**Теоретическая часть для выполнения лабораторной работы №1 «Создание простой сети»**

# Навигация по операционной системе IOS

## Режимы работы операционной системы CISCO IOS

После того, как сетевой специалист установит соединение с устройством, он может начать его настройку. Сетевой специалист должен переключаться между различными режимами IOS. Режимы CISCO IOS для коммутаторов и маршрутизаторов весьма похожи. Интерфейс командной строки (CLI) использует иерархическую структуру для режимов.

В иерархическом порядке режимов от базового до наиболее специализированного основными режимами являются:

1. Пользовательский режим

2. Привилегированный режим

3. Режим глобальной конфигурации

Другие специальные режимы конфигурации, такие как режим конфигурации интерфейса

В каждом режиме есть отличительная командная строка, которая используется для выполнения определённых задач с определённым набором команд, доступным только в этом режиме. Например, режим глобальной конфигурации позволяет техническому специалисту задавать на устройстве общие настройки, например, назначить устройству имя. При этом, если сетевому специалисту необходимо настроить, например, параметры безопасности на конкретном порте коммутатора, ему потребуется использовать другой режим. В этом случае следует войти в режим конфигурации интерфейса для этого конкретного порта. Все настройки, вводимые в режиме конфигурации интерфейса, применяются только к этому порту.

Для обеспечения безопасности можно настроить иерархическую структуру. Для каждого режима в иерархии могут требоваться разные процедуры аутентификации. Это позволяет контролировать уровень доступа, которым обладают сетевые специалисты.

## Основные режимы

Основными режимами являются пользовательский и привилегированный. Осуществляя функции защиты, ПО CISCO IOS разделяет сессии режимов на два уровня доступа.

**Пользовательский режим**

Функциональные возможности пользовательского режима ограничены, при этом он эффективно выполняет некоторые базовые операции. Пользовательский режим находится на базовом уровне иерархической структуры режимов. Это первый режим, в котором пользователь начинает работу при входе в интерфейс командной строки (CLI) устройства IOS.

Пользовательский режим позволяет выполнять ограниченное количество базовых команд. Этот режим часто называют «режимом для просмотра». В пользовательском режиме запрещается выполнять команды, которые могут изменить параметры устройства.

По умолчанию для входа в пользовательский режим из консоли аутентификация не требуется. Однако во время начальной конфигурации рекомендуется настроить процедуру аутентификации.

Пользовательский режим определяется с помощью команды интерфейса командной строки, оканчивающейся символом «>». Следующий пример демонстрирует символ «>» в командной строке:

Switch>

**Привилегированный режим**

Для выполнения команд конфигурации и управления сетевой администратор должен использовать привилегированный режим или более специализированный режим в иерархии. Это означает, что сначала пользователю нужно войти в пользовательский режим, а из него — в привилегированный режим.

Привилегированный режим можно определить с помощью командной строки, оканчивающейся символом «#».

Switch#

По умолчанию для привилегированного режима аутентификация не требуется. Рекомендуется убедиться в настройке аутентификации.

Привилегированный режим открывает доступ к режиму глобальной конфигурации и ко всем другим более конкретным режимам настройки. В последнем разделе данной главы мы рассмотрим конфигурацию устройств и некоторые режимы конфигурации.

## Режим глобальной конфигурации и дополнительные режимы

Привилегированный режим открывает доступ к режиму глобальной конфигурации и ко всем другим более конкретным режимам настройки.

**Режим глобальной конфигурации**

Основной режим конфигурации называется глобальным режимом конфигурации. В режиме глобальной конфигурации выполняются изменения конфигурации интерфейса командной строки (CLI), влияющие на работу устройства в целом. Перед доступом к специализированным режимам конфигурации нужно войти в режим глобальной конфигурации.

Чтобы перевести устройство из привилегированного режима в режим глобальной конфигурации и выполнить ввод команд конфигурации из терминала, используется следующая команда интерфейса командной строки:

Switch# configure terminal

После ввода команды командная строка изменяется таким образом, чтобы показать, что он находится в режиме глобальной конфигурации.

Switch(config)#

**Специальные режимы конфигурации**

Из режима глобальной конфигурации пользователь может перейти в различные режимы конфигурации для подкоманд. Каждый из этих режимов позволяет выполнить настройку параметров конкретной области или функции устройства с операционной системой IOS. Ниже приведены некоторые из них:

* Режим конфигурации интерфейса предназначен для настройки одного из сетевых интерфейсов (Fa0/0 (S0/0/0)
* Режим конфигурации линии предназначен для настройки одной из физических или виртуальных линий (консоль, AUX, VTY)

Чтобы вернуться в режим глобальной конфигурации из конкретного режима, введите exit в командной строке. Чтобы окончательно выйти из режима конфигурации и вернуться в привилегированный режим, введите end или воспользуйтесь комбинацией клавиш Ctrl-Z.

**Командные строки**

При использовании интерфейса командной строки (CLI) режим определяется по командной строке, которая является уникальной для каждого режима. По умолчанию каждая командная строка начинается с имени устройства. После имени следует остаток командной строки, который определяет режим. Например, запрос по умолчанию для режима глобальной конфигурации на коммутаторе выглядит так:

Switch(config)#

## Навигация между режимами IOS

**Навигация между пользовательским и привилегированным режимами**

Команды enable и disable используются для переключения интерфейса командной строки (CLI) между пользовательским и привилегированным режимами соответственно.

Чтобы получить доступ к привилегированному режиму, используйте команду enable. Иногда привилегированный режим называют режимом включения (enable).

Синтаксис для ввода enable выглядит так:

Switch> **enable**

Выполнение этой команды не требует какого-либо параметра или ключевого слова. После нажатия клавиши Enter командная строка изменится так:

Switch#

Символ «#» в конце командной строки означает, что коммутатор переключён в привилегированный режим.

Если в привилегированном режиме настроена аутентификация паролем, IOS запросит пароль.

Например:

Switch> **enable**

Password:

Switch#

Для возврата из привилегированного режима в пользовательский используется команда disable.

Например:

Switch# **disable**

Switch>

Команды для доступа к привилегированному режиму и для возврата в пользовательский режим на маршрутизаторе Cisco идентичны тем же командам на коммутаторе Cisco.

**Включение и выключение режима глобальной конфигурации и подрежимов.**

Для выхода из режима глобальной конфигурации и возврата в привилегированный режим введите команду **exit**.

Обратите внимание, что ввод команды **exit** в привилегированном режиме приводит к закрытию сеанса консоли. Это означает, что при вводе команды **exit** в привилегированном режиме вы увидите экран, который открывается при первом запуске сеанса консоли. На этом экране вы должны нажать клавишу Enter, чтобы войти в пользовательский режим.

Для перехода из любого подрежима глобальной конфигурации в следующий режим иерархии введите команду **exit**. Для перемещения из любого подрежима привилегированного режима в привилегированный режим введите команду **end** или используйте сочетание клавиш **Ctrl+Z**.

Для перемещения из любого подрежима глобальной конфигурации в другой «актуальный» подрежим глобальной конфигурации просто введите соответствующие команды, которые обычно вводятся в режиме глобальной конфигурации.

# Команды проверки IOS

Для проверки и устранения неполадок в сети следует проверить работу устройств. Базовая команда для проверки — **show**.

Существует много различных вариантов этой команды. Научившись работать с IOS, вы узнаете, как использовать и интерпретировать выходные данные команд **show**. Используйте команду **show ?** для получения списка доступных команд в рамках указанного контекста или режима.

Типичная команда **show** предоставляет сведения о конфигурации, эксплуатации и состоянии компонентов коммутатора или маршрутизатора Cisco.

В этом курсе мы рассмотрим базовые команды **show**.

Довольно распространённая команда группы **show** — **show interfaces**. Эта команда служит для отображения статистических сведений по всем интерфейсам устройства. Для отображения статистики по определённому интерфейсу введите команду **show interfaces** с указанием типа интерфейса и номера порта (слота). Например:

Switch# **show interfaces fastethernet 0/1**

К дополнительным командам **show**, часто используемым специалистами сети, относятся:

**show startup-config**Отображает сохранённую конфигурацию, расположенную в NVRAM.

**show running-config**Отображает содержимое файла текущей конфигурации.

**Запрос More**

Когда команда показывает больше выходных данных, чем может отобразить экран, внизу экрана появляется окно**More**. В случае появления запроса **--More--** нажмите **Пробел** для просмотра следующей части выходных данных. Чтобы просмотреть только следующую строку, нажмите клавишу **Enter**. При нажатии любой другой клавиши выходные данные отменяются, а пользователь возвращается к командной строке.

К числу наиболее часто используемых команд коммутатора или маршрутизатора относятся:

Switch# **show version**

Отображает сведения о загруженной версии IOS, а также данные об устройстве и аппаратном обеспечении. Если выполнен удалённый вход в маршрутизатор или коммутатор, команда **show version** поможет быстро узнать полезную информацию об устройстве, к которому вы присоединились. Данная команда выводит следующие данные:

* **Software version**— версия программного обеспечения IOS (хранится во флеш памяти)
* **Bootstrap version** — версия программы начальной загрузки (хранится в загрузочном ПЗУ)
* **System up-time**— время с момента последней перезагрузки
* **System restart info**— способ перезапуска (например, цикл включения-выключения, сбой системы)
* **Software image name** — имя файла образа IOS, хранящегося во флеш памяти
* **Router type and processor type** — номер модели и тип процессора
* **Memory type and allocation (shared/main)**— ОЗУ главного процессора и буферизация ввода/вывода пакета
* **Software features** — поддерживаемые протоколы/наборы функций
* **Hardware interfaces** — доступные на устройстве интерфейсы
* **Configuration register**— спецификации загрузки, настройка скорости консоли и других параметров

# Имена узлов

Сетевые администраторы распознают устройства по сети или через Интернет именно с помощью имен узлов.

В соответствии с руководствами по обозначению имена должны:

* начинаться с буквы
* не содержать пробелов
* оканчиваться на букву или цифру
* содержать только буквы, цифры и тире
* содержать не более 64 символов

**Настройка имени узла IOS**

Из привилегированного режима перейдите в режим глобальной конфигурации с помощью команды **configure terminal**:

Switch# **configure terminal**

После ввода команды командная строка будет содержать следующее:

Switch(config)#

В режиме глобальной конфигурации введите имя узла:

Switch(config)# **hostname Sw-Floor-1**

После ввода команды командная строка будет содержать следующее:

Sw-Floor-1 (config)#

Обратите внимание, что узел отображается в окне запроса. Для выхода из режима глобальной конфигурации используйте команду **exit**.

Каждый раз, когда добавляется или изменяется устройство, должна обновляться документация. В этой документации устройствам должны быть присвоены своё местоположение, назначение и адрес.

**Примечание**. Чтобы отменить действие команды, введите перед ней ключевое слово **no**.

Например, чтобы удалить имя устройства, потребуется следующая команда:

Sw-Floor-1 (config)# **no hostname**

Switch(config)#

Обратите внимание, что команда **no hostname** вернула имя коммутатора по умолчанию — «Switch».

# Ограничение доступа к файлам конфигурации устройств

## Защита доступа к устройствам

Рекомендуется физически ограничивать доступ к сетевым устройствам, размещая их в отдельных помещениях или в закрытых шкафах. Тем не менее, пароли остаются основным средством защиты от несанкционированного доступа к сетевым устройствам. На каждом устройстве, даже на домашних маршрутизаторах, должны быть установлены пароли для ограничения доступа. Позже мы узнаем, как усилить защиту, настроив запрос имени пользователя вместе с паролем. На данный момент мы рассмотрим базовые меры безопасности, используя только пароли.

Как отмечалось ранее, для обеспечения безопасности устройство IOS использует иерархические режимы. Для усиления защиты IOS может потребовать несколько паролей, чтобы разрешать доступ к разным уровням иерархии.

К приведённым здесь типам паролей относятся:

* **Пароль привилегированного режима** — ограничивает доступ в привилегированный режим
* **Секретный пароль** — зашифрованный пароль, ограничивающий доступ в привилегированный режим
* **Пароль консоли** — ограничивает доступ к устройствам через консольное подключение
* **Пароль для VTY** — ограничивает доступ к устройствам через Telnet

Рекомендуется использовать различные пароли аутентификации для каждого из уровней доступа. Несмотря на то, что вход в систему с несколькими различными паролями неудобен, это необходимая мера защиты инфраструктуры сети от несанкционированного доступа.

Кроме того, используйте надёжные пароли, которые сложно подобрать. Использование ненадёжных паролей или тех, которые легко подобрать, по-прежнему представляет серьёзную угрозу безопасности во многих сферах бизнеса.

При выборе пароля примите во внимание следующие основные моменты.

* Используйте пароли длиной более 8 символов.
* Используйте сочетание прописных и заглавных букв, чисел, специальных знаков и/или числовых последовательностей.
* На разных устройствах рекомендуется использовать разные пароли.
* Не следует использовать общеупотребительные слова, такие как «пароль» или «администратор», так как их легко подобрать.

## Защита доступа к привилегированному режиму

Для защиты доступа к привилегированному режиму используйте команду **enable secret***password*. Устаревшая, менее безопасная версия этой команды — **enable password***password*. Хотя для настройки аутентификации перед доступом в привилегированный режим подходят обе эти команды, рекомендуется использовать **enable secret**. Команда  **enable secret** обеспечивает более высокий уровень безопасности, поскольку пароль зашифрован.

Пример команды для установления паролей:

Switch(config)# **enable secret class**

## Защита доступа к пользовательскому режиму

Консольный порт сетевых устройств необходимо защитить как минимум надёжным паролем. Это снижает вероятность доступа неавторизованных сотрудников, которые включают кабель и пытаются получить доступ к устройству.

Чтобы установить пароль для консоли строки в режиме глобальной конфигурации, нужно ввести следующие команды:

Switch(config)# **line console 0**

Switch(config-line)# **password cisco**

Switch(config-line)# **login**

В режиме глобальной конфигурации используется команда **line console 0**, чтобы войти в режим конфигурации строки для консоли. Ноль используется для обозначения первого (а в большинстве случаев — единственного) интерфейса консоли.

Вторая команда —**password cisco** определяет пароль для консоли строки.

Команда **login** настраивает коммутатор для аутентификации при входе в систему. Если включена процедура входа и настроен пароль, пользователь консоли должен будет ввести пароль, чтобы получить доступ к интерфейсу командной строки (CLI).

**Пароль для VTY**

Каналы VTY обеспечивают доступ к устройствам Cisco по протоколу Telnet. По умолчанию многие коммутаторы Cisco поддерживают до 16 каналов VTY, пронумерованных от 0 до 15. Количество каналов VTY, поддерживаемых на маршрутизаторе Cisco, зависит от типа маршрутизатора и версии IOS. Но чаще всего установлены пять каналов VTY. Эти каналы пронумерованы от 0 до 4 по умолчанию, хотя можно настроить дополнительные каналы. Пароль нужно установить для всех доступных каналов VTY. Для всех соединений можно установить один пароль. При этом часто возникает необходимость задать уникальный пароль для одного канала, чтобы обеспечить администратору резервный доступ в том случае, если все остальные соединения заняты.

Команды, используемые для назначения пароля каналов VTY:

Switch(config)# **line vty 0 15**

Switch(config-line)# **password cisco**

Switch(config-line)# **login**

По умолчанию в IOS встроена команда **login**на каналах VTY. Это предотвращает доступ по протоколу Telnet к устройству без аутентификации. Если по ошибке была введена команда **no login**, из-за чего была снята аутентификация, по протоколу Telnet к сети могут присоединиться неавторизованные пользователи. Это представляет определённую угрозу безопасности.

## Шифрование пароля

Ещё одна важная команда, которая защищает пароль во время просмотра файлов конфигурации. Это **service password-encryption**.

Эта команда шифрует пароли во время их настройки. Команда**service password-encryption**шифрует все незашифрованные пароли. Шифрование применяется только к паролям в файле конфигурации, но не к паролям, которые отправлены по среде передачи данных. Эта команда не позволяет неавторизованным сотрудникам прочитать пароль.

Если выполнить команды**show running-config**или**show startup-config** до выполнения команды**service password-encryption**, то незашифрованные пароли будут видны в выходных данных конфигурации. Затем можно выполнить команду service password-encryption, после чего пароли будут зашифрованы. После этого шифрование нельзя будет отменить.

## Баннерные сообщения

Несмотря на то, что пароли защищают сеть от неавторизованных пользователей, необходимо использовать уведомления о том, что лишь авторизованным пользователям можно получить доступ к устройству. Для этого нужно добавить баннер в выходные данные устройства.

Баннеры могут пригодиться во время судебного процесса, если пользователь был обвинён в неразрешенном доступе. В некоторых системах правосудия не разрешено судебное преследование или слежение за пользователями без предупреждения.

Точное содержание или формулировка баннера зависят от местного законодательства и корпоративной политики. Ниже представлены примеры формулировок, которые могут содержаться в таких информационных баннерах:

* «Доступ к устройству разрешён только для авторизованных пользователей».
* «Действия могут отслеживаться».
* «Любые попытки неавторизованного использования будут преследоваться по закону».

Поскольку баннеры видит каждый, кто пытается получить доступ к устройству, сообщение необходимо тщательно сформулировать. Не следует использовать в формулировке выражения типа «Добро пожаловать» или нечто подобное. Если пользователь нарушает работу сети после незаконного проникновения, при наличии приветственных слов сложно будет доказать преступление.

Создать баннеры не трудно, но их текст необходимо тщательно продумать. Баннер не должен приглашать каждого пользователя получить доступ к устройству. В нём необходимо указать, что только авторизованные пользователи могут получить доступ к устройству. Кроме того, баннер может содержать расписание отключений системы и другие сведения, которые могут быть полезны другим пользователям сети.

IOS предоставляет множество типов баннеров. Сообщение текущего дня — достаточно распространенный баннер. Часто используется для законного уведомления, так как его видят все присоединённые терминалы.

Настройте сообщение текущего дня с помощью команды **banner motd** в режиме глобальной конфигурации.

Для использования команды **banner motd** необходимы разграничители, чтобы можно было распознать содержимое баннерного сообщения. После команды **banner motd** следуют пробел и разделительный символ. Затем вводится одна или более строк текста для создания баннерного сообщения. Второй разделительный символ означает конец сообщения. Разграничительным символом может быть любой символ, которого нет в данном сообщении. Поэтому часто используются такие символы, как «#».

Для настройки сообщения текущего дня в режиме глобальной конфигурации используйте следующий синтаксис:

Switch(config)# **banner motd #***message* **#**

После выполнения команды баннер будет показан при всех последующих попытках доступа к устройству, пока он не будет удалён.

# Сохранение конфигурации

Файл текущей конфигурации отражает текущую конфигурацию, функционирующую на устройстве CISCO IOS. Он содержит команды, используемые для определения принципов работы устройства в сети. Изменения текущей конфигурации незамедлительно влияют на работу устройства Cisco.

Файл текущей конфигурации хранится в рабочей памяти устройства или в оперативном запоминающем устройстве (ОЗУ). Это означает, что файл текущей конфигурации временно активен, когда работает устройство Cisco (подключено к питанию). Однако при отключении питания устройства или перезапуске устройства все несохранённые изменения конфигурации будут потеряны.

После внесения изменений в файл текущей конфигурации следует рассмотреть следующие варианты действий.

* Вернуть устройство к исходной конфигурации.
* Удалить все внесённые изменения.
* Сделать изменённую конфигурацию новой начальной конфигурацией.

Файл загрузочной конфигурации отображает конфигурацию, которая будет применена на устройстве после перезагрузки. Файл загрузочной конфигурации хранится в энергонезависимой памяти (NVRAM). После настройки сетевого устройства и изменения текущей конфигурации важно сохранить эти изменения в файл загрузочной конфигурации. Это предотвращает потери изменений вследствие сбоя питания или случайной перезагрузки.

Перед внесением изменений воспользуйтесь соответствующими командами **show** для проверки работоспособности устройства. Как показано на рисунке, команду **show running-config** можно использовать для просмотра файла текущей конфигурации. Когда изменения проверены, используйте команду **copy running-config startup-config** в командной строке привилегированного режима. Команда для сохранения файла текущей конфигурации в файл загрузочной конфигурации выглядит так:

Switch# **copy running-config startup-config**

После выполнения команды файл текущей конфигурации обновляет файл загрузочной конфигурации.

Если изменения, внесённые в ходе конфигурации, не принесли желаемого результата, возможно, понадобится восстановить предыдущую конфигурацию устройства. Если мы не переписывали начальную конфигурацию с изменениями, текущую конфигурацию можно заменить начальной. Лучше всего это осуществляется путём перезапуска устройства и ввода команды **reload** в командной строке привилегированного режима.

Выполняя перезагрузку, IOS определит, что изменённая конфигурация не была сохранена в файл начальной конфигурации. IOS запросит, нужно ли сохранить изменения. Для отмены изменений введите **n** или **no**.

Для подтверждения перезагрузки появится дополнительный запрос. Для подтверждения нажмите Enter. Нажатие любой другой клавиши приведёт к преждевременному завершению данного процесса.

Чтобы удалить файл загрузочной конфигурации, введите команды **erase NVRAM: startup-config** или **erase startup-config** в командную строку привилегированного режима:

Switch# **erase startup-config**

После ввода команды появится запрос о подтверждении:

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Ответ по умолчанию — «Подтверждаю». Для подтверждения и удаления файла загрузочной конфигурации нажмите клавишу Enter. Нажатие любой другой клавиши приведёт к преждевременному завершению данного процесса.

**Внимание**. Будьте внимательны при использовании команды **erase**. Эту команду можно использовать для удаления любого файла в устройстве. Неправильное использование этой команды может привести к удалению самой IOS или других важных файлов.

Кроме того, на коммутаторе необходимо выполнить команду **delete vlan.dat** в дополнение к команде **erase startup-config**, чтобы вернуть конфигурацию, «встроенную» по умолчанию (соответствующую установленной на предприятии):

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

После удаления начальной конфигурации из NVRAM (и удаления файла vlan.dat из коммутатора) перезапустите устройство, чтобы удалить файл текущей конфигурации из ОЗУ. Затем устройство загрузит файл начальной конфигурации, встроенной по умолчанию, в текущую конфигурацию.

# Адресация устройств

## Настройка виртуального интерфейса коммутатора

Для удалённого доступа к коммутатору на виртуальном интерфейсе коммутатора нужно настроить IP-адрес и маску подсети:

* **IP-адрес** — совместно с маской подсети идентифицирует оконечное устройство в сетевом взаимодействии
* **Маска подсети** — определяет, какая часть крупной сети используется IP-адресом

В данный момент основное внимание фокусируется на адресах IPv4. Адреса IPv6 подробно рассмотрим позже.

Впоследствии вы поймете важность IP-адресов, но в данный момент необходимо научиться быстро настраивать коммутатор для поддержки удалённого доступа. Ниже приведены команды для активации IP соединения с коммутатором S1 при помощи IP-адреса 192.168.10.2:

Switch(config)# **interface vlan 1**

Switch(config**-**if)# **ip address 192.168.10.2 255.255.255.0**

Switch(config**-**if)# **no shutdown**

* **interface vlan 1** - применяется для перехода в режим настройки интерфейса из режима глобальной конфигурации
* **ip address 192.168.10.2 255.255.255.0** - настраивает IP-адрес и маску подсети для коммутатора (только одно из нескольких возможных сочетаний IP-адреса и маски подсети)
* **no shutdown** - активирует интерфейс

После настройки этих команд все IP-элементы в коммутаторе будут готовы для передачи данных по сети.

**Примечание**. Для удалённого управления коммутатора по-прежнему необходима настройка одного или нескольких физических портов, а также каналов VTY.