**Сетевая операционная система IOS**

**1. Основные понятия**

Операционная система сетевого взаимодействия Cisco (IOS) — это общий термин для группы сетевых операционных систем, используемых на сетевых устройствах Cisco. Операционная система Cisco IOS используется в большинстве устройств Cisco, независимо от их типа и размеров. Наиболее распространённый способ доступа к этим устройствам — использование интерфейса командной строки (CLI).

Последней версией CISCO IOS является версия 15.x.

Размер самого файла IOS составляет несколько мегабайт и хранится в полупостоянной памяти, которая называется флэш-памятью. Флэш-память обеспечивает энергонезависимое хранение данных.

При подключении к сети IOS копируется из флеш памяти в оперативное запоминающее устройство (ОЗУ). Затем, при работе устройства, IOS запускается из ОЗУ, которая считается энергозависимой памятью, поскольку данные теряются во время отключения питания.

Примечание:

Операционная система на домашних маршрутизаторах обычно называется микропрограммой. Наиболее распространенный способ настройки домашнего маршрутизатора — доступ к графическому интерфейсу через веб-браузер. На большинстве домашних маршрутизаторов при появлении новых функций или уязвимых мест в безопасности активируется обновление микропрограмм.

**2. Доступ к устройству Cisco IOS**

Доступ к сервисам, предоставляемым CISCO IOS, обычно осуществляется с помощью интерфейса командной строки (CLI).

Существует несколько способов доступа к среде интерфейса командной строки:

* Консоль
* Telnet или SSH
* Порт AUX

**Консоль**

Консольный порт — это порт управления, обеспечивающий возможность внеполосного доступа к устройству Cisco. Внеполосный доступ — это доступ через выделенный административный канал, который используется исключительно в целях технического обслуживания устройства. Преимущество использования порта консоли состоит в том, что доступ к устройству возможен даже без настройки сетевых услуг, например, начальной конфигурации сетевого устройства. При выполнении начальной конфигурации компьютер, подключается к порту консоли устройства с помощью специального кабеля и запускается программа эмуляции терминала для настройки сетевого оборудования. Команды конфигурации для настройки коммутатора или маршрутизатора можно ввести на подключённом компьютере.

Консольный порт также можно использовать, когда работа сетевых сервисов нарушена и удалённый доступ к устройству на базе CISCO IOS невозможен. В этом случае подключение к консольному порту позволяет компьютеру определять состояние устройства. По умолчанию с помощью консольного соединения можно наблюдать загрузку сетевого устройства, осуществлять устранение неполадок, просматривать сообщения об ошибках. После того как сетевой специалист подключился к устройству, он может выполнить все необходимые команды конфигурации с помощью сеанса консоли.

**Telnet**

Telnet — это способ удалённого установления сеанса интерфейса командной строки через виртуальный интерфейс по сети. В отличие от консольного подключения, для сеансов Telnet требуются активные сетевые сервисы на устройстве. В сетевом устройстве должен быть настроен хотя бы один активный интерфейс с интернет-адресом, например, с адресом IPv4.

**SSH**

Протокол Secure Shell (SSH) предоставляет удалённый вход в систему аналогично Telnet, за исключением того, что он использует более безопасные сетевые службы. Протокол SSH предоставляет более высокий уровень аутентификации на основе пароля, чем протокол Telnet, и при передаче информации о сеансе использует шифрование. Это защищает данные пользователя, пароль и сведения о сеансе управления. По возможности рекомендуется использовать SSH вместо протокола Telnet.

**AUX**

Устаревший метод установления сеанса интерфейса командной строки — с помощью коммутируемого соединения по телефону к вспомогательному порту (AUX) маршрутизатора. Аналогично с подключением консоли вспомогательный метод также обеспечивает внеполосное подключение и не требует настройки или наличия каких-либо сетевых сервисов. Если работа сетевых сервисов была нарушена, удалённый администратор может получить доступ к коммутатору или маршрутизатору по телефонной линии.

Для подключения к сетевому устройству используются программы эмуляции терминала:

PuTTY

Tera Term

SecureCRT

HyperTerminal

Terminal OS X и другие.

**3. Навигация по операционной системе IOS**

Интерфейс командной строки IOS использует иерархическую структуру, к которой относятся следующие режимы:

* Пользовательский
* Привилегированный
* Режим глобальной конфигурации
* Другие специальные режимы конфигурации, такие как режим конфигурации интерфейса.

**Пользовательский режим**

Это первый режим, в котором пользователь начинает работу при входе в IOS.

Пользовательский режим позволяет выполнять ограниченное количество базовых команд. Этот режим часто называют «режимом для просмотра». Командная строка в этом режиме имеет вид, например:

Switch>

**Привилегированный режим**

Для выполнения команд конфигурации и управления сетевой администратор должен использовать привилегированный режим. Для доступа к привилегированному режиму, используется команда **enable**.

Switch> **enable**

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.

**Режим глобальной конфигурации**

Основной режим конфигурации называется глобальным режимом конфигурации. В режиме глобальной конфигурации выполняются изменения конфигурации интерфейса командной строки, влияющие на работу устройства в целом.

Для перевода устройства в режим глобальной конфигурации используется команда:

Switch# **configure terminal**

После этого командная строка принимает следующий вид:

Switch(config)#

**Специальные режимы конфигурации**

Из режима глобальной конфигурации можно перейти в различные режимы конфигурации для подкоманд. Каждый из этих режимов позволяет выполнить настройку параметров конкретной области или функции устройства с операционной системой IOS. К ним относятся:

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

Чтобы вернуться в режим глобальной конфигурации из конкретного режима, используется команда **exit**. Чтобы вернуться в привилегированный режим, используется команда **end** или комбинация клавиш **Ctrl-Z**.

**4. Справочная система IOS**

В операционной системе IOS предусмотрены несколько доступных видов справки:

* Контекстная справка
* Проверка синтаксиса команды

**Контекстная справка**

Контекстная справка предоставляет список команд и параметров, связанных с этими командами в контексте текущего режима. Для доступа к контекстной справке введите вопросительный знак (**?**) в любой командной строке. Последует немедленный ответ даже без нажатия клавиши Enter.

**5. Горячие клавиши и клавиши быстрого вызова**

Интерфейс командной строки (CLI) IOS предусматривает горячие клавиши и клавиши быстрого вызова, которые упрощают процесс настройки, мониторинга, поиска и устранения неполадок.

**Горячие клавиши:**

* **Стрелка вниз** — позволяет пользователю пролистывать предыдущие команды вперед
* **Стрелка вверх** — позволяет пользователю пролистывать предыдущие команды назад
* **Tab** — завершает частично набранную команду или ключевое слово
* **Ctrl-А** — перемещает в начало строки
* **Ctrl-Е** — перемещает в конец строки
* **Ctrl-R** — обновляет строку
* **Ctrl-Z** — выходит из режима конфигурации и возвращает в пользовательский режим
* **Ctrl-C** — выходит из режима конфигурации или прерывает текущую команду
* **Ctrl-Shift-6** — позволяет пользователю прервать процесс IOS, например, ping или traceroute.

**6. Сокращённые команды или ключевые слова**

Команды и ключевые слова можно сократить до минимального количества символов, которые останутся уникальными. Например, команду **configure** можно сократить до **conf**, поскольку **configure** — это единственная команда, которая начинается с символов **conf**. Сокращение **con** не подходит, так как с символов **con** начинается несколько команд.

Ключевые слова также можно сокращать.

Например, **show interfaces** можно сократить следующим образом:

Switch# **show interfaces**

Switch# **show int**

Можно сокращать как команды, так и ключевые слова.

Например:

Switch# **sh int**

**Запрос More**

Когда команда показывает больше выходных данных, чем может отобразить экран, внизу экрана появляется окно **More**. В случае появления запроса **--More—**нажимается **Пробел** для просмотра следующей части выходных данных. Чтобы просмотреть только следующую строку, нажимается клавиша **Enter**.

**7. Имена узлов**

Один из первых шагов при настройке сетевого устройства — это назначение уникального имени устройства или узла. Узлы отображаются в окнах интерфейса командной строки и используются в различных процессах аутентификации между устройствами. Их нужно использовать в топологических схемах.

Имена узлов настраиваются на активном сетевом устройстве. Если имя устройства не задано, CISCO IOS использует имя, назначенное по умолчанию производителем.

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

В именах узлов, используемых в устройствах IOS, сохраняются все прописные и строчные символы. Поэтому использовать прописные буквы можно так же, как и всегда. Этот метод отличается от большинства способов назначения имён в Интернете, в которых нет различий между прописными и строчными буквами.

**Настройка имени узла IOS**

Настройка имени узла осуществляется в режиме глобальной конфигурации с помощью команды **configure terminal**.

Например:

Switch# **configure terminal**

После ввода команды вводится имя узла.

Например:

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

После ввода имени командная строка будет содержать следующее:

Sw-Floor-1 (config)#

Чтобы отменить действие команды, вводится ключевое слово **no**.

Sw-Floor-1 (config)# **no hostname**

Switch(config)#

**8. Ограничение доступа к файлам конфигурации устройств**

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. Для усиления защиты IOS может потребовать несколько паролей, чтобы разрешать доступ к разным уровням иерархии.

К основным 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.

При выборе пароля необходимо принимать во внимание следующие основные моменты.

* Пароль должен быть длиной более 8 символов.
* Использование сочетаний 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.

Для защиты доступа к привилегированному режиму используется команда **enable secret** *password*. Команда **enable secret** обеспечивает высокий уровень безопасности, поскольку пароль зашифрован.

Пример команды для установления паролей:

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

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**

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.

**Пароль для VTY**

Команды, используемые для назначения пароля каналов VTY:

Switch(config)# **line vty 0 15**

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

Switch(config-line)# **login**

Команда, которая защищает пароль во время просмотра файлов конфигурации: **service password-encryption**. Эта команда шифрует пароли во время их настройки.

**Баннеры**

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.

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

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

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

**9. Сохранение конфигураций**

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 несохраненные изменения конфигурации будут потеряны.

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.

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.

Для восстановления предыдущей конфигурации устройства осуществляется его перезапуск путём ввода команды **reload** в командной строке привилегированного режима.

Если нежелательные изменения сохранены в файл начальной конфигурации, возможно, понадобится очистить все конфигурации. Для этого нужно удалить начальную конфигурацию и перезапустить устройство.

Начальную конфигурацию можно удалить с помощью команды **erase startup-config**.

Например:

Switch# **erase startup-config**

**10. Тестирование оконечных и сетевых устройств**

**Тестирование логического интерфейса Loopback**

Для проверки внутренней IP-конфигурации на локальном узле используется команда **ping**. Это тестирование выполняется с помощью команды **ping** на зарезервированном loopback-адресе (127.0.0.1). Loopback-адрес, 127.0.0.1, определяется протоколом TCP/IP как зарезервированный адрес, который направляет пакеты обратно к узлу.

Команды ping вводятся в командной строке на локальном узле с помощью следующего синтаксиса:

C:\> **ping 127.0.0.1**

**Проверка интерфейсов коммутаторов**

Используется команда **show ip interface brief**.

**Тестирование соединения между ПК и коммутатором**

Команду **ping** можно использовать на ПК так же, как и на устройстве CISCO IOS.