Глава 2: Настройка сетевой операционной системы 2.0.1.1 Знакомство с операционной системой Cisco IOS

Домашние сети, как правило, соединяют широкий спектр оконечных устройств, включая ПК, ноутбуки, планшетные компьютеры, смартфоны, интеллектуальные, цифровые медиа-плееры сети (DLNA), такие как Xbox 360 или PlayStation 3, а также многие другие устройства.

Все эти оконечные устройства обычно подключаются к домашнему маршрутизатору. Домашние маршрутизаторы — это фактически четыре устройства в одном:

* **Маршрутизатор** **-** передает и получает пакеты данных из сети Интернет
* **Коммутатор** **-** соединяет оконечные устройства с помощью сетевых кабелей
* **Точка беспроводного доступа** **-**состоит из радиопередатчика, который осуществляет беспроводное соединение оконечных устройств
* **Устройство межсетевого экрана** **-**защищает исходящий и запрещает входящий трафик.

В крупных корпоративных сетях со значительно большим количеством устройств и объёмным трафиком эти устройства часто функционируют как независимые, автономные устройства, обеспечивающие специализированное обслуживание. Оконечные устройства, такие как ПК и ноутбуки, подключаются к сетевым коммутаторам с помощью проводных соединений. Чтобы отправлять пакеты за пределы локальной сети, сетевые коммутаторы подключаются к маршрутизаторам сети. Беспроводные точки доступа и выделенные устройства обеспечения безопасности, например, межсетевой экран — это другие устройства инфраструктуры, находящиеся в сети.

Оборудование, назначение и возможности каждого устройства значительно отличаются. Но в любом случае функционировать устройствам позволяет именно операционная система.

Операционные системы используются на всех оконечных и сетевых устройствах, подключённых к сети Интернет. Устройства конечных пользователей — это смартфоны, планшетные компьютеры, ПК и ноутбуки. Сетевые или промежуточные устройства — это устройства, используемые для передачи данных по сети, а также коммутаторы, маршрутизаторы, точки беспроводного доступа и межсетевые экраны. Операционную систему на сетевом устройстве называют сетевой операционной системой.

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.

Для демонстрации работы Cisco IOS в этой главе мы рассмотрим топологию базового сетевого подключения, которая состоит из двух коммутаторов и двух ПК.

2.1.1.1 Операционные системы

Все оконечные и сетевые устройства, подключенные к сети Интернет, функционируют благодаря операционной системе (ОС).

При включении компьютер загружает ОС в ОЗУ (обычно с диска). Часть кода ОС, которая непосредственно взаимодействует с аппаратным обеспечением компьютера, называется ядром ОС. Часть, которая обеспечивает связь между приложениями и пользователем, называется оболочкой. Пользователь взаимодействует с оболочкой посредством интерфейса командной строки (CLI) или графического интерфейса пользователя (GUI).

При использовании интерфейса командной строки происходит непосредственное обращение к системе в текстовом режиме методом ввода команд с клавиатуры в командную строку. Система выполняет команду, часто выводя выходные данные в текстовом формате. Графический интерфейс обеспечивает взаимодействие с системой в среде, где используются графические изображения, мультимедиа и текст. Действия выполняются с помощью изображений на экране. Графический интерфейс удобнее и не требует таких знаний структуры команд, как интерфейс командной строки. Именно поэтому многие используют графический интерфейс (GUI). В большинстве операционных систем есть оба интерфейса.

Для получения дополнительной информации нажмите на изображение оборудования, ядра ОС и оболочки.

Доступ к большинству операционных систем оконечных устройств осуществляется с помощью графического интерфейса пользователя, включая доступ к MS Windows, MAC OS X, ОС Linux, Apple iOS, Аndroid и другим.

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.

Сетевые устройства инфраструктуры работают на основе сетевой операционной системе. Сетевая операционная система, используемая на устройствах Cisco, называется операционной системой сетевого взаимодействия Cisco (IOS). 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).

В этой главе мы подробно рассмотрим топологию сетевого коммутатора малого бизнеса. Топология состоит из двух коммутаторов и двух ПК. На ней мы продемонстрируем использование CISCO IOS с помощью интерфейса командной строки (CLI).

2.1.1.2 Назначение операционной системы

Сетевые операционные системы во многом похожи на ОС для ПК. Операционная система выполняет набор технических скрытых функций, которые позволяют пользователю:

* использовать мышь;
* просматривать выходные данные на экране монитора;
* вводить текстовые команды;
* выбирать параметры в диалоговом окне.

Скрытые функции коммутаторов и маршрутизаторов очень похожи. IOS на коммутаторе или маршрутизаторе предоставляет интерфейс сетевому специалисту. Технический специалист может ввести определённые команды, чтобы настроить или запрограммировать устройство для выполнения различных сетевых функций. Функциональные возможности IOS отличаются на разных сетевых устройствах в зависимости от назначения устройств и поддерживаемых функций.

Cisco IOS — это термин, который включает в себя ряд различных операционных систем, которые работают на различных сетевых устройствах. Существуют различные виды Cisco IOS:

* IOS для коммутаторов, маршрутизаторов и других сетевых устройств Cisco
* Версии IOS для конкретного сетевого устройства Cisco
* Наборы функций IOS, обеспечивающие определённые пакеты функций и сервисов

Так же, как ПК работает с Microsoft Windows 8 и MacBook работает с OS X, сетевое устройство Cisco функционирует на под управлением определённой версии Cisco IOS. Версия IOS зависит от типа используемого устройства и наиболее значимых функций. Хотя устройства поставляются с ОС и набором функций по умолчанию, можно использовать дополнительные возможности, обновив версию IOS и набор функций.

В этом курсе основное внимание уделено версии 15.x. CISCO IOS. На рис. 1 показан список версий IOS для коммутатора Cisco Catalyst 2960. На рис. 2 показан список версий IOS для маршрутизаторов с интреграцией сервисов Cisco 2911 (ISR).

2.1.1.3 Местоположение операционной системы CISCO IOS

Размер самого файла IOS составляет несколько мегабайт и хранится в полупостоянной памяти, которая называется флеш памятью. На рисунке показана карта флеш памяти. Флеш память обеспечивает энергонезависимое хранение данных. Это означает, что содержимое устройства сохраняется, даже если потеряно питание. Несмотря на то, что содержимое флеш памяти не теряется во время потери питания, при необходимости их можно изменить или перезаписать. Благодаря этому IOS можно обновлять до более новой версии или добавлять новые функциональные возможности без замены оборудования. Кроме того, флеш память можно использовать для одновременного хранения нескольких версий ПО IOS.

Во многих устройствах Cisco при подключении к сети IOS копируется из флеш памяти в оперативное запоминающее устройство (ОЗУ). Затем, при работе устройства, IOS запускается из ОЗУ. ОЗУ обладает множеством функций, включая хранение данных, которые используются устройством для поддержки работы сети. Запуск IOS из ОЗУ повышает производительность устройства, при этом ОЗУ считается энергозависимой памятью, поскольку данные теряются во время отключения питания. Отключение питания может происходить из-за случайной или намеренной перезагрузки.

Количество необходимой флеш памяти и оперативной памяти зависит от версии IOS. Для технического обслуживания сети и планирования крайне важно определить требования флеш памяти и ОЗУ для каждого устройства, включая максимальные конфигурации флеш памяти и ОЗУ. Возможно, новейшие версии IOS могут запросить больше ОЗУ и флеш памяти, чем возможно установить на некоторых устройствах.

2.1.1.4 Функции операционной системы IOS

Специалисты в области сетевого проектирования полагаются именно на функции маршрутизаторов и коммутаторов Cisco IOS, чтобы проектируемые сети функционировали должным образом. К наиболее значимым функциям маршрутизаторов или коммутаторов Cisco относятся:

* обеспечение безопасности сети;
* IP-адресация виртуальных и физических интерфейсов;
* возможность настройки интерфейса для оптимизации подключения соответствующей среды передачи данных;
* маршрутизация;
* настройка технологий качества обслуживания (QoS);
* поддержка технологий управления сетью.

Каждая функция или служба имеет соответствующий набор команд конфигурации, которые позволяют сетевому специалисту её активировать.

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

2.1.2.1 Метод консольного доступа

Существует несколько способов доступа к среде интерфейса командной строки (CLI). Ниже приведены наиболее распространённые методы.

* 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.

Для многих устройств IOS консольное подключение происходит без использования технологий для обеспечения безопасности подключения. При этом для предотвращения несанкционированного доступа к устройствам доступ должен быть защищён паролем. В случае утери пароля существует целый ряд мер, позволяющих получить доступ к данному устройству без пароля. Также устройство должно располагаться в закрытом помещении или аппаратной комнате для предотвращения несанкционированного физического доступа.



2.1.2.2 Методы доступа с помощью Telnet, SSH и AUX

**Telnet**

Telnet — это способ удалённого установления сеанса интерфейса командной строки (CLI) 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. Устройства CISCO IOS включают в себя процесс сервера Telnet, позволяющий пользователям вводить команды конфигурации от клиента Telnet. Кроме поддержки процесса сервера Telnet устройство CISCO IOS также содержит клиент Telnet. Это позволяет администратору сети отправлять запрос по протоколу telnet с интерфейса командной строки (CLI) устройств Cisco любому другому устройству с поддержкой процесса сервера Telnet.

**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.

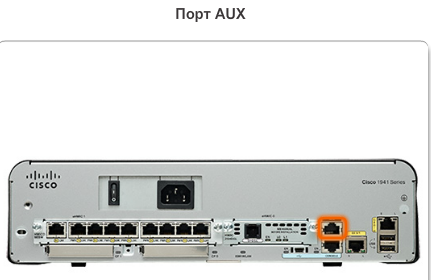
Большинство версий CISCO IOS включают в себя SSH-сервер. В некоторых устройствах эта сетевая служба по умолчанию включена. В других устройствах SSH-сервер требуется включать вручную. Устройства на базе Cisco IOS также содержат SSH-клиент, который можно использовать для установления SSH-сеансов с другими устройствами.

**AUX**

Устаревший метод установления сеанса интерфейса командной строки (CLI) — с помощью коммутируемого соединения по телефону к вспомогательному порту (AUX) маршрутизатора, который выделен на рисунке. 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.

Порт AUX может также использоваться локально, как и консольный порт, с прямым подключением к компьютеру, на котором работает программа эмуляции терминала. При этом консольный порт предпочтительнее порта AUX для поиска и устранения неполадок, так как он по умолчанию отображает сообщения о запуске, устранении неполадок и ошибках.

**Примечание**. Коммутаторы Cisco Catalyst не поддерживают вспомогательное соединение.

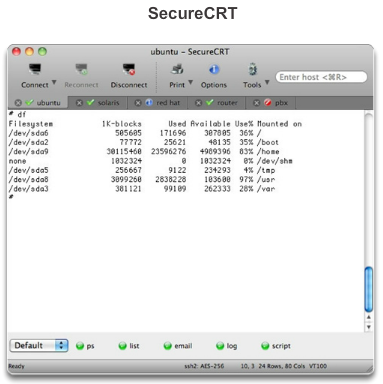
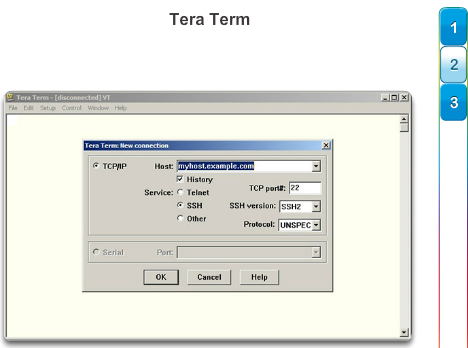
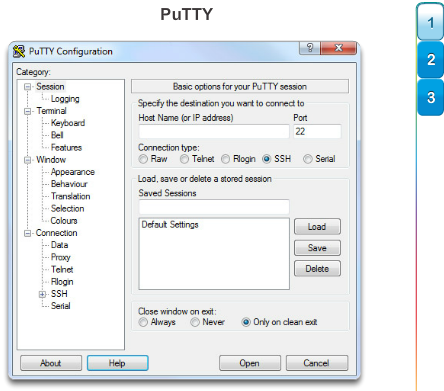


2.1.2.3 Программы эмуляции терминала

Существует множество программ эмуляции терминала, доступных для подключения к сетевому устройству или последовательного подключения через консольный порт или соединение Telnet/SSH. К некоторым из этих программ относятся:

* PuTTY (рис. 1)
* Tera Term (рис. 2)
* SecureCRT (рис. 3)
* HyperTerminal
* Terminal OS X

Эти программы позволяют максимально повысить продуктивность работы за счёт регулировки размеров окна, изменения размера шрифта и изменения комбинации цветов.



2.1.3.1 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.

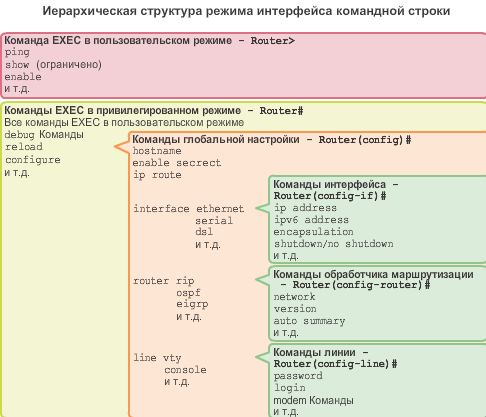
В иерархическом порядке режимов от базового до наиболее специализированного основными режимами являются:

* Пользовательский режим
* Привилегированный режим
* 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.

На рисунке показана структура режимов IOS с использованием стандартных командных строк и функций.



2.1.3.2 Основные режимы

Основными режимами являются пользовательский и привилегированный. Осуществляя функции защиты, ПО CISCO IOS разделяет сессии режимов на два уровня доступа. Как показано на рисунке, привилегированный режим обладает более высоким уровнем прав в возможностях использования устройства.

**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**

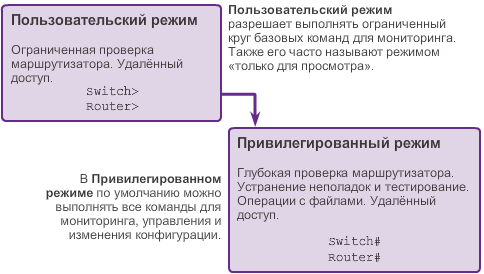
Для выполнения команд конфигурации и управления сетевой администратор должен использовать привилегированный режим или более специализированный режим в иерархии. Это означает, что сначала пользователю нужно войти в пользовательский режим, а из него — в привилегированный режим.

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.



2.1.3.3 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)

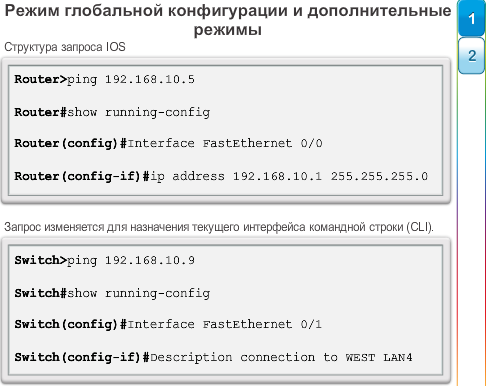
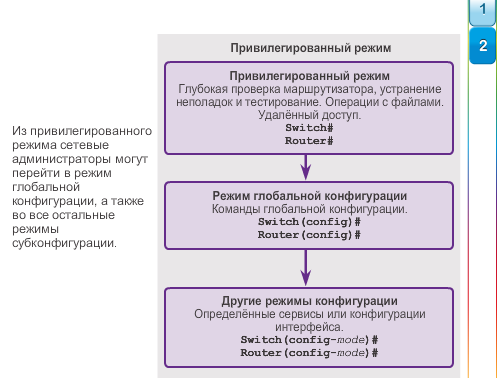
На рис. 1 показаны командные строки для некоторых из этих режимов. Чтобы вернуться в режим глобальной конфигурации из конкретного режима, введите**exit**в командной строке. Чтобы окончательно выйти из режима конфигурации и вернуться в привилегированный режим, введите **end**или воспользуйтесь комбинацией 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)#

По мере выполнения команд и изменения режимов изменяется и командная строка, которая отражает текущие контекстные данные, как показано на рис. 2.



2.1.3.4 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**

Пароль:

Switch#

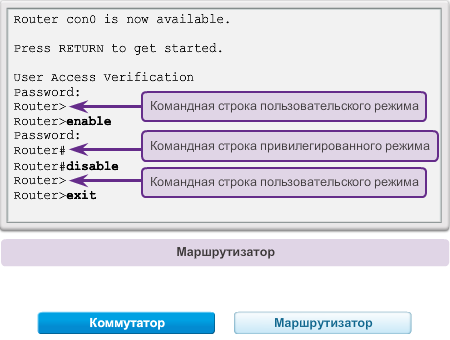
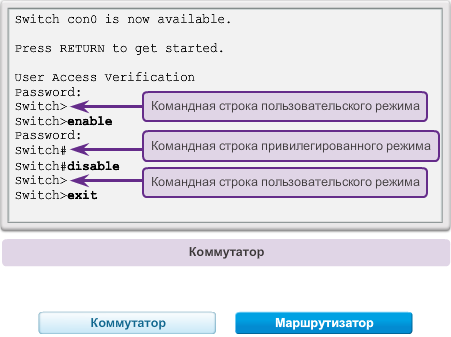
Для возврата из привилегированного режима в пользовательский используется команда **disable**.

Например:

Switch# **disable**

Switch>

Как показано на рисунке, команды для доступа к привилегированному режиму и для возврата в пользовательский режим на маршрутизаторе Cisco идентичны тем же командам на коммутаторе Cisco.



2.1.3.5 Навигация между режимами IOS (продолж.)

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

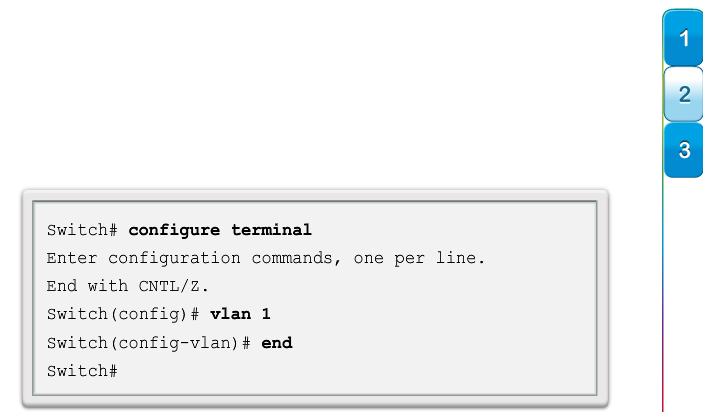
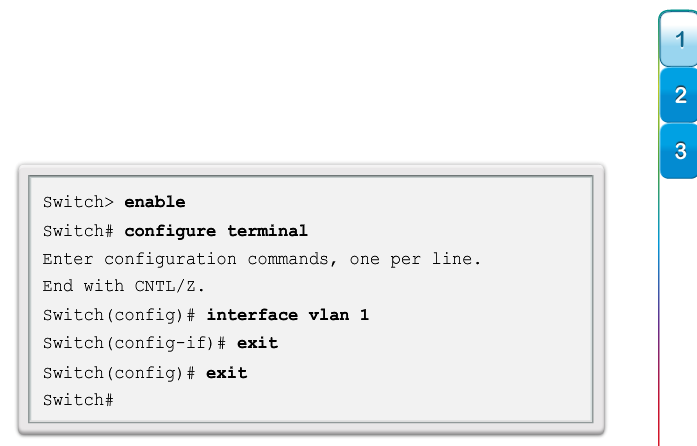
Для выхода из режима глобальной конфигурации и возврата в привилегированный режим введите команду **exit**.

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**. На рис. 1 представлен переход из пользовательского режима в привилегированный, затем переход в режим глобальной конфигурации, режим конфигурации интерфейса, обратно в режим глобальной конфигурации и снова в привилегированный режим с помощью команды **exit**.

Для перемещения из любого подрежима привилегированного режима в привилегированный режим введите команду **end** или используйте сочетание клавиш **Ctrl+Z**. На рис. 2 представлен переход из режима конфигурации виртуальной локальной сети (VLAN) в привилегированный режим с помощью команды **end**.

Для перемещения из любого подрежима глобальной конфигурации в другой «актуальный» подрежим глобальной конфигурации просто введите соответствующие команды, которые обычно вводятся в режиме глобальной конфигурации. На рис. 3 представлен переход из режима конфигурации строки,Switch(config-line)# в режим настройки интерфейса,Switch(config-if)#, без выхода из режима конфигурации строки.



# 2.1.4.1 Структура команд операционной системы IOS

**Базовая структура команд операционной системы IOS**

Устройства CISCO IOS поддерживают множество различных команд. Каждая команда IOS имеет определённый формат или синтаксис. Каждая команда выполняется только из соответствующего режима. Общий синтаксис команды — это команда, за которой следуют соответствующие ключевые слова и параметры. Некоторые команды состоят из ключевых слов и параметров, обеспечивающих дополнительные функциональные возможности. Команды используются для выполнения каких-либо действий, а ключевые слова используются для определения того, где и как нужно выполнить команду.

Как показано на рис. 1, команда — это аббревиатура или слова, введённые в командной строке после запроса. При вводе команд регистр не учитывается. Вслед за текстом команды вводится одно или несколько ключевых слов и параметров. После ввода каждой полной команды, включая все ключевые слова и параметры, нажмите клавишу Enter, чтобы отправить эту команду в командный процессор.

Ключевые слова описывают командному процессору определённые параметры. Например, команда **show** используется для просмотра информации об устройстве. Эта команда обладает несколькими ключевыми словами, которые нужно использовать, чтобы определить, какие выходные данные нужно отобразить. Например:

Switch# **show running-config**

После команды **show** следует ключевое слово **running-config**. Ключевое слово уточняет, что текущую конфигурацию нужно отобразить в выходных данных.

**Условные обозначения команд IOS**

Команда может потребовать одно или несколько параметров. В отличие от ключевого слова, параметр, как правило, не является предопределённым словом. Параметр — это значение или переменная, определённая пользователем. Чтобы понять, какие ключевые слова и параметры необходимы той или иной команде, см. раздел синтаксиса команд. Синтаксис обеспечивает шаблон или формат, который необходимо использовать при вводе команды.

Например, для использования команды**description** необходим такой синтаксис:

Switch(config-if)# **description** *string*

Как показано на рис. 2, команды и ключевые слова отображаются полужирным шрифтом, а текст курсивом отображает параметр, которому нужно дать значение. Параметром команды**description** является значение строки. Значение строки может быть представлено любым текстом, содержащим до 80 символов.

Таким образом, применяя описание для интерфейса с помощью команды**description**, введите такую строку:

Switch(config-if)# **description** **MainHQ Office Switch**

Команда — **description**, пользовательский параметр — **MainHQ Office Switch**.

Следующие примеры демонстрируют некоторые обозначения, используемые для документирования и использования команд IOS.

Для команды **ping**:

Синтаксис:

Switch> **ping** *ip-address*

Пример со значениями:

Switch> **ping** **10.10.10.5**

Команда — **ping**, пользовательский параметр — **10.10.10.5**.

Таким образом, синтаксис для ввода команды **traceroute** выглядит следующим образом:

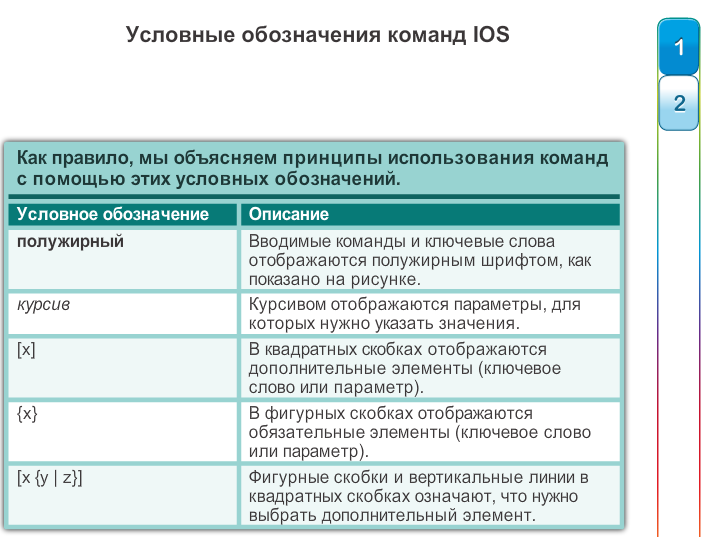
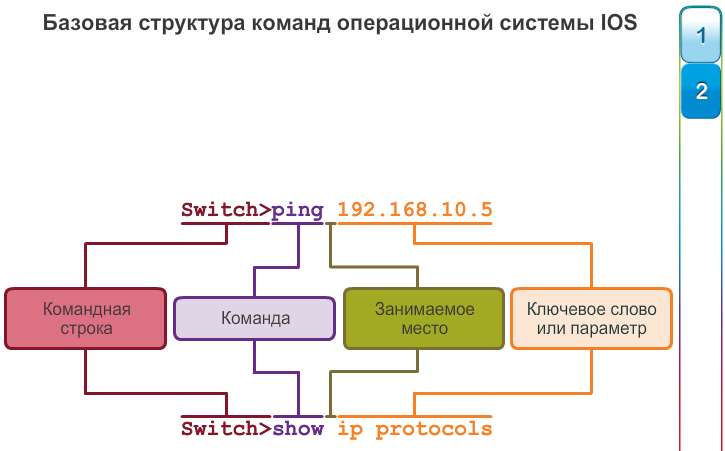
Синтаксис:

Switch> **traceroute** *ip-address*

Пример со значениями:

Switch> **traceroute** **192.168.254.254**

Команда — **traceroute**, пользовательский параметр —**192.168.254.254**.



# 2.1.4.2 Справочное руководство по командам CISCO IOS

Справочное руководство по командам CISCO IOS — это набор онлайн-документации, которая подробно описывает команды IOS, используемые в устройствах Cisco. Справочное руководство — основной источник информации для определённой команды IOS, точно так же, как словарь — основной источник для получения информации о конкретном слове.

Справочное руководство — основной источник, которым пользуются разработчики сетей для проверки различных характеристик заданной команды IOS. Ниже перечислены некоторые из наиболее распространенных характеристик:

* **Синтаксис**— наиболее подробная версия синтаксиса команд из существующих
* **По умолчанию**— способ реализации команды на устройстве с конфигурацией по умолчанию
* **Режим**— режим конфигурации на устройстве для ввода команды
* **История**— описания реализации команд в соответствующей версии IOS
* **Инструкции по применению** — рекомендации по реализации команд
* **Примеры**— полезные примеры, демонстрирующие распространённые случаи использования команды

Для перехода к Справочному руководству и поиска определённой команды выполните следующие действия:

**Шаг 1**. Перейдите по адресу[www.cisco.com](http://www.cisco.com/).

**Шаг 2**. Перейдите во вкладку**Поддержка**(Support)

**Шаг 3**. Выберите **Сетевое программное обеспечение** (IOS и NX-OS).

**Шаг 4**. Выберите **15.2M&T** (в качестве примера).

**Шаг 5**. Выберите **Справочные руководства**.

**Шаг 6**. Выберите**Справочныеруководства**

**Шаг 7**. Выберите конкретную технологию, содержащую команду, на которую вы ссылаетесь.

**Шаг 8**. Выберите ссылку слева, соответствующую алфавитному указателю команды, на которую вы ссылаетесь.

**Шаг 9**. Нажмите ссылку этой команды.

Например, команду **description** можно найти в *Справочном руководстве аппаратных компонентов и интерфейса Cisco IOS* под ссылкой алфавитного порядка *от D до E*.

**Примечание**. Полные версии PDF Справочных руководств для конкретной технологии можно загрузить по ссылкам на странице, которую вы увидите после завершения шага 7.

# 2.1.4.3 Контекстная справка

В операционной системе IOS предусмотрены несколько доступных видов справки:

* Контекстная справка
* Проверка синтаксиса команды
* Горячие клавиши и клавиши быстрого вызова

**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.

Контекстная справка полезна для получения списка доступных команд. Этот вид справки можно использовать в тех случаях, когда вы не знаете имени команды или хотите узнать, поддерживает ли IOS ту или иную команду в определённом режиме.

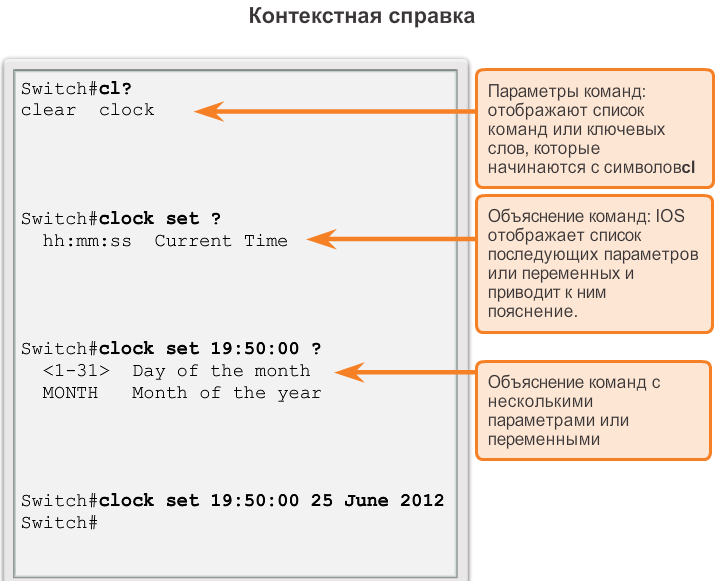
Например, для получения списка доступных команд в пользовательском режиме введите вопросительный знак (**?**) в командной строке Switch>.

Кроме того, контекстную справку можно использовать для отображения списка команд или ключевых слов, которые начинаются с определённого символа или символов. Если указать вопросительный знак без пробела сразу после ввода последовательности символов, IOS отобразит список команд или ключевых слов для этого контекста, которые начинаются с указанных символов.

Например, введите **sh?** для получения списка команд, которые начинаются с сочетания символов **sh**.

Последний вид контекстной справки используется для определения параметров, ключевых слов или параметров, соотносящихся с определённой командой. При вводе команды введите пробел перед вопросительным знаком **?**, чтобы определить, что можно или нужно ввести далее.

Как показано на рисунке, после команды**clock set 19:50:00** можно ввести символ **?**, чтобы определить дополнительные параметры или ключевые слова, доступные для этой команды.



# 2.1.4.4 Проверка синтаксиса команды

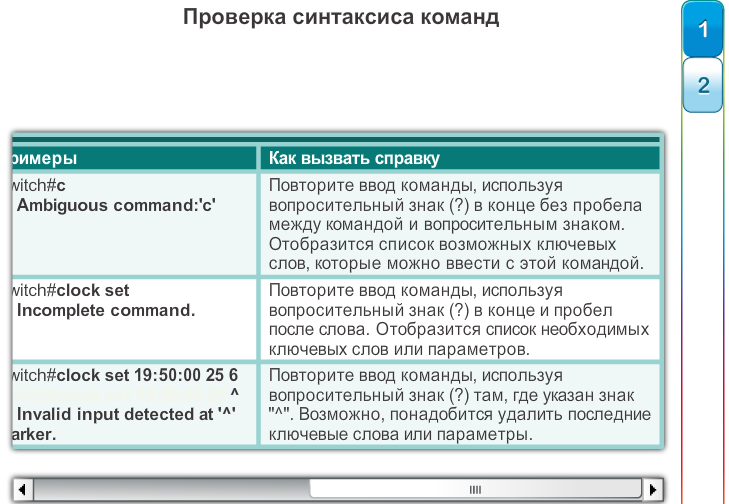
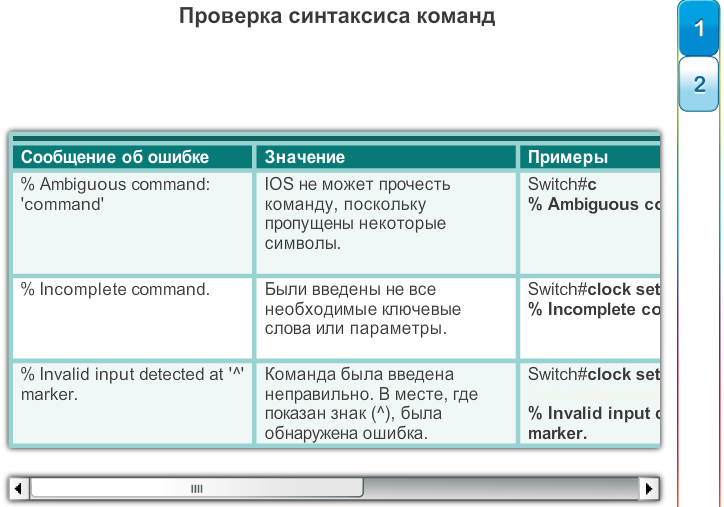
**Проверка синтаксиса команды**

Когда команда подтверждена клавишей Enter, командный интерпретатор анализирует команду слева направо, чтобы определить, какое действие требуется выполнить. Как показано на рис. 1, IOS выводит ответные сообщения при ошибочном вводе команды. Если интерпретатор понимает команду, то происходит выполнение требуемого действия и интерфейс командной строки (CLI) возвращается к соответствующей командной строке. Однако, если интерпретатор не распознаёт введённую команду, он объясняет, что в этой команде не так.

На рис. 2 показаны три различных типа сообщений об ошибке:

* Неоднозначная команда
* Неполная команда
* Неверная команда

Команда **clock set**оптимальна для экспериментирования с различными сообщениями проверки синтаксиса команд, как показано на рис. 1. На рис. 2 показаны три типа сообщений об ошибке.



# 2.1.4.5 Горячие клавиши и клавиши быстрого вызова

**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.

На рисунке показано большинство сокращений. Необходимо отметить следующие 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

Рассмотрим некоторые горячие клавиши подробнее.

**Tab**

Tab используется для завершения сокращённых команд и параметров, если сокращение можно отличить от другой доступной команды или параметра. После введения достаточного количества символов нажмите клавишу**Tab**, и интерфейс командной строки (CLI) завершит команду или ключевое слово.

Этот способ можно использовать при обучении, поскольку он позволяет просматривать полное слово, используемое для команды или ключевого слова.

**Ctrl-R**

Это сочетание клавиш обновляет строку. Используйте сочетание клавиш **Ctrl-R**для обновления строки. Например, когда вы вводите символы в строке, IOS может отправлять сообщение в интерфейс командной строки (CLI). Чтобы обновить строку и не вводить команду заново, используйте сочетание клавиш **Ctrl-R**.

В данном примере по мере ввода команды отправляется сообщение о нарушении работы интерфейса.

Switch# **show mac-**

16w4d: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down

16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down

Для обновления строки используйте сочетание клавиш **Ctrl-R**:

Switch# **show mac**

**Ctrl-Z**

Выход из режима конфигурации возвращает пользователя в привилегированный режим. Поскольку IOS использует иерархическую структуру режимов, вы можете оказаться на несколько уровней ниже. Рекомендуется не выходить из каждого режима отдельно, а использовать сочетание клавиш **Ctrl-Z**, чтобы сразу вернуться в командную строку привилегированного режима на верхний уровень.

**Стрелки вверх и вниз**

Эти клавиши быстрого вызова отображают историю введённых команд. Программное обеспечение CISCO IOS резервирует несколько последних команд и символов для отображения. Буфер используется для повторного ввода команд, без необходимости их набора на клавиатуре.

Для пролистывания команд в буфере можно использовать последовательности клавиш. Используйте клавишу **Стрелка вверх**(**Ctrl-P**), чтобы отобразить ранее введённые команды. При каждом следующем нажатии клавиши будет отображена предыдущая команда. Используйте клавишу **Стрелка вниз**(**Ctrl-N**), чтобы пролистать историю команд.

**Ctrl-Shift-6**

Последовательность выхода прервёт любой текущий процесс. При запуске процесса IOS из интерфейса командной строки, такого как ping или traceroute, эта команда будет выполняться до её завершения или до тех пор, пока она не будет прервана. Интерфейс командной строки не будет реагировать на запросы во время выполнения данного процесса. Чтобы прервать выходные данные и начать работу с интерфейсом командной строки (CLI), нажмите сочетание клавиш**Ctrl-Shift-6**.

**Ctrl-C**

Эта команда прерывает ввод команды и выполняет выход из режима конфигурации. Эту комбинацию можно использовать для отмены введённой команды.

**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**



# 2.1.4.6 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. На рисунке выделены несколько наиболее распространённых команд IOS.

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**

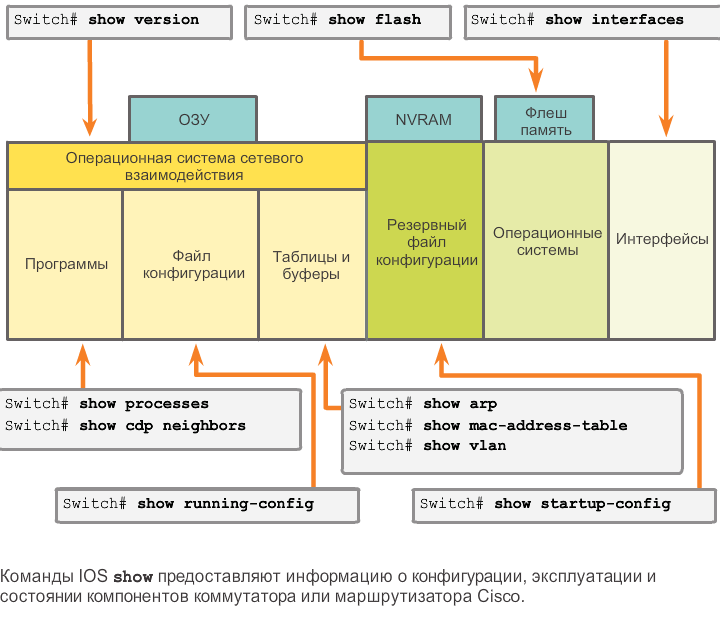
К дополнительным командам **show**, часто используемым специалистами сети, относятся:

**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.



# 2.1.4.7 Команда show version

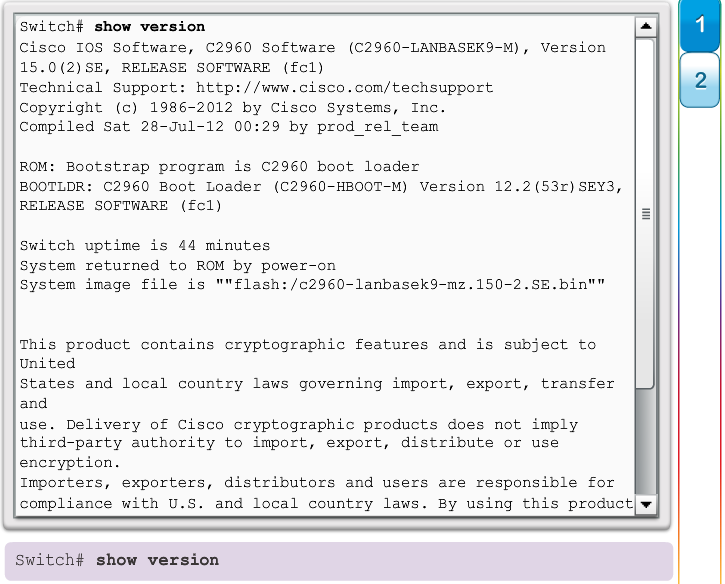
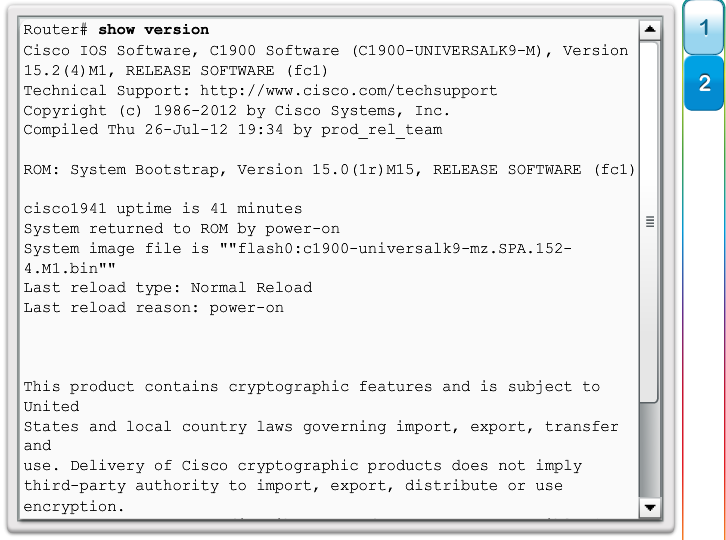
К числу наиболее часто используемых команд коммутатора или маршрутизатора относятся:

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

На рис. 1 показаны выходные данные для маршрутизатора Cisco 1941, а на рис. 2 — для коммутатора Cisco Catalyst 2960.



# 2.2.1.1 Почему коммутатор?

Как было упомянуто ранее, коммутаторы и маршрутизаторы Cisco во многом похожи. Они работают на аналогичной операционной системе, поддерживают схожие структуры команд, кроме того, многие команды в точности такие же. Кроме того, при внедрении этих двух устройств в сеть потребуется выполнить одинаковые настройки.

Однако коммутатор CISCO IOS является одним из самых простых устройств, которое можно установить в сети. Это связано с тем, что коммутатор может функционировать и без дополнительной конфигурации. В самом простом случае коммутатор можно подключить и без конфигурации, и он будет исправно осуществлять передачу данных между двумя устройствами.

Кроме того, коммутатор — одно из основных устройств, используемых в создании небольшой сети. После подключения двух ПК к коммутатору между этими компьютерами сразу будет установлено соединение.

Поэтому в оставшейся части данной главы мы рассмотрим создание малой сети из двух ПК, подключённых друг к другу через коммутатор с первоначальным настройками. Начальные параметры — это назначение имени коммутатора, ограничение доступа к конфигурации устройства, настройка баннерных сообщений и сохранение конфигурации.

# 2.2.1.2 Имена устройств

Один из первых шагов при настройке сетевого устройства — это назначение уникального имени устройства или узла. Узлы отображаются в окнах интерфейса командной строки (CLI) 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. Имя коммутатора CISCO IOS по умолчанию — «Коммутатор».

Представьте себе, что в сетевом взаимодействии участвуют несколько коммутаторов, которым было назначено имя по умолчанию «Коммутатор» (как показано на рисунке). Это может создать значительные проблемы при настройке сети и обслуживании. При доступе к удалённому устройству с помощью протокола SSH важно иметь подтверждение того, что вы подключены к нужному устройству. Если у всех устройств остались имена по умолчанию, будет сложно определить, подключено ли нужное устройство.

Если разумно назначить имена устройствам, будет легче запоминать сетевые устройства, обсуждать их работу, обслуживать и различать. Чтобы правильно назначить имена, нужно учитывать соглашение об именах, которое распространяется на компанию или местоположение устройства. Рекомендуется в одно время создать соглашение об именах и схему адресации, чтобы не нарушить целостность организации.

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.



# 2.2.1.3 Имена узлов

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

**Пример применения имен**

Для примера возьмем три коммутатора, подключённых к сети, которая охватывает три этажа.

Чтобы создать для этих трех коммутаторов соглашение имён, нужно учесть их местоположение и назначение.

Например, на рисунке мы назвали три коммутатора Ком-Этаж-1, Ком-Этаж-2 и Ком-Этаж-3.

Для поддержания целостности документации мы зарегистрировали их имена и указали причины такого наименования.

После заключения соглашения имен нужно присвоить устройствам имена с помощью интерфейса командной строки (CLI).

# 2.2.1.4 Настройка узлов

**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)#

Как показано на рисунке, 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**.

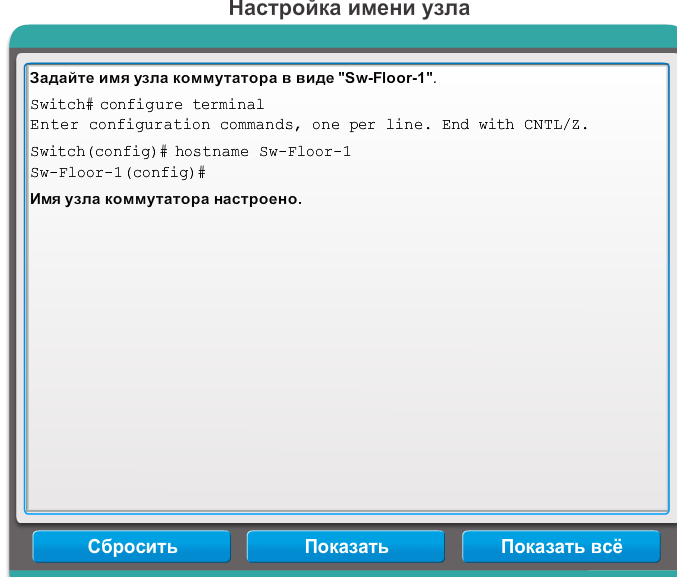
Например, чтобы удалить имя устройства, потребуется следующая команда:

Sw-Floor-1 (config)# **no hostname**

Switch(config)#

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

Отработайте на рисунке назначение имени узла на коммутаторе.



# 2.2.2.1 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.

**Примечание**. В большинстве лабораторных работ по данному курсу мы будем использовать простые пароли — **cisco** или **class**. Эти пароли ненадёжны и их легко подобрать, поэтому использовать их в рабочей среде не рекомендуется. Мы используем эти пароли лишь для удобства работы в учебной аудитории или для демонстрации примеров.

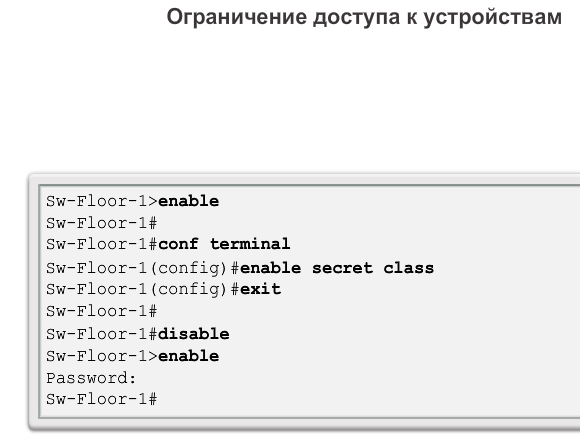
# 2.2.2.2 Защита доступа к привилегированному режиму

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**

Пример на рисунке показывает, что при первом использовании команды **enable**пароль не требуется. Далее нужно ввести команду **enable secret class**, и доступ в привилегированный режим будет защищён. Обратите внимание, что в целях безопасности пароль при вводе не отображается.



# 2.2.2.3 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:

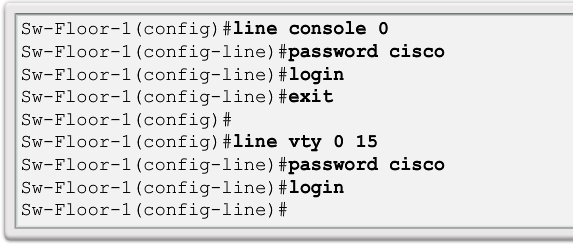
Switch(config)# **line vty 0 15**

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.

На рисунке продемонстрировано, как осуществляется защита доступа к пользовательскому режиму на консоли и по каналам Telnet.



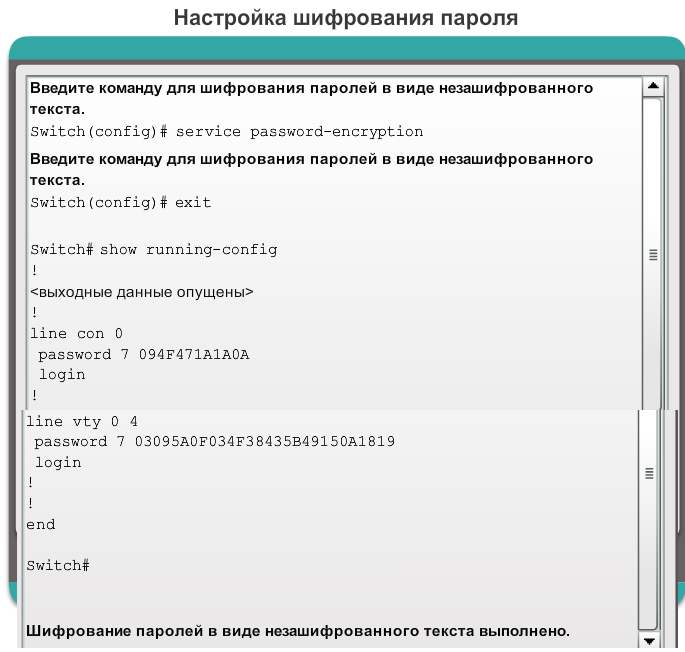
# 2.2.2.4 Шифрование пароля

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.

На рисунке отработайте ввод команды для шифрования пароля.



# 2.2.2.5 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.

На рисунке показан пример баннера, настроенного с помощью разделительного символа «#». Обратите внимание на способ отображения баннера при получении доступа к коммутатору.

# 2.2.3.1 Файлы конфигурации

Файл текущей конфигурации отражает текущую конфигурацию, функционирующую на устройстве CISCO IOS. Он содержит команды, используемые для определения принципов работы устройства в сети, как показано на рисунке 1. 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.

Например:

Switch# **reload**

System configuration has been modified. Save? [yes/no]: **n**

Proceed with reload? [confirm]

\*Apr 13 01:34:15.758: %SYS-5-RELOAD: Reload requested by console. Reload Reason:

Reload Command.

System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2004 by cisco Systems, Inc.

PLD version 0x10

GIO ASIC version 0x127

c1841 platform with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled

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**.

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]

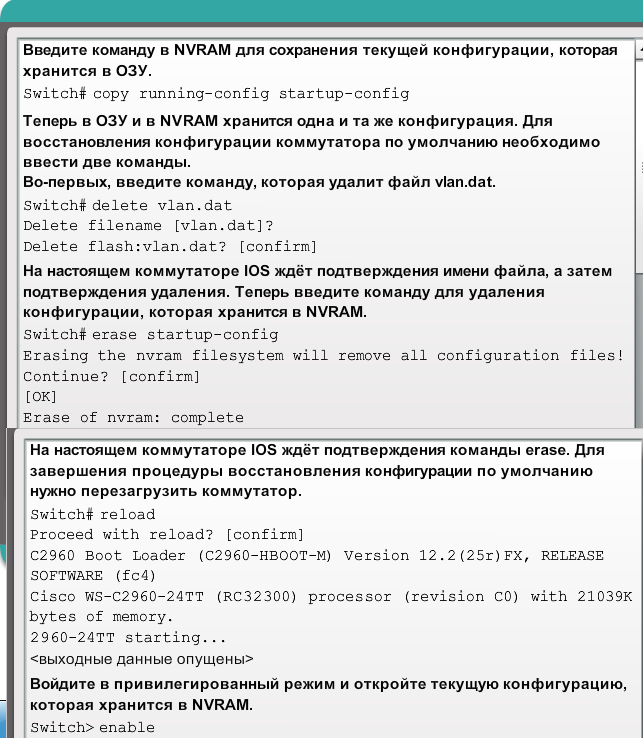
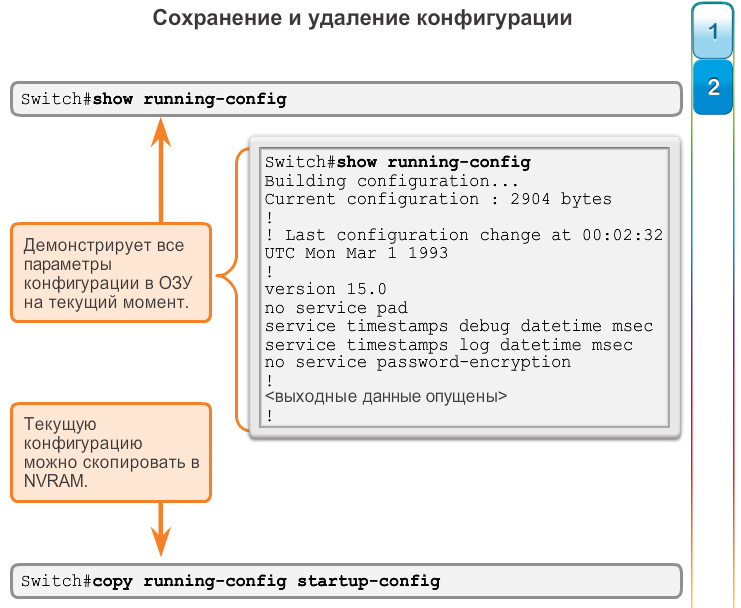
[OK]

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.

На рисунке 2 отработайте ввод команд для сохранения текущей конфигурации из ОЗУ в NVRAM.



# 2.2.3.2 Захват текста

**Резервная конфигурация с захватом текста**

В дополнение к сохранению текущей конфигурации в начальную файлы конфигурации можно сохранить в текстовый документ. Эта последовательность действий позволит в дальнейшем редактировать или использовать рабочую копию файлов конфигурации.

На рис. 1 показано, как файлы конфигурации можно сохранять и архивировать в текстовый документ с помощью программы Tera Term.

Вам необходимо совершить следующие действия.

* Выберите пункт **«Журнал»** в пункте меню «Файл».
* Выберите местоположение. Программа Tera Term запустит процесс захвата текста.
* После начала данного процесса в отобразившейся командной строке привилегированного режима выполните команды **show running-config** или **show startup-config** . Текст, отображённый в окне, будет помещён в выбранный файл.
* По окончании захвата текста нажмите **«Закрыть»** в окне журнала программы Tera Term.
* Просмотрите выходные данные, чтобы убедиться в том, что он не был повреждён.

На рис. 2 показано, как файлы можно сохранять в текстовый документ с помощью программы HyperTerminal.

**Восстановление текстовых конфигураций**

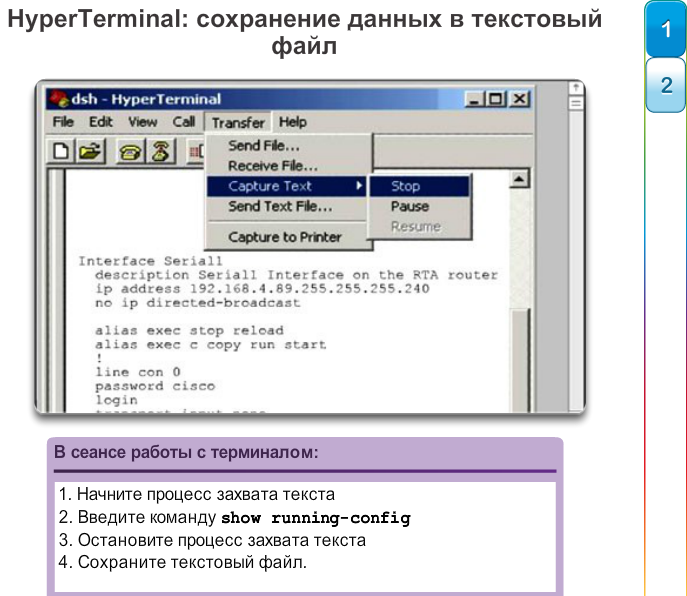
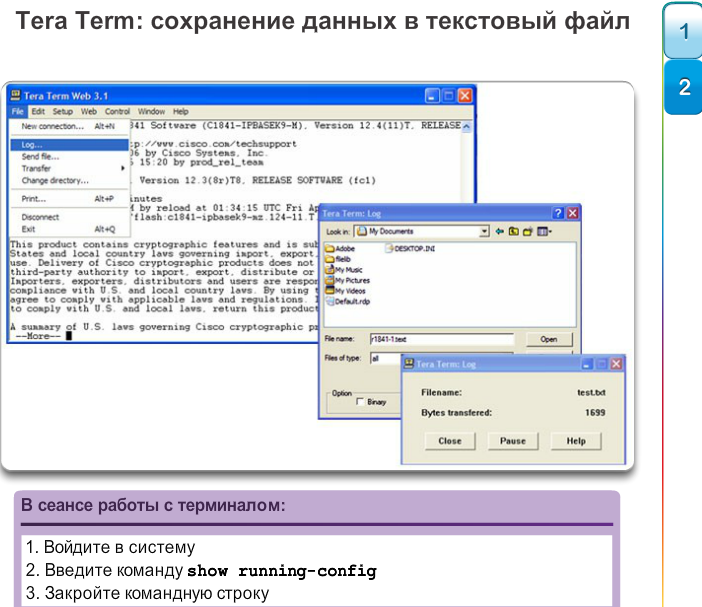
Файл конфигурации можно скопировать из хранилища в память устройства. IOS выполняет каждую строку текста конфигурации в качестве команды во время копирования этого файла в терминал. Перед копированием файл, скорее всего, потребуется изменить. Рекомендуется изменить зашифрованные пароли читаемым текстом и удалить параметр, цифру 5 или 7, который указывает на то, что пароль зашифрован. Некомандный текст, например, «--More--» и сообщения IOS должны быть удалены. Этот процесс рассматривается в ходе лабораторной работы.

На следующем этапе в интерфейсе командной строки (CLI) для данного устройства необходимо задать режим глобальной конфигурации, чтобы получать команды из копируемого текстового файла.

При использовании программы Tera Term необходимо выполнить следующий порядок действий.

* Очистите текст от некомандных сообщений и сохраните его.
* В пункте меню **File** нажмите**Отправить**.
* Укажите путь к файлу, который необходимо скопировать на данное устройство, и нажмите **«Открыть»**.
* После этого служебная программа Tera Term выполнит вставку этого файла в память устройства.

В интерфейсе командной строки текстовое содержимое этого файла будет использоваться в качестве команд и начнёт выполнять функцию текущего файла конфигурации данного устройства. Это удобный способ ручной настройки устройства.



# 2.3.1.1 IP-адресация устройств

Чтобы устройства обнаружили друг друга и установили сквозное подключение по сети Интернет, используются IP-адреса, адреса IPv4 или IPv6. Фактически IP-адреса обеспечивают связь между устройствами от источника до назначения и обратно в любом сетевом взаимодействии.

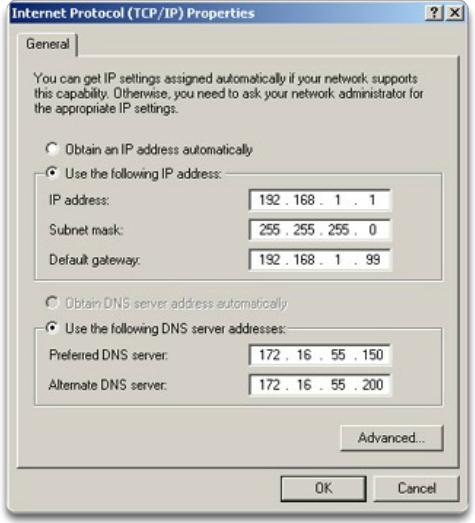
Каждое оконечное устройство в сети должно иметь IP-адрес. К оконечным устройствам относятся следующие:

* Компьютеры (рабочие станции, ноутбуки, файловые серверы, веб-серверы)
* Сетевые принтеры
* VoIP-телефоны
* Камеры видеонаблюдения
* Смартфоны
* Мобильные карманные устройства (например, беспроводные сканеры штрих-кодов)

Структура адреса IPv4 — это точечно-десятичное представление в виде четырёх десятичных чисел в диапазоне от 0 до 255. Адреса IPv4 — это номера, присвоенные отдельным устройствам, подключённым к сети. Они имеют логическую природу, поскольку предоставляют информацию о местоположении устройства.

Помимо IP-адреса необходима маска подсети. Маска подсети — это особый тип адреса IPv4, который совместно с IP-адресом определяет, к какой именно подсети, принадлежащей крупной сети, подключено данное устройство.

IP-адреса могут быть присвоены физическим портам и виртуальным интерфейсам на всех устройствах. Виртуальный интерфейс означает, что с данным устройством не связано дополнительное физическое оборудование.



# 2.3.1.2 Интерфейсы и порты

Передача данных по сети зависит от интерфейсов конечных устройств, интерфейсов сетевых устройств и кабелей, осуществляющих соединение.

Каждый физический интерфейс определяется своими техническими характеристиками или стандартами. Соединяющий кабель должен соответствовать всем физическим стандартам интерфейса. Передача данных осуществляется посредством витых медных кабелей, оптоволоконных кабелей, коаксиальных кабелей или с помощью беспроводной связи. Разные типы сетевых средств передачи данных отличаются характерными функциями и преимуществами. Сетевые средства передачи данных могут иметь разные характеристики и выполнять разные задачи. К некоторым отличиям между различными типами средств передачи данных относятся следующие.

* Расстояние, которое может покрывать средство передачи данных
* Среда, в которой может быть установлено средство передачи данных
* Объёмы данных и скорость передачи
* Стоимость средства передачи данных и его установка

Каждая ссылка в сети Интернет не только требует особого типа среды, но и отдельной сетевой технологии. Ethernet — наиболее распространённая технология локальной сети (LAN) на сегодняшний день. Порты Ethernet можно найти на устройствах конечных пользователей, коммутационных и других сетевых устройствах, которые могут осуществлять физическое подключение к сети с помощью кабеля. Чтобы кабель мог соединять устройства с помощью порта Ethernet, кабель должен быть снабжён правильным разъёмом — RJ-45.

Коммутаторы CISCO IOS не только оснащены физическими портами для устройств, но также одним или несколькими виртуальными интерфейсами коммутаторов (SVI). Такие интерфейсы называются виртуальными, поскольку в устройстве нет связанного с ними физического оборудования. Виртуальный интерфейс создан в программном обеспечении. Виртуальный интерфейс позволяет удалённо управлять коммутатором через сеть с помощью IPv4. Каждый коммутатор поставляется с одним виртуальным интерфейсом коммутатора в конфигурации по умолчанию. Виртуальным интерфейсом по умолчанию является VLAN1.

# 2.3.2.1 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.

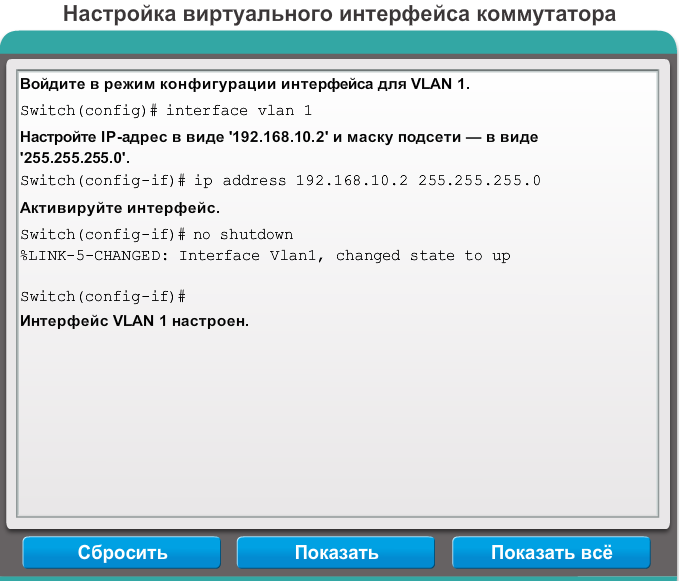
Впоследствии вы поймете важность IP-адресов, но в данный момент необходимо научиться быстро настраивать коммутатор для поддержки удалённого доступа. На рисунке показана команда для активации IP соединения с коммутатором S1 при помощи IP-адреса 192.168.10.2:

* **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.

На данном рисунке отработайте настройку виртуального интерфейса коммутатора путем ввода команд.



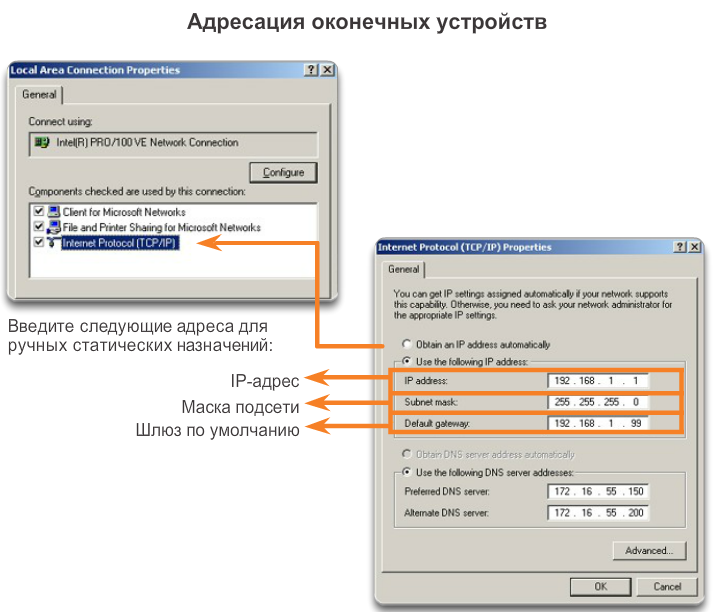
# 2.3.2.2 Настройка IP-адресов оконечных устройств вручную

Для обеспечения связи оконечного устройства со всей сетью его нужно правильно настроить с IP-данными. Как и виртуальному интерфейсу коммутатора, оконечному устройству нужно присвоить IP-адрес и маску подсети. Эти данные настраиваются в параметрах ПК.

Чтобы оконечное устройство было правильно подключено к сети, на нём нужно настроить все эти параметры. Эта информация настраивается в области параметров сети ПК. Кроме IP-адреса и данных о маске подсети, можно настроить шлюз по умолчанию и данные сервера DNS, как показано на рисунке.

Адрес шлюза по умолчанию — это IP-адрес интерфейса маршрутизатора, используемого для выхода сетевого трафика из локальной сети. Шлюз по умолчанию — это IP-адрес, который часто назначает сетевой администратор. Его используют, когда трафик нужно направить в другую сеть.

Адрес сервера DNS — это IP-адрес сервера службы доменных имен (DNS), который используется для преобразования IP-адресов в веб-адреса, например, [www.cisco.com](http://www.cisco.com/). Доступ к устройствам в Интернете осуществляется с помощью IP-адреса. Однако пользователям легче запомнить имена, а не цифры. Поэтому для простоты веб-сайтам присваиваются имена. Сервер DNS используется для поддержания сопоставления между IP-адресами и различными устройствами.



# 2.3.2.3 Автоматическая настройка IP-адресов оконечных устройств

Информацию об IP-адресе можно ввести в ПК вручную или получить автоматически с помощью протокола динамической конфигурации сетевого узла (DHCP). DHCP обеспечивает автоматическую настройку IP-данных оконечным устройствам.

DHCP — это технология, которая используется практически во всех корпоративных сетях. Чтобы понять преимущества этой технологии, можно оценить объём работы, который пришлось бы выполнять без её применения.

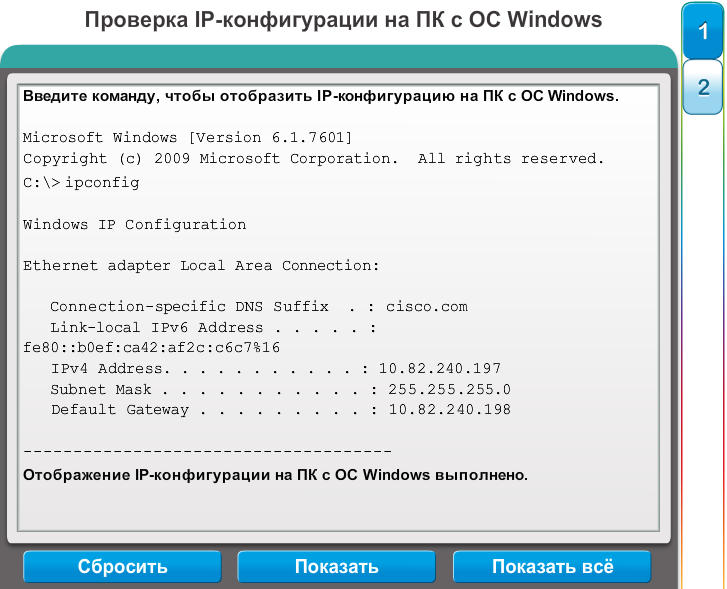
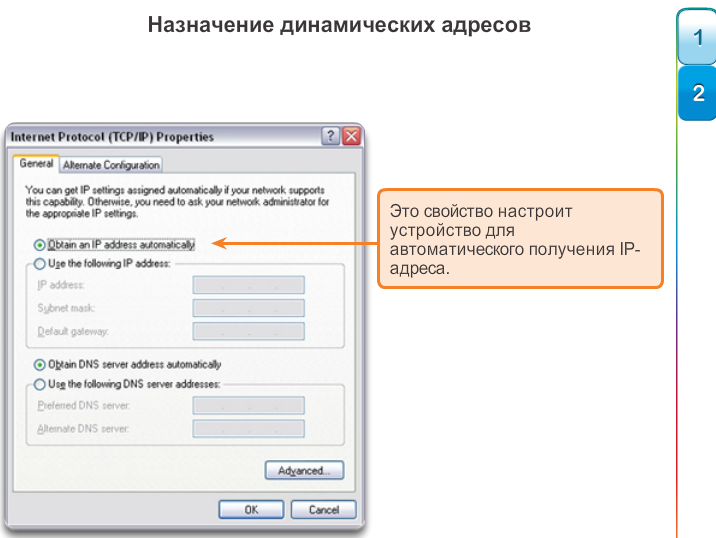
DHCP автоматически настраивает адреса IPv4 для каждого оконечного устройства в сети с включённым протоколом DHCP. Представьте, сколько времени вы бы тратили, если бы при каждом присоединении сети вам приходилось бы вручную вводить данные IP-адреса, маски подсети, шлюза по умолчанию и сервера DNS. Умножьте это на количество пользователей и их устройств в сети, и вы сразу поймёте преимущества DHCP.

DHCP — пример наиболее эффективной технологии. Одно из основных назначений любой технологии — облегчить работу человека. При наличии DHCP конечный пользователь может придти в любое место, где есть сетевое подключение, и подключиться к сети кабелем Ethernet или через беспроводное соединение, и вся информация IPv4, необходимая для полноценной связи по сети, будет настроена автоматически.

Как показано на рисунке 1, для настройки протокола DHCP на ПК с ОС Windows необходимо только выбрать параметры «Получить IP-адрес автоматически» и «Получить адрес сервера DNS автоматически». Вашему ПК будут присвоены данные из пула IP-адресов, а также вся соответствующая информация, имеющаяся на сервере DHCP.

Чтобы просмотреть настройки IP для ПК с ОС Windows, в командной строке введите команду **ipconfig**. В выходных данных команды вы увидите IP-адрес, маску подсети и шлюз, которые ПК получил с сервера DHCP.

На рисунке 2 отработайте отображение IP-адреса на ПК с ОС Windows при помощи соответствующих команд.



# 2.3.2.4 Конфликты IP-адресов

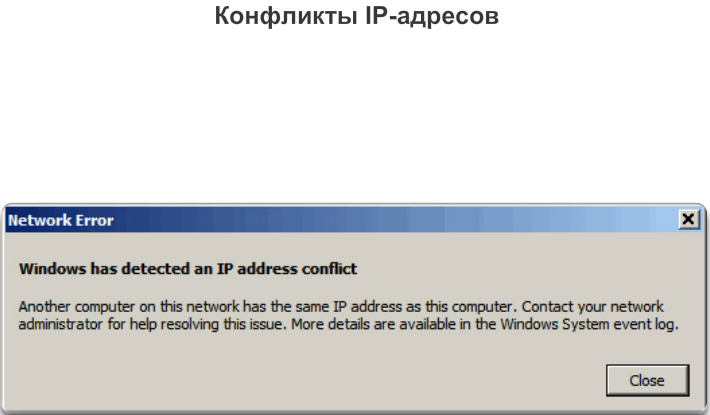
Если для сетевых устройств, например, для принтера, был определён статичный (ручной) IP-адрес, а затем установлен сервер DHCP, между сетевым устройством и ПК, который автоматически получает IP-данные с сервера DHCP, может произойти конфликт двойного IP-адреса. Также конфликт может возникнуть, если в случае сбоя работы сети и сервера DHCP вручную указать статический IP-адрес для сетевого устройства. Конфликт возникнет после исправления неполадок и восстановления сервера DHCP в сети.

Чтобы разрешить такой конфликт IP-адресации, нужно подключить сетевое устройство со статичным IP-адресом к клиенту DHCP. Также можно исключить статичный IP-адрес оконечного устройства из диапазона адресов DHCP.

Во втором случае необходимо обладать правами администратора на сервере DHCP и уметь работать с DHCP на сервере.

Кроме того, вы можете столкнуться с IP-конфликтами при ручной настройке IP на оконечном устройстве в сети, в которой используются только статические IP-адреса. В этом случае необходимо определить, какие IP-адреса доступны на конкретной подсети IP и настроить их соответствующим образом. Этот случай демонстрирует, насколько важно сетевому администратору вести подробную документацию, в том числе назначения IP-адресов для оконечных устройств.

**Примечание**. Как правило, статические IP-адреса используются с серверами и принтерами в сетях малого и среднего размера, а данные IP, настроенные автоматически с помощью сервера DHCP, используются выделенными устройствами сотрудников.



# 2.3.3.1 Проверка loopback-адреса на оконечном устройстве

**Тестирование логического интерфейса Loopback**

На рисунке показан первый шаг в последовательности тестирования. 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**

Ответ данной команды будет выглядеть примерно следующим образом:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

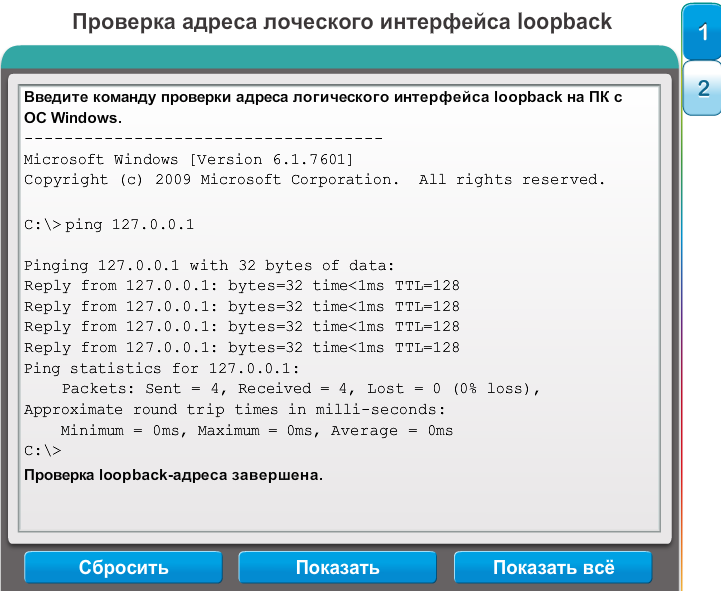
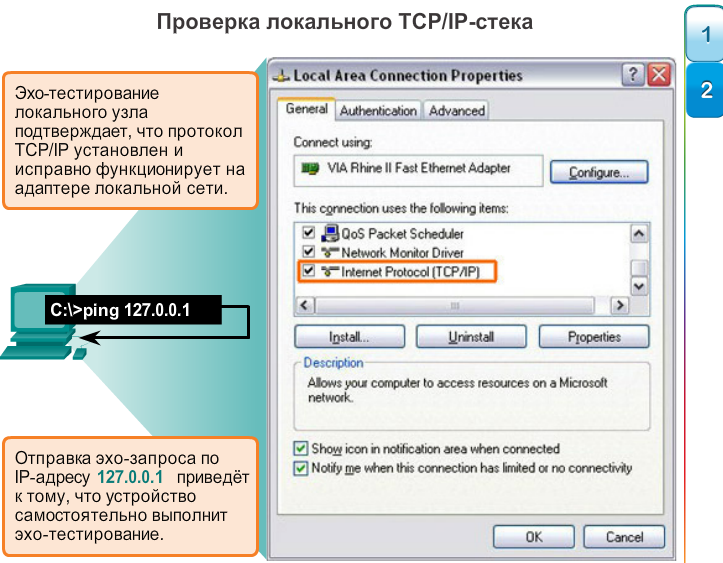
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Результат показывает, что четыре тестовых пакета каждый по 32 байта были отправлены и возвращены от узла 127.0.0.1 быстрее, чем за 1 мс. Этот успешный эхо-запрос доказывает, что сетевая интерфейсная плата, драйверы и реализация TCP/IP функционируют правильно.

На рисунке 2 отработайте проверку loopback-адреса путём ввода необходимых команд.



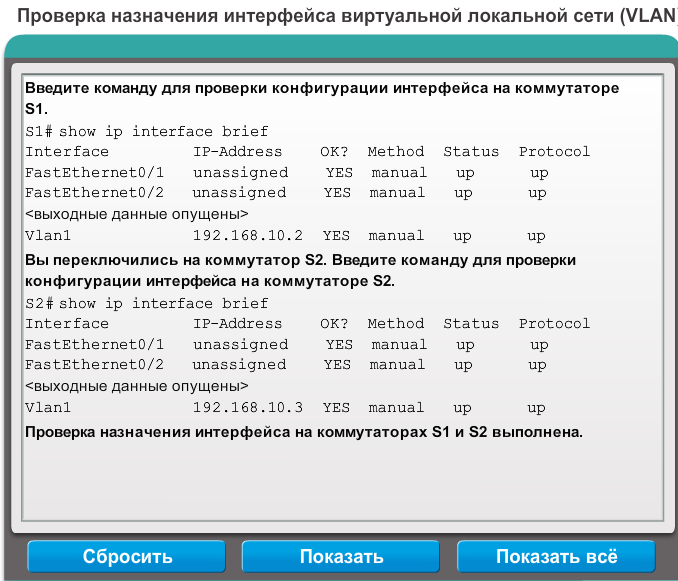
# 2.3.3.2 Тестирование назначения интерфейса

Так же, как вы используете команды и утилиты для проверки конфигурации узла, вы используете команды для проверки интерфейсов промежуточных устройств. IOS предоставляет команды для проверки работы интерфейсов маршрутизатора и коммутатора.

**Проверка интерфейсов коммутаторов**

Используйте команду **show ip interface brief** для проверки состояния интерфейсов коммутаторов S1 и S2, как показано на рисунке. IP-адрес, назначенный интерфейсу VLAN 1 на коммутаторе S1, — 192.168.10.2. IP-адрес, назначенный интерфейсу VLAN 1 на коммутаторе S2, — 192.168.10.3. Физические интерфейсы F0/1 и F0/2 на коммутаторе S1 являются рабочими, как и физические интерфейсы F0/1 и F0/2 на коммутаторе S2.

Чтобы отработать проверку интерфейса виртуальной локальной сети (VLAN), введите команды на рисунке.



# 2.3.3.3 Тестирование сквозного подключения

**Тестирование соединения между ПК и коммутатором**

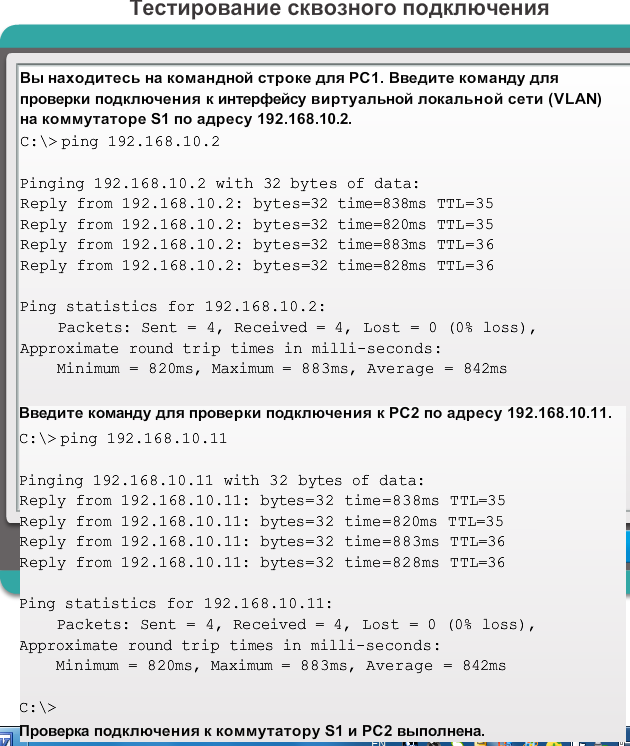
Команду **ping** можно использовать на ПК так же, как и на устройстве CISCO IOS. На рисунке показано, что эхо-запрос с ПК1 на IP-адрес интерфейса VLAN 1 на коммутаторе S1, 192.168.10.2 должен быть выполнен успешно.

**Тестирование сквозного подключения**

IP-адрес ПК1 — 192.168.10.10, маска подсети — 255.255.255.0, шлюз по умолчанию — 192.168.10.1.

IP-адрес ПК2 — 192.168.10.11, маска подсети — 255.255.255.0, шлюз по умолчанию — 192.168.10.1.

Эхо-запрос с ПК1 на ПК2 также должен быть выполнен успешно. Успешное тестирование с помощью команды ping с ПК1 на ПК2 подтверждает сквозное подключение по сети!



# 2.4.1.3 Заключение

CISCO IOS — это термин, который включает в себя ряд различных операционных систем, которые работают на различных сетевых устройствах. Технический специалист может ввести определённые команды, чтобы настроить или запрограммировать устройство для выполнения различных сетевых функций. Специалисты в области сетевого проектирования полагаются именно на функции маршрутизаторов и коммутаторов Cisco IOS, чтобы проектируемые сети функционировали должным образом.

Доступ к сервисам CISCO IOS осуществляется с помощью интерфейса командной строки (CLI), войти в который можно через консольный порт, порт AUX или по протоколам Telnet или SSH. Один раз подключившись к интерфейсу командной строки (CLI), сетевые специалисты могут изменять конфигурации устройств CISCO IOS. CISCO IOS разработана как операционная система с режимами, т.е. сетевой специалист должен уметь переключаться между различными иерархическими режимами IOS. Каждый режим поддерживает различные команды IOS.

Справочное руководство CISCO IOS — это набор онлайн-документов, подробно описывающих команды IOS, которые используются на устройствах Cisco (например, на маршрутизаторах и коммутаторах CISCO IOS).

Маршрутизаторы и коммутаторы CISCO IOS поддерживают подобную операционную систему с режимами, аналогичные командные структуры и многие схожие команды. Кроме того, при внедрении этих двух устройств в сеть потребуется выполнить одинаковые настройки.

В этой главе мы познакомились с операционной системой CISCO IOS. Мы подробно рассмотрели различные режимы CISCO IOS и изучили основную командную структуру, используемую для настройки этой операционной системы. Кроме того, вы получили общее представление о начальных параметрах коммутатора CISCO IOS, в том числе о назначении имени, ограничении доступа к конфигурации устройства, настройках и сохранении конфигурации.

В следующей главе мы узнаем, как пакеты перемещаются по сетевой инфраструктуре и изучим основные правила передачи пакетов.

