm: Command::LogResponse: Telnet server enabled.
I [Jan 1 00:00:05] ndm: Configurator: configuration loaded.
I [Jan 1 00:00:05] ndm: Core::Hotplug::Manager: scanning hardware.
I [Jan 1 00:00:05] ag: HTTP::DigestAuthFilter: user accounts database: 1
records loaded.
I [Jan 1 00:00:06] ag: ServerApp: ready.
I [Jan 1 00:00:08] ndm: Core::Hotplug::Manager: scanning hardware: done.
I [Jan 1 00:00:08] ndm: Core::Main: system ready.
I [Jan 1 00:00:08] ndm: Core::Server: waiting for an incoming connection...
I [Jan 1 00:00:10] l2tp_plugin[727]: Maximum retries exceeded for tunnel 5403.
Closing.

W [Jan 1 00:00:10] l2tp_plugin[727]: stop_pppd: exit(3).

E [Jan 1 00:00:10] l2tp_plugin[719]: l2tp_get_socket failed
I [Jan 1 00:00:10] l2tp_plugin[719]: Exit.
```

Свойства

Идентификатор	600.50
Префикс no	нет
Меняет настройки	нет
Фоновый режим	да

tools ping

Отправляет запросы Echo-Request протокола ICMP указанному узлу сети и фиксирует поступающие ответы Echo-Reply. Время между отправкой запроса и получением ответа Round Trip Time (RTT) позволяет определять двусторонние задержки по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

Свойства

Идентификатор	601.1
Префикс no	нет
Меняет настройки	нет
Фоновый режим	да

Аргументы

(tools)> ping <host> [count <count>] [size <packetsize>]

	Тип	Описание
host	Строка	Доменное имя или IP-адрес хоста
count	Целое число	Количество ICMP-запросов. Если значение отсутствует, команда будет работать до прерывания пользователем.
packetsize	Целое число	Размер поля данных Echo-Request в байтах. По умолчанию — 56, что вместе с 8-байтовым заголовком задает размер ICMP-пакета — 64 байта.

Примеры настроек

Тестирование пропускной способности

Две подсети 192.168.1.0/24 и 192.168.2.0/24 непосредственно подключены к маршрутизатору. Первая сеть подключается через любой порт с 1 по 4, а вторая — через порт 5. Трансляция адресов отключена, маршрут по умолчанию отсутствует. Такая конфигурация используется для тестирования пропускной способности маршрутизатора при передаче пакетов из одной сети в другую.

```
system
set net.ipv4.ip_forward 1
!
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access
access vlan 1
!
port 3
mode access
access vlan 1
!
port 4
mode access
```

```

access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
security-level private
ip address 192.168.1.1 255.255.255.0
up
!
interface Switch0/VLAN2
security-level private
ip address 192.168.2.1 255.255.255.0
up
!
user admin
password md5 553de4d6e06ee424cd68ec66a39e5b78
!
service http
service telnet

```

Маршрутизация с включенной трансляцией адресов

Простейший вариант подключения к интернету. На интерфейсе `Switch0/VLAN2` настроен глобальный IP-адрес, прописан маршрут по умолчанию через шлюз `203.0.113.241` и настроены адреса DNS-серверов. Все хосты, подключенные к сети `Switch0/VLAN1`, выходят в интернет через NAT и DNS-прокси.

Отдельно нужно обратить внимание на то, что интерфейс `Switch0/VLAN1` имеет уровень безопасности `private`, а интерфейс `Switch0/VLAN2` — `public`. Таким образом задается политика безопасности: встроенный брандмауэр разрешает инициировать соединения только из VLAN 1 в VLAN 2. Из VLAN 2 запрещен доступ к устройству и к хостам VLAN 1. Затем с помощью команд `access-list` и `interface ip access-group` можно задать исключения из общего правила.

```

system
set net.ipv4.ip_forward 1
set net.ipv4.netfilter.ip_conntrack_max 4096
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
!
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access
access vlan 1
!
port 3
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1

```

```

security-level private
ip address 192.168.1.1 255.255.255.0
up
!
interface Switch0/VLAN2
security-level public
ip address 203.0.113.242 255.255.255.240
up
!
user admin
password md5 553de4d6e06ee424cd68ec66a39e5b78
!
ip route default 203.0.113.241
ip name-server 8.8.8.8 8.8.4.4
ip nat Switch0/VLAN1
global Switch0/VLAN2
service dns-proxy
service http
service telnet

```

DHCP-сервер и DHCP-клиент

Пример с трансляцией адресов дополнен получением динамического IP-адреса по DHCP на интерфейсе WAN. Для этого включен DHCP-клиент командой `interface ip dhcp`.

Кроме того, в локальную сеть `172.16.1.0/24` раздаются адреса по DHCP из диапазона `172.16.1.33–172.16.1.53`. Для этого включен DHCP-сервер командой `service dhcp` и настроен пул `_WEBADMIN`. В настройках нигде явно не указывается, что пул `_WEBADMIN` будет работать на интерфейсе `Switch0/VLAN1`. Привязка происходит автоматически, когда диапазон адресов пула попадает в сеть `172.16.1.0/24`, настроенную на интерфейсе.

```

system
set net.ipv4.ip_forward 1
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.netfilter.ip_conntrack_max 4096
!
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access
access vlan 1
!
port 3
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
description "LAN interface, DHCP server"
ip address 172.16.1.1/24
security-level private
up
!

```

```

interface Switch0/VLAN2
description "WAN interface, DHCP client"
ip dhcp
security-level public
up
!
ip dhcp pool _WEBADMIN
range 172.16.1.33 20
dns-server 172.16.1.1
default-router 172.16.1.1
!
global Switch/VLAN2
ip nat Switch/VLAN1
user admin
password md5 553de4d6e06ee424cd68ec66a39e5b78
!
service dhcp
service dns-proxy
service http
service telnet

```

Беспроводная точка доступа и станция в режиме моста

Дополним пример с DHCP-клиентом и сервером, добавив туда беспроводную точку доступа и станцию.

Допустим, требуется сделать беспроводное подключение к локальной сети (LAN), так чтобы хосты проводной и беспроводной части LAN «видели» друг друга непосредственно в одном сегменте Ethernet. Для этого создается интерфейс `Bridge0`, в который включаются интерфейсы `Switch0/VLAN1` и `WifiMaster0/AccessPoint0`. Теперь проводная и беспроводная сеть соединены через мост. IP-адрес `172.16.1.1` наследуется мостом `Bridge0` от проводного интерфейса `Switch0/VLAN1`.

Аналогично, интерфейс беспроводного клиента `WifiStation0` подключается через мост `Bridge1` к `Switch0/VLAN2`. Можно теперь подключить станцию `WifiStation0` к провайдеру, если он предоставляет услуги по Wi-Fi.

```

system
set net.ipv4.ip_forward 1
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.netfilter.ip_conntrack_max 4096
!
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access
access vlan 1
!
port 3
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
ip address 172.16.1.1/24

```

```

security-level private
up
!
interface Switch0/VLAN2
ip dhcp
security-level public
up
!
interface WifiStation0
description "WAN, wireless station"
security-level public
country-code RU
compatibility BGN
no up
!
interface WifiMaster0
country-code RU
compatibility BGN
up
!
interface WifiMaster0/AccessPoint0
description "LAN, wireless Access Point"
security-level private
ssid KEENETIC
up
!
interface Bridge0
description "LAN, IP address inherited from Switch0/VLAN1"
security-level private
include WifiMaster0/AccessPoint0
inherit Switch0/VLAN1
!
interface Bridgel
description "WAN, DHCP client inherited from Switch0/VLAN2"
security-level public
include WifiStation0
inherit Switch0/VLAN2
!
ip dhcp pool _WEBADMIN
range 172.16.1.33 20
dns-server 172.16.1.1
default-router 172.16.1.1
!
global Bridgel
ip nat Bridge0
service dhcp
service dns-proxy
service http
service telnet

```

Подключение к провайдеру по PPPoE

```

system
set net.ipv4.ip_forward 1
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.netfilter.ip_conntrack_max 4096
!
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access
access vlan 1

```

```

!
port 3
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
description "LAN interface, DHCP server"
ip address 172.16.1.1/24
security-level private
up
!
interface Switch0/VLAN2
description "WAN interface for PPPoE"
security-level public
up
!
interface PPPoE0
description "Internet connection"
discovery Switch/VLAN2
lcp echo 30 3
ipcp default-route
ipcp name-servers
authentication identity andreyd
authentication password amd031181
authentication chap
ip tcp adjust-mss pmtu
connect
up
!
ip dhcp pool _WEBADMIN
range 172.16.1.33 20
dns-server 172.16.1.1
default-router 172.16.1.1
!
global PPPoE0
ip nat Switch/VLAN1
service dhcp
service dns-proxy
service http
service telnet

```

Подключение к провайдеру по PPTP

```

system
set net.ipv4.ip_forward 1
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.netfilter.ip_conntrack_max 4096
!
interface Switch0
port 1
mode access
access vlan 1
!
port 2
mode access

```

```

access vlan 1
!
port 3
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
description "LAN interface, DHCP server"
ip address 172.16.1.1/24
security-level private
up
!
interface Switch0/VLAN2
description "WAN interface, DHCP client"
ip dhcp
security-level public
up
!
interface PPTP0
description "Internet connection"
peer vpn.corbina.net
lcp echo 30 3
ipcp default-route
ipcp name-servers
authentication identity sergeymv
authentication password smv050859
authentication chap
connect
up
!
ip dhcp pool _WEBADMIN
range 172.16.1.33 20
dns-server 172.16.1.1
default-router 172.16.1.1
!
global Switch/VLAN2
global PPTP0
ip nat Switch/VLAN1
service dhcp
service dns-proxy
service http
service telnet

```

Подключение к провайдеру по L2TP

```

system
set net.ipv4.ip_forward 1
set net.ipv4.tcp_fin_timeout 30
set net.ipv4.tcp_keepalive_time 120
set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
set net.ipv4.netfilter.ip_conntrack_max 4096
!
interface Switch0
port 1
mode access
access vlan 1
!

```

```

port 2
mode access
access vlan 1
!
port 3
mode access
access vlan 1
!
port 4
mode access
access vlan 1
!
port 5
mode access
access vlan 2
!
up
!
interface Switch0/VLAN1
description "LAN interface, DHCP server"
ip address 172.16.1.1/24
security-level private
up
!
interface Switch0/VLAN2
description "WAN interface, DHCP client"
ip dhcp
security-level public
up
!
interface L2TP0
description "Internet connection"
peer tp.corbina.net
lcp echo 30 3
ipcp default-route
ipcp name-servers
authentication identity sergeymv
authentication password smv050859
authentication chap
connect
up
!
ip dhcp pool _WEBADMIN
range 172.16.1.33 20
dns-server 172.16.1.1
default-router 172.16.1.1
!
global Switch/VLAN2
global L2TP0
ip nat Switch/VLAN1
service dhcp
service dns-proxy
service http
service telnet

```

Несколько беспроводных сетей и VLAN с тегом

Требуется сделать три беспроводные сети:

- с защищенным доступом для сотрудников предприятия, SSID «Example Services Inc.»
- открытая для гостей, SSID «Guest Access»
- с защищенным доступом для беспроводных камер видеонаблюдения, SSID «Cameras»

Трафик из беспроводных сетей передается по кабелю в виде трех VLAN с номерами 100, 101 и 102 соответственно. Все VLAN передаются с тегом через порт 5.

Отдельно есть VLAN с номером 1, который используется для управления устройством. Он передается с тегом через порт 5 и без тега — через порт 1 для непосредственного подключения к устройству. На интерфейсе управления настроен IP-адрес 172.16.1.15/24, маршрутизация отключена. Остальные интерфейсы не имеют IP-адресов и работают в режиме моста.

```
interface Switch0
  port 1
  mode access
  access vlan 1
  !
  port 5
  mode trunk
  trunk vlan 1
  trunk vlan 100
  trunk vlan 101
  trunk vlan 102
  !
  up
  !
interface WifiMaster0/AccessPoint0
  security-level public
  authentication wpa-psk sdfWEAgfjcXoiu3ivo83987v987xi3Iu
  encryption enable
  encryption wpa2
  ssid "Example Services Inc."
  up
  !
interface WifiMaster0/AccessPoint1
  security-level public
  ssid "Guest Access"
  up
  !
interface WifiMaster0/AccessPoint2
  security-level public
  authentication wpa-psk id309Vc0Ledv0Ldpoirp)llvvLddkpee
  encryption enable
  encryption wpa2
  ssid "Cameras"
  up
  !
interface Switch0/VLAN1
  description "Management VLAN"
  ip address 172.16.1.15/24
  security-level private
  up
  !
interface Switch0/VLAN100
  description "WPA2 protected VLAN"
  security-level public
  up
  !
interface Switch0/VLAN101
  description "Guest VLAN"
  security-level public
  up
  !
interface Switch0/VLAN102
  description "Surveillance VLAN"
  security-level public
  up
  !
interface Bridge0
  include Switch0/VLAN100
  include WifiMaster0/AccessPoint0
  up
  !
interface Bridge1
  include Switch0/VLAN101
  include WifiMaster0/AccessPoint1
```

```
up
!  
interface Bridge2  
  include Switch0/VLAN102  
  include WifiMaster0/AccessPoint2  
up  
!  
ip route default 172.16.1.1  
user admin  
  password md5 553de4d6e06ee424cd68ec66a39e5b78  
!  
service telnet
```