



МОСКОВСКИЙ  
АВИАЦИОННЫЙ  
ИНСТИТУТ

НАЦИОНАЛЬНЫЙ  
ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ

# Современные сетевые технологии



## Введение в сетевые технологии



Современные сетевые технологии

# Сети сегодня – Сети без границ

Общение почти так же важно для нас, как воздух, вода, пища и кров.

В современном мире за счет использования сетей мы связаны друг с другом, как никогда раньше.

- Мир без границ
- Глобальные сообщества
- Сети, объединяющие людей



Предоставление ресурсов в рамках сети

# Сети различных масштабов



Небольшие домашние сети



Сети для малого и домашнего офиса



Средние и крупные сети



Глобальные сети

# Предоставление ресурсов в рамках сети

## Клиенты и серверы



Все компьютеры в сети классифицируются как **узлы (хосты)** или **оконечные устройства**.

**Клиентами** являются компьютеры, отправляющие запросы на получение информации на серверы:

- веб-страницы с веб-сервера
- электронная почта с сервера электронной почты

Узлы могут работать как **клиент, сервер или как и то, и другое**. Роль компьютера в сети определяется программным обеспечением.

На одном компьютере можно параллельно установить несколько типов серверного ПО или запускать несколько типов клиентского программного обеспечения.

**Серверы** — это компьютеры, предоставляющие информацию оконечным устройствам в сети:

- серверы электронной почты
- веб-серверы
- сервер файлов

Для работы каждой службы необходимо отдельное серверное программное обеспечение.

Компьютер с серверным программным обеспечением может одновременно обслуживать одного и более клиентов.

## Предоставление ресурсов в рамках сети

# Одноранговые сети

Это бессерверная сетевая технология, которая позволяет нескольким сетевым устройствам совместно использовать ресурсы и взаимодействовать друг с другом напрямую.



### Преимущества одноранговой сети:

- лёгкость установки;
- простота;
- сокращение расходов (поскольку сетевые устройства и выделенные серверы могут не потребоваться);
- можно использовать для простых задач, таких как передача файлов и совместное использование принтеров.

### Недостатки одноранговой сети:

- отсутствует централизованное управление;
- не вполне безопасна;
- не масштабируется;
- все устройства могут выступать в качестве как клиента, так и сервера, что может замедлить их работу.

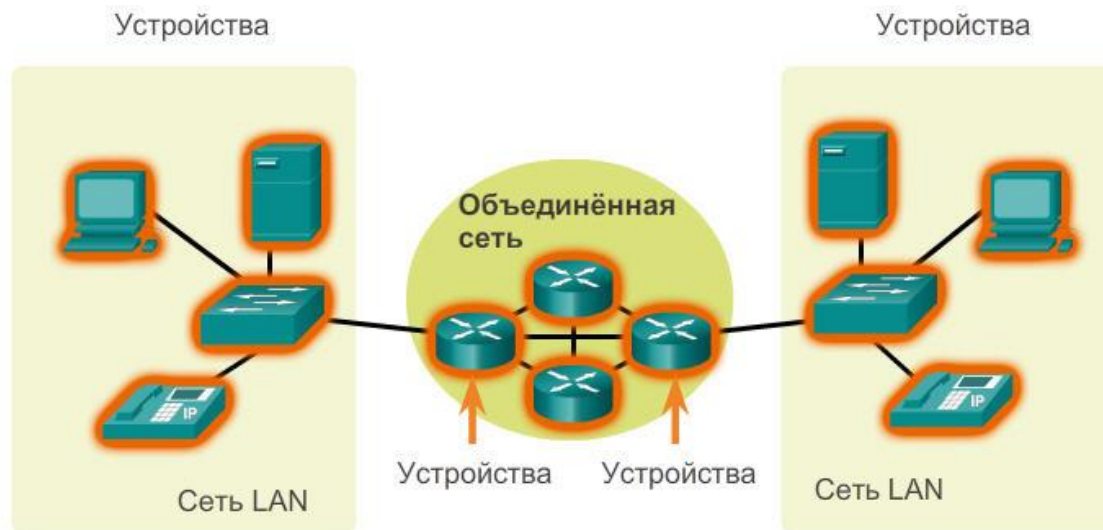


# Локальные сети LAN, сети WAN и сети Интернет

## Компоненты сети

Существует три категории компонентов сети:

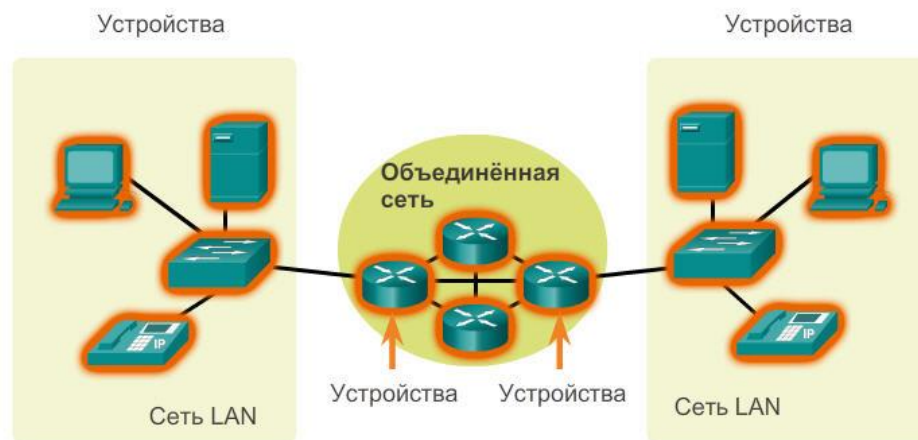
- устройства;
- среда передачи данных;
- службы.



# Оконечные устройства

К конечным устройствам относятся:

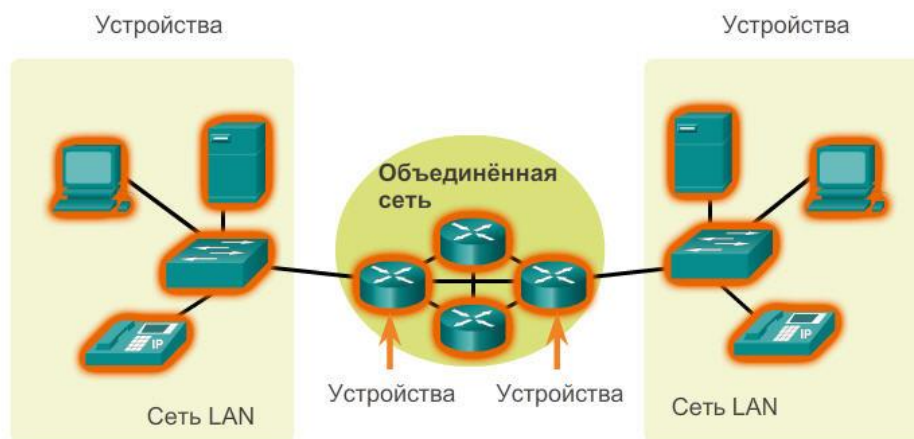
- компьютеры (рабочие станции, ноутбуки, файловые серверы, веб-серверы);
- сетевые принтеры;
- телефоны VoIP;
- оконечные устройства системы дистанционного присутствия TelePresence;
- камеры видеонаблюдения;
- портативные мобильные устройства (смартфоны, планшетные ПК, КПК, беспроводные считыватели кредитных и дебетовых карт и сканеры штрих-кодов).



# Устройства инфраструктуры сети

К промежуточным сетевым устройствам относятся:

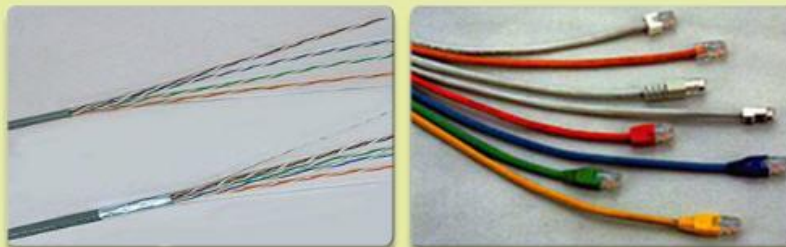
- устройства сетевого доступа (коммутаторы и точки беспроводного доступа);
- устройства сетевого взаимодействия (маршрутизаторы);
- устройства системы безопасности (межсетевые экраны).





# Сетевая среда

Медный кабель



Оптоволоконный кабель

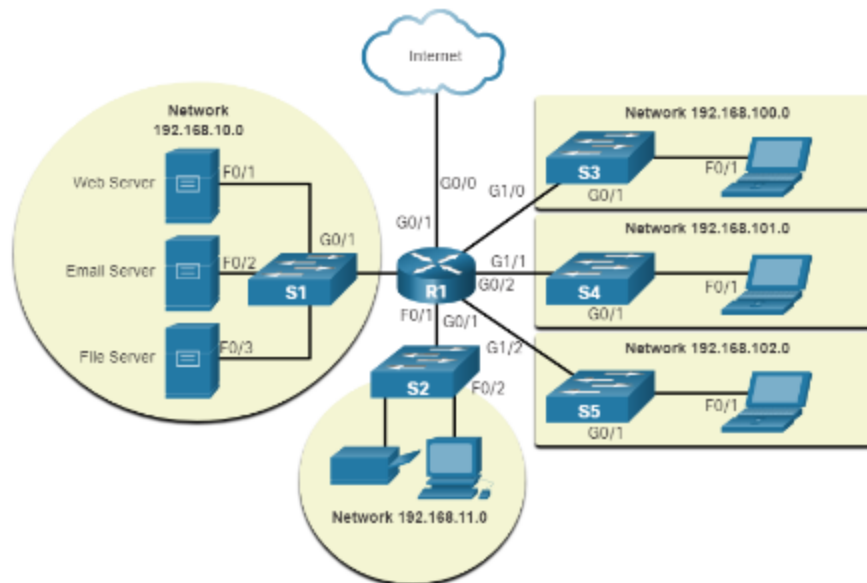
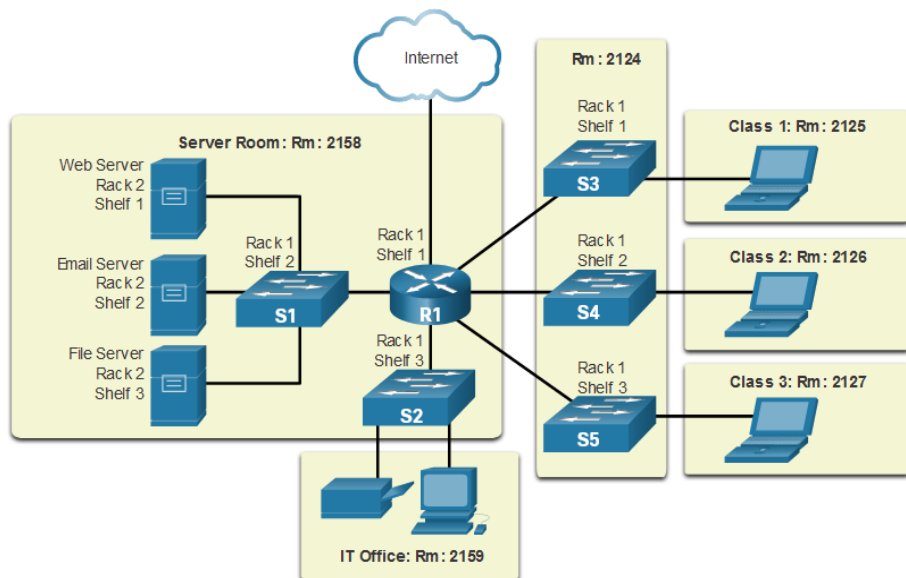


Беспроводная сеть



- Электрические импульсы;
- Импульсы света;
- Электромагнитное излучение.

# Диаграммы топологий



Схемы физической топологии — физическое расположение промежуточных устройств и кабельных линий.

Схемы логической топологии — определение устройств, портов и схемы адресации.



## Типы сетей

**Сетевые инфраструктуры могут в значительной мере отличаться по следующим критериям:**

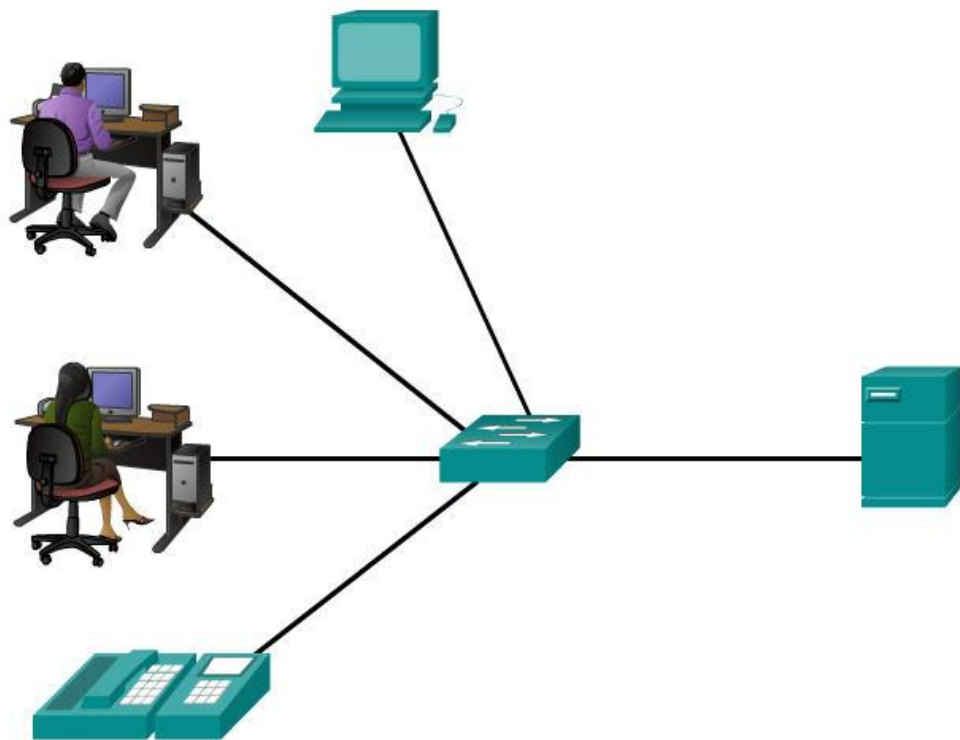
- Размер обслуживаемой территории
- Количество подключённых пользователей
- Число и типы доступных сервисов

Два наиболее распространённых типа сетевых инфраструктур:

- **локальная сеть (LAN)** — сетевая инфраструктура, которая обеспечивает доступ пользователям и оконечным устройствам в небольшой географической области;
- **глобальная сеть (WAN)** — сетевая инфраструктура, которая предоставляет доступ к другим сетям на обширной географической области.

Локальные сети LAN и сети WAN

# Локальные сети (LAN)



Сеть, обслуживающая дома, здания или территорию учебного заведения, считается локальной сетью (LAN).

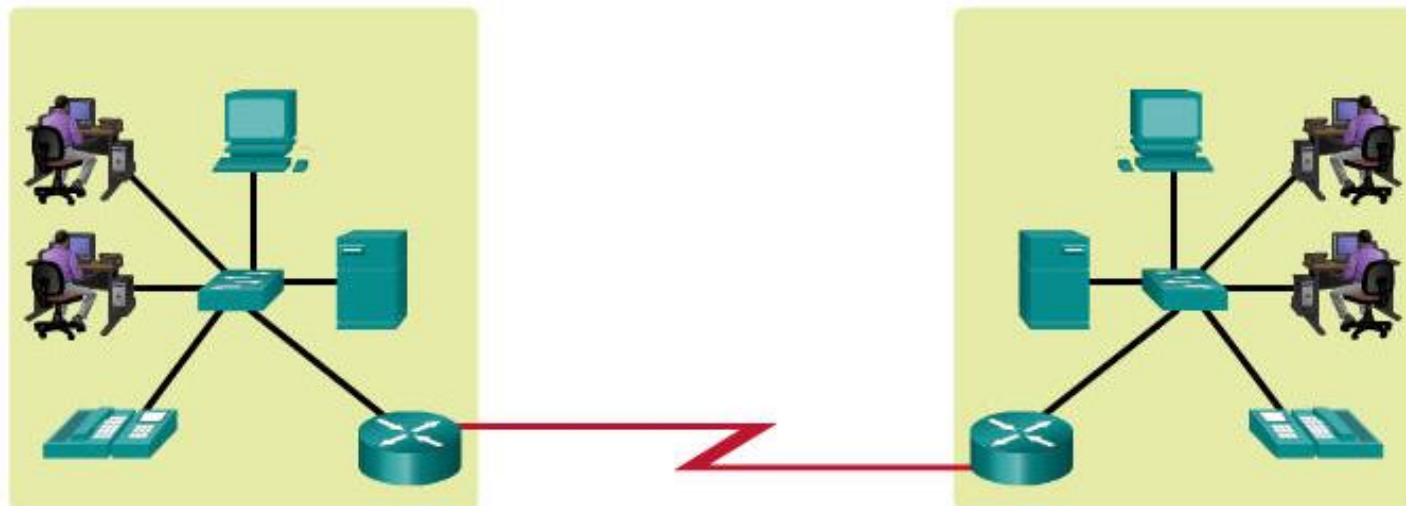
Локальные сети (LAN) — сетевая инфраструктура, которая охватывает небольшую географическую область.

Локальные сети связывают оконечные устройства в ограниченной области, например, в доме, школе, офисном здании или комплексе зданий.

Локальные сети WAN и сети WAN

# Глобальные сети (WAN)

Сеть WAN

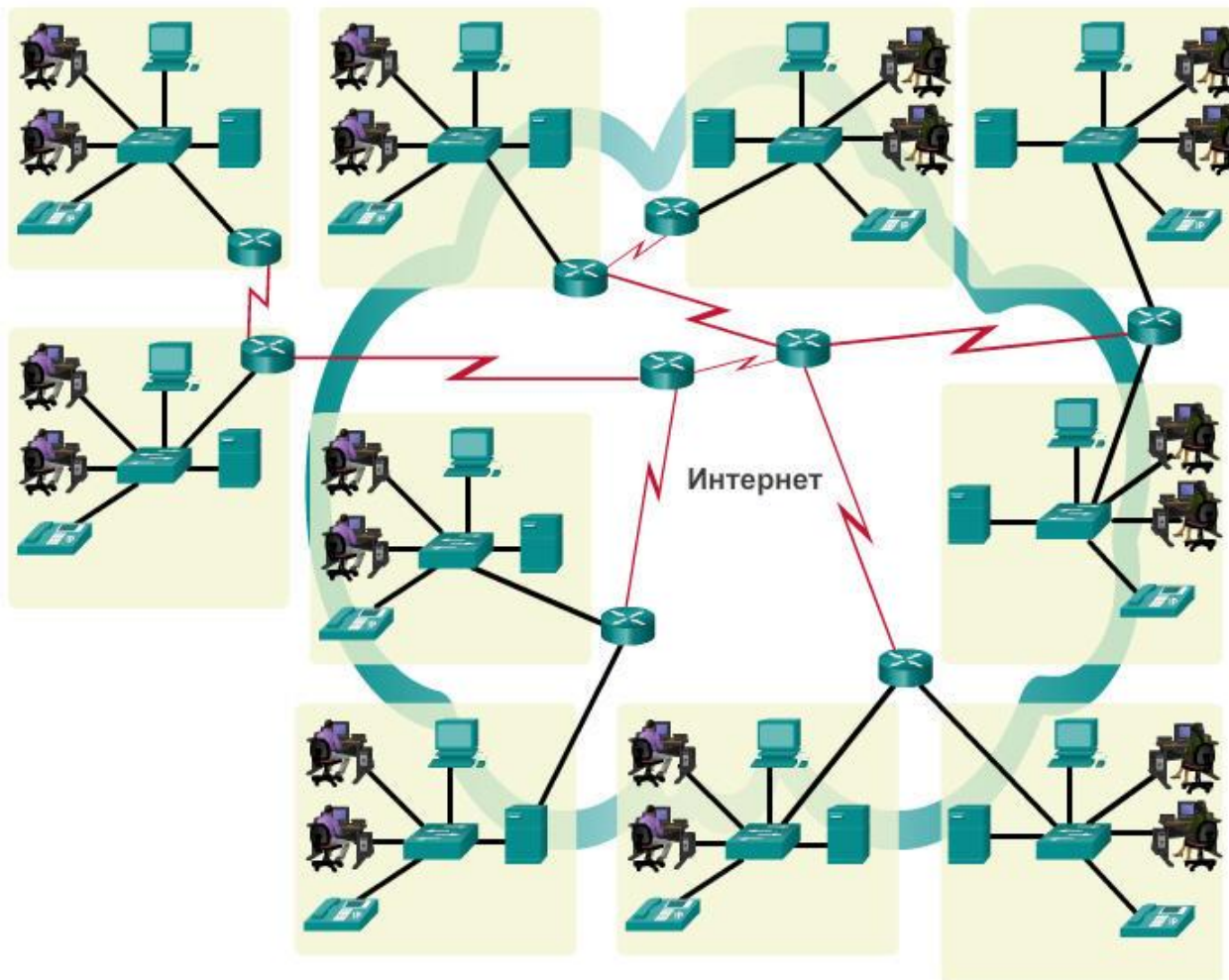


Локальные сети (LAN), разделённые географическим расстоянием, объединены сетью, которая называется глобальной (WAN).

Глобальные сети (WAN) — сетевая инфраструктура, которая охватывает обширную географическую область. Управление глобальными сетями обычно осуществляется операторами связи (SP) или Интернет-провайдерами (ISP).

# Локальные сети LAN, сети WAN и сети Интернет

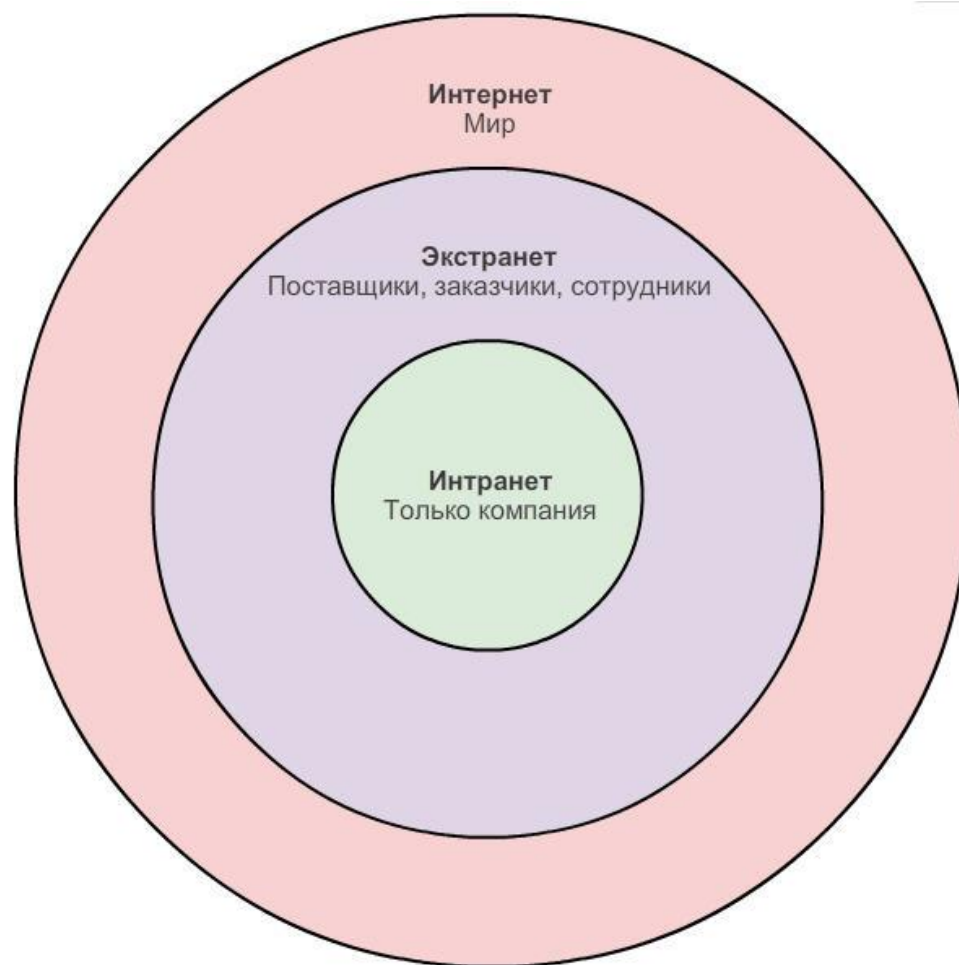
## Сеть Интернет



Локальные (LAN) и глобальные (WAN) сети могут быть подключены в объединённую сеть.



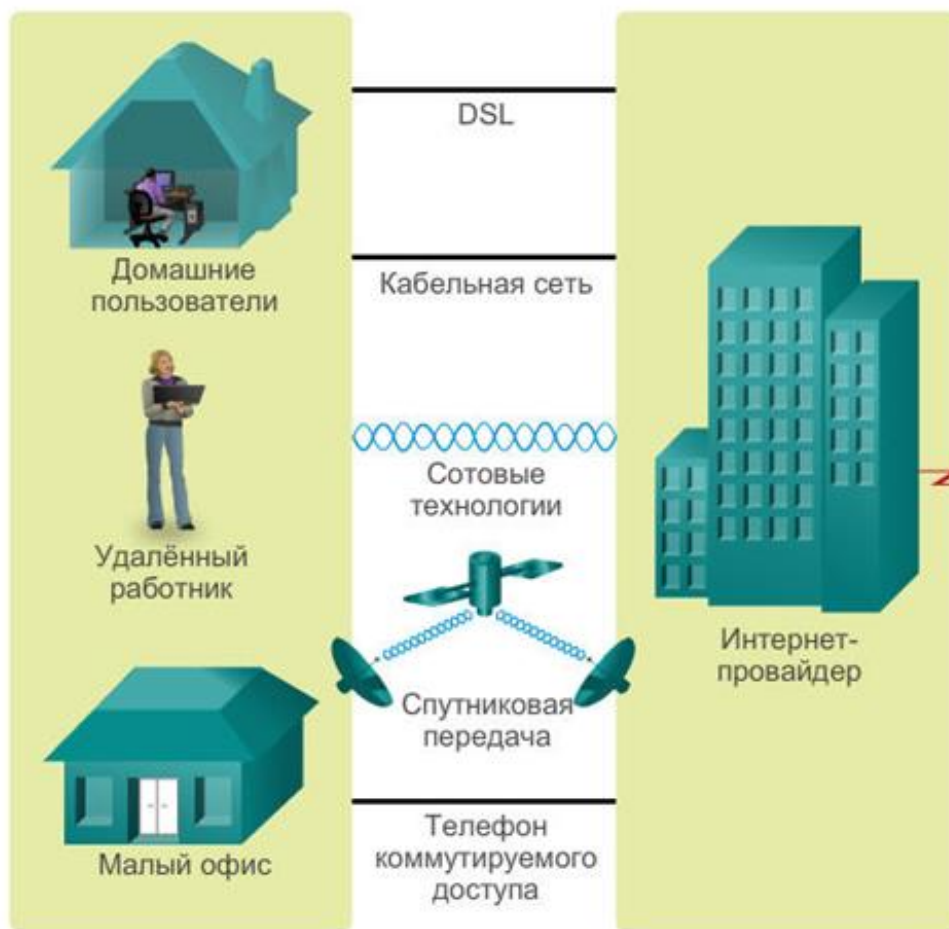
# Инtranет и Экстрaнет



Термин «**Инtranет**» (внутренние сети) часто используется для обозначения локальных и глобальных сетей, которые принадлежат организации и доступны только её членам, сотрудникам и прочим авторизованным лицам.

Организация может использовать **Экстрaнет** (внешние сети) для обеспечения защищённого и безопасного доступа сотрудников, которые работают в различных организациях и которым необходимы данные компании.

# Подключение удалённых пользователей малых и домашних офисов к сети Интернет



**DSL:** обеспечивает подключение к Интернету с высокой пропускной способностью и постоянным доступом к сети. Используется высокоскоростной модем, разделяющий цифровой сигнал от телефонного, и Ethernet-соединение для подключения компьютера или сети LAN. DSL работает по телефонной линии, разделённой на три канала: для телефонных вызовов голосовой связи, канал загрузки для получения информации из Интернета и для отправки информации. Чем дальше пользователь находится от центральной телефонной станции, тем медленнее соединение.

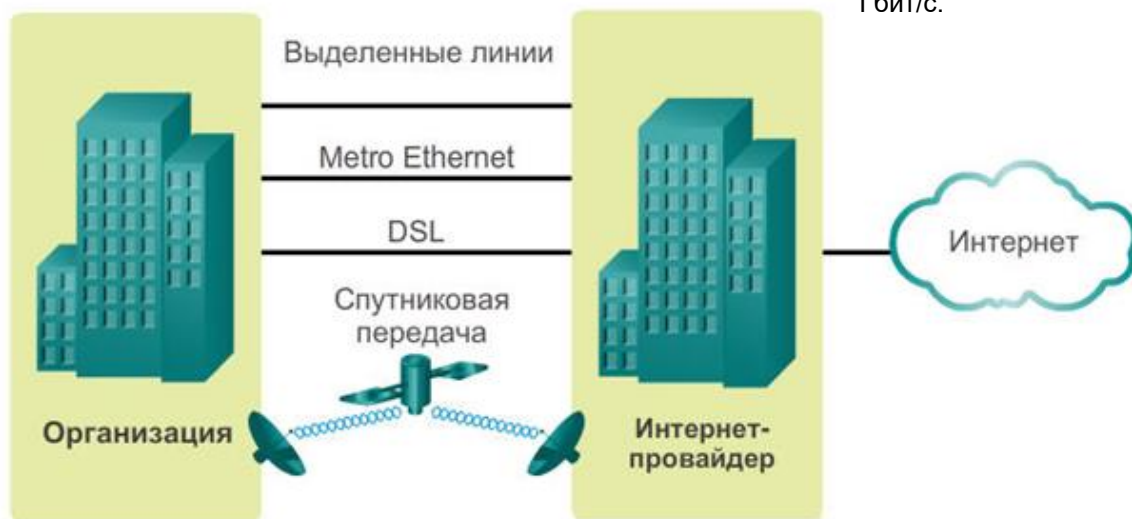
**Кабельное подключение:** сигнал данных Интернета передаётся по тому же коаксиальному кабелю, который используется для передачи сигналов кабельного телевидения. Этот способ обеспечивает подключения к Интернету с высокой пропускной способностью и постоянным доступом к сети. Специальный кабельный модем отделяет сигналы Интернет от других, при этом Ethernet-порт используется для подключения компьютера или сети LAN.

**Сотовая связь:** используется мобильная телефонная сеть. В любой точке, где доступен сотовый сигнал, можно получить сотовый доступ в Интернет.

**Спутниковая связь:** является удобным вариантом для дома или офиса, не имеющего доступа к цифровой абонентской линии (DSL) или кабелю. Спутниковые антенны требуют беспрепятственной прямой видимости спутника и, следовательно, могут быть трудно применимы в лесистых местностях или в местах с другими наземными препятствиями.

**Телефонный коммутируемый доступ:** недорогой способ, в котором используется телефонная линия и модем. Для подключения к Интернет-провайдеру пользователь вызывает телефонный номер доступа провайдера. Подключение по коммутируемой линии обеспечивает низкую пропускную способность.

# Подключение компаний к сети Интернет



**Выделенная арендуемая линия** — это выделенное подключение от оператора связи до абонентского оборудования в виде фактически зарезервированных каналов, которые объединяют географически разделённые офисы для голосовой связи и/или передачи данных. **Стандарт Metro Ethernet** обычно доступен от оператора до абонентского оборудования по выделенным медным или оптоволоконным линиям со скоростью подключения (пропускной способностью) от 10 Мбит/с до 10 Гбит/с.

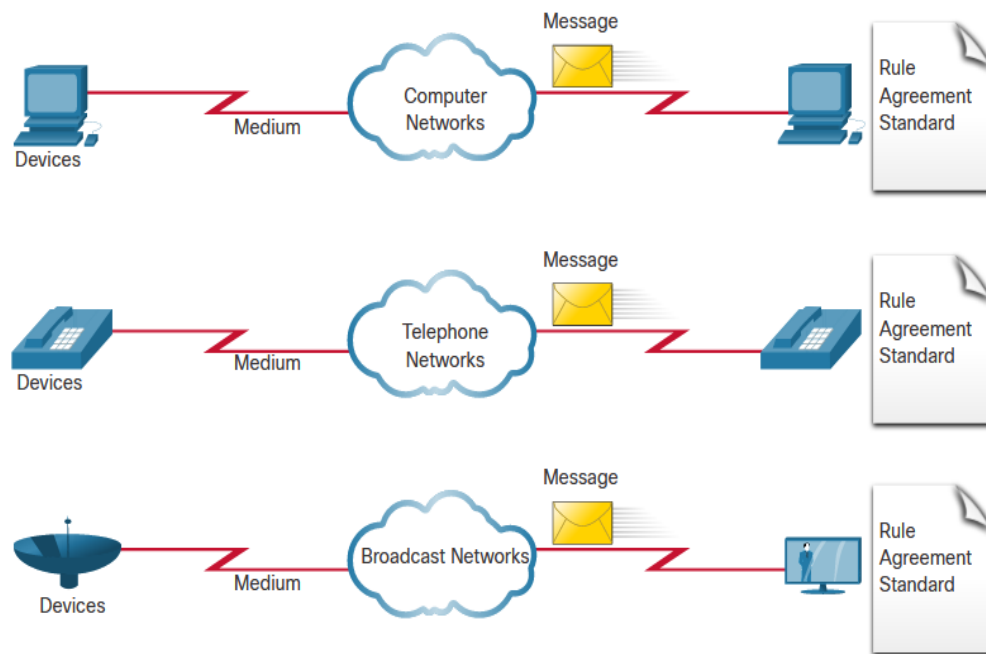
**DSL:** DSL-подключение для предприятий доступно в различных форматах. Популярный выбор — симметричные цифровые абонентские линии (SDSL), подобные асимметричной цифровой абонентской линии (ADSL), но обеспечивающие равную скорость получения и отправки файлов. ADSL призвана обеспечить пропускную способность с разной скоростью передачи входящего и исходящего трафика. Например, клиент доступа в Интернет может иметь скорость входящего трафика в диапазоне от 1,5 до 9 Мбит/с и диапазон пропускной способности исходящего трафика от 16 до 640 Кбит/с. Соединения ADSL работают на расстояния до 5 км 488 м по одной медной витой паре.

**Спутниковая связь** способна обеспечить соединение при отсутствии проводных решений. Спутниковые антенны требуют беспрепятственной прямой видимости спутнику. Стоимость оборудования и установки может быть высокой, с умеренной ежемесячной платой. Эти подключения медленнее и, как правило, менее надёжны по сравнению с наземными вариантами, что делает их менее привлекательными по сравнению с другими решениями.

# Конвергентные сети

До конвергентных сетей организация должна была иметь отдельный кабель для телефона, видео и данных. Каждая из этих сетей использует различные технологии для передачи сигнала.

Каждая из этих технологий использует свои правила и стандарты.

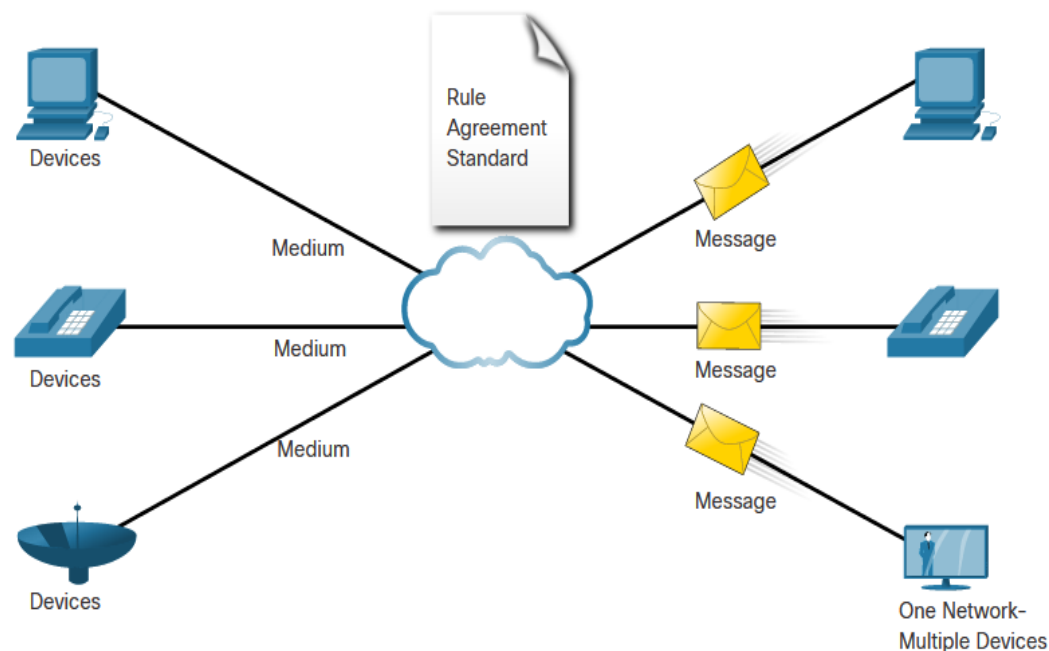


# Конвергентные сети

Конвергентные сети передачи данных обеспечивают работу несколько служб в одном канале, включая:

- данные
- голос
- видео

В отличие от выделенных сетей конвергентные сети позволяют передавать данные, голос и видео между различными типами устройств при использовании одной и той же сетевой инфраструктуры. Сетевая инфраструктура использует один и тот же набор правил и стандартов.



# Поддержка сетевой архитектуры

**Сетевая архитектура** — это технологии, поддерживающие инфраструктуру и обеспечивающие обмен данными по сети.

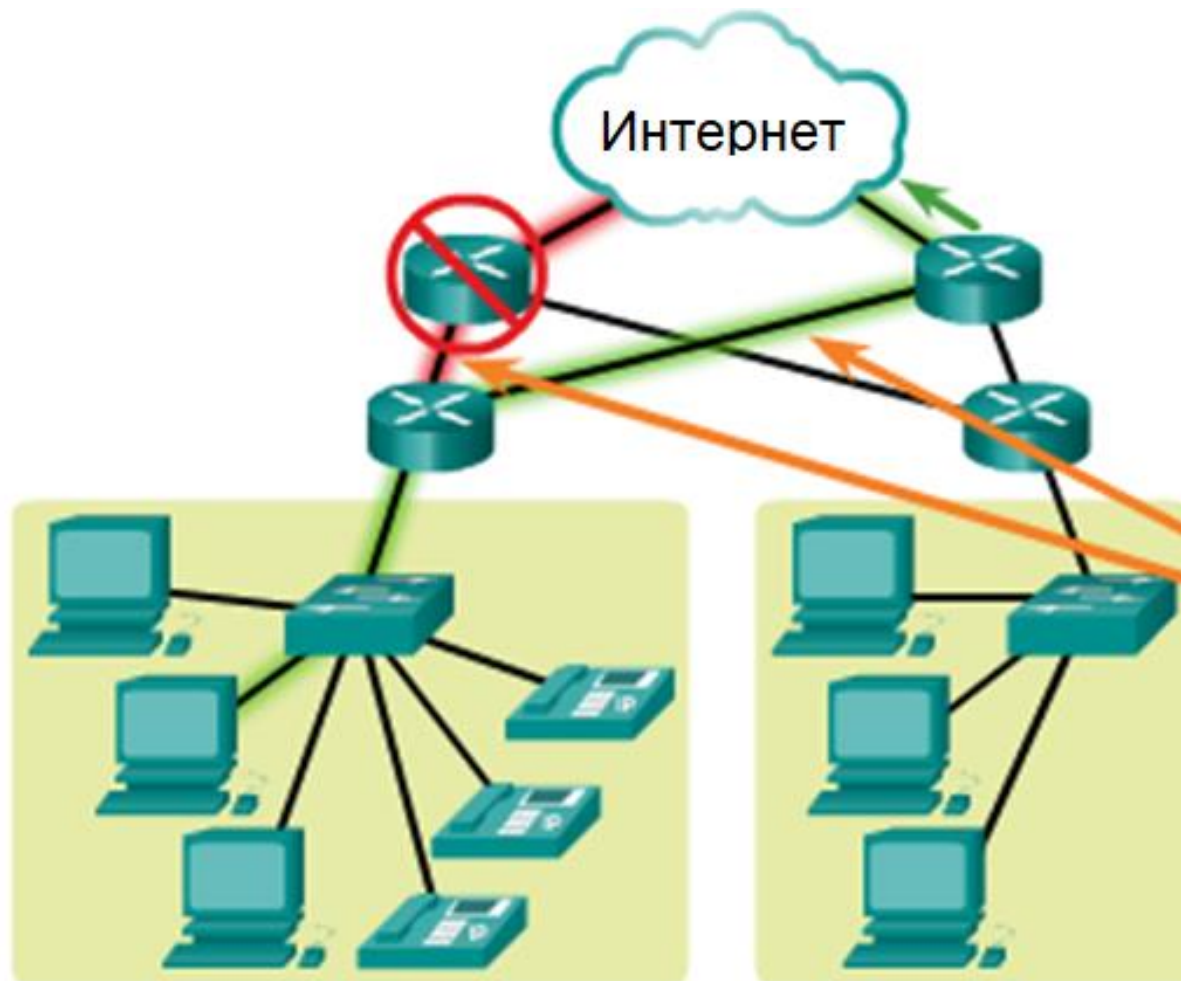
Существует **четыре базовые характеристики**, которыми должна обладать базовая сетевая архитектура в соответствии с ожиданиями пользователей:

- Отказоустойчивость
- Масштабируемость
- Гарантированная полоса пропускания (QoS)
- Безопасность



Надёжная сеть

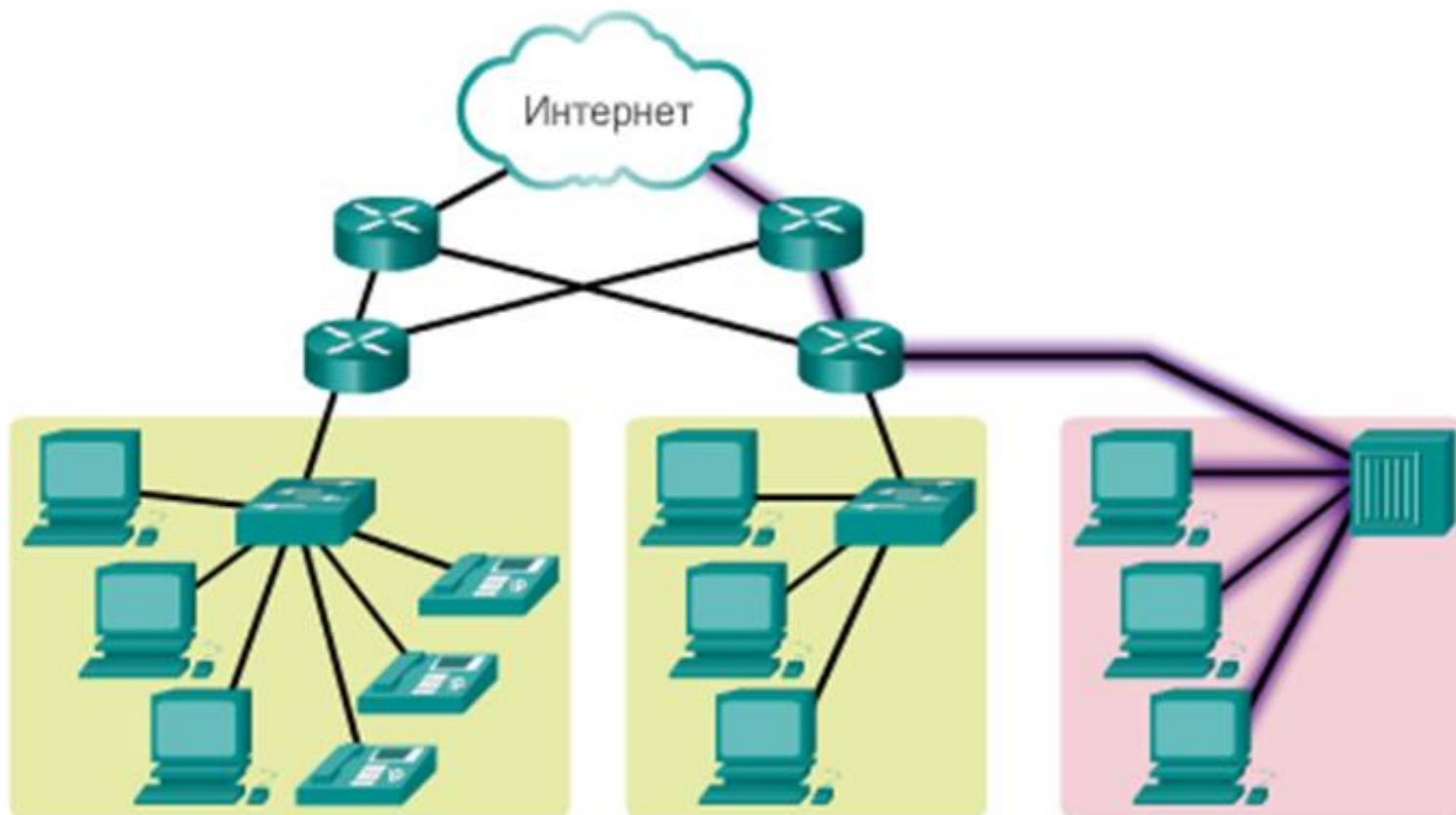
# Отказоустойчивость



Резервные соединения позволяют использовать альтернативные пути при сбое устройства или канала. Взаимодействие с пользователем остается без изменений.

Надёжная сеть

# Масштабируемость

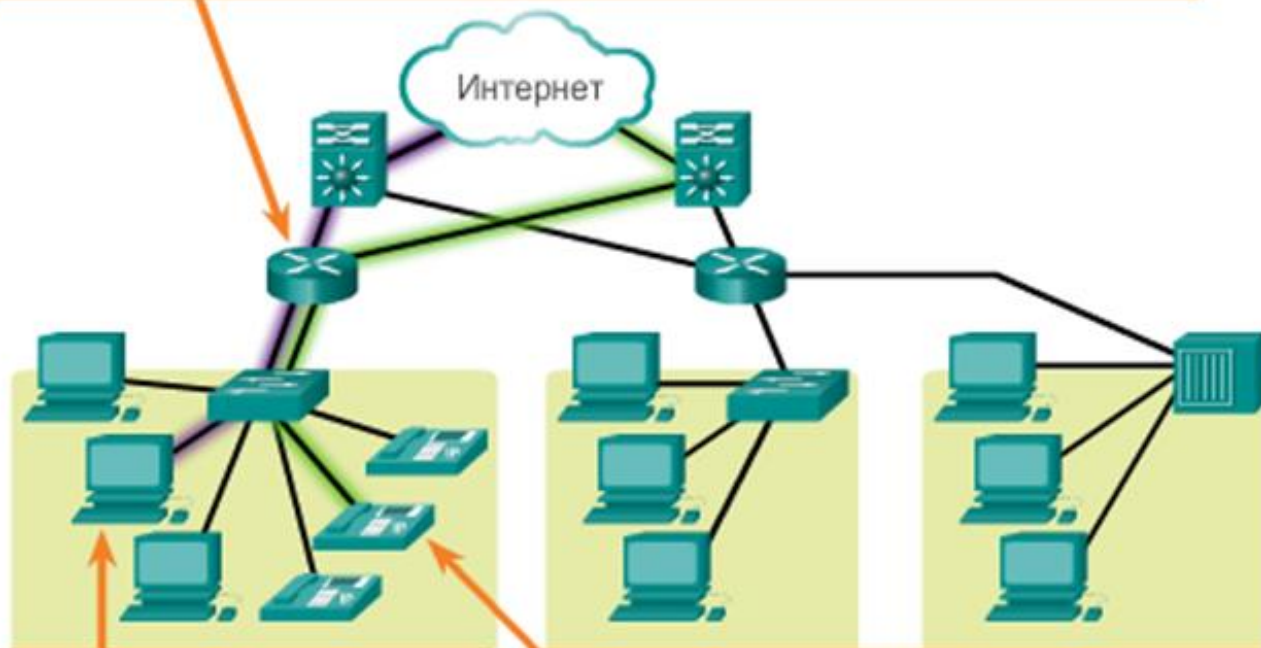


Дополнительные пользователи и целые сети могут быть подключены к Интернету без снижения производительности для существующих пользователей

## Надёжная сеть

# Гарантированная полоса пропускания – качество обслуживания(QoS)

Качество обслуживания, управляемое маршрутизатором, гарантирует, что приоритеты соответствуют типу коммуникации и её важности для организации.



Веб-страницы, как правило, получают более низкий приоритет.

Потоковому мультимедиа необходим приоритет для поддержания точного и непрерывного взаимодействия с пользователем.

Примеры приоритетных решений для организации.

- Чувствительный к задержкам обмен данными: **повышенный приоритет** таких служб, как телефония или распределение видеосигналов.
- Нечувствительный к задержкам обмен данными: **пониженный приоритет** получения веб-страниц и сообщений электронной почты.
- Высокая степень важности для организаций: **повышенный приоритет** контроля производства или данных о бизнес-операциях.
- Нежелательный обмен данными: **снижение приоритета или блокировка несанкционированной активности**, такой как обмен файлами между одноранговыми узлами или интерактивные развлечения.

# Безопасность

Необходимо учесть два основных типа безопасности сети:

- **Информационная безопасность сетевой инфраструктуры**

- Физическая безопасность сетевых устройств
- Предотвращение несанкционированного доступа

- **Безопасность информации**

- Защита информации или данных, передаваемых по сети

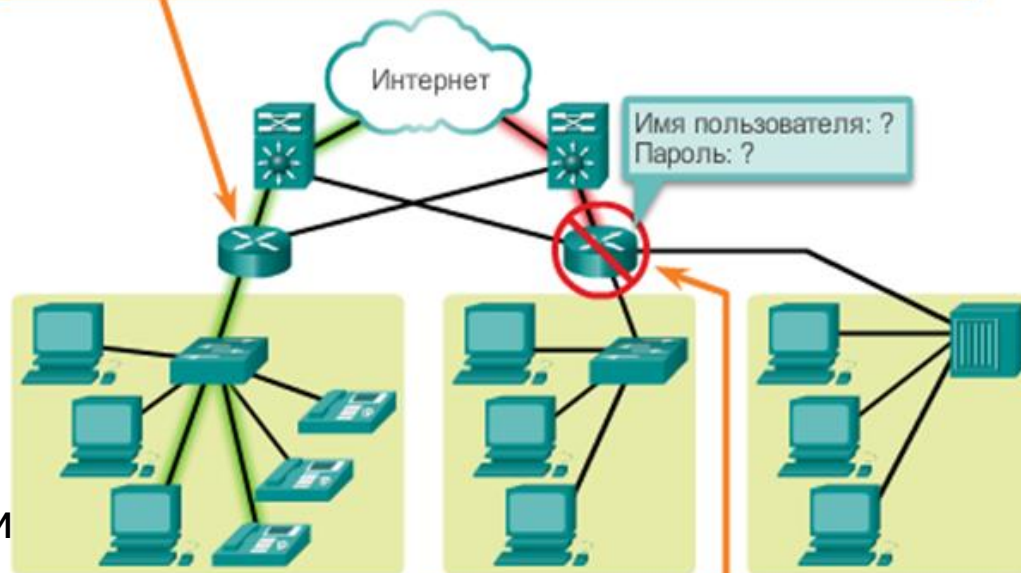
Три цели обеспечения безопасности сети:

**Конфиденциальность** — только указанные получатели могут считывать данные.

**Целостность** — гарантия того, что данные не будут изменены во время передачи.

**Доступность** — обеспечение своевременного и надежного доступа к данным для авторизованных пользователей.

Администраторы могут защитить сеть с помощью программного и аппаратного обеспечения безопасности, предотвращая тем самым физический доступ к сетевым устройствам.



Меры безопасности защищают сеть от несанкционированного доступа.





Тенденция развития сетей

# Новые тенденции в развитии сетевых технологий

Среди некоторых основных тенденций можно выделить следующие:

- концепция «Принеси своё собственное устройство» (BYOD);
- совместная работа через сеть Интернет;
- видеосвязь;
- облачные вычисления.

# Технологические тенденции в домашних сетях

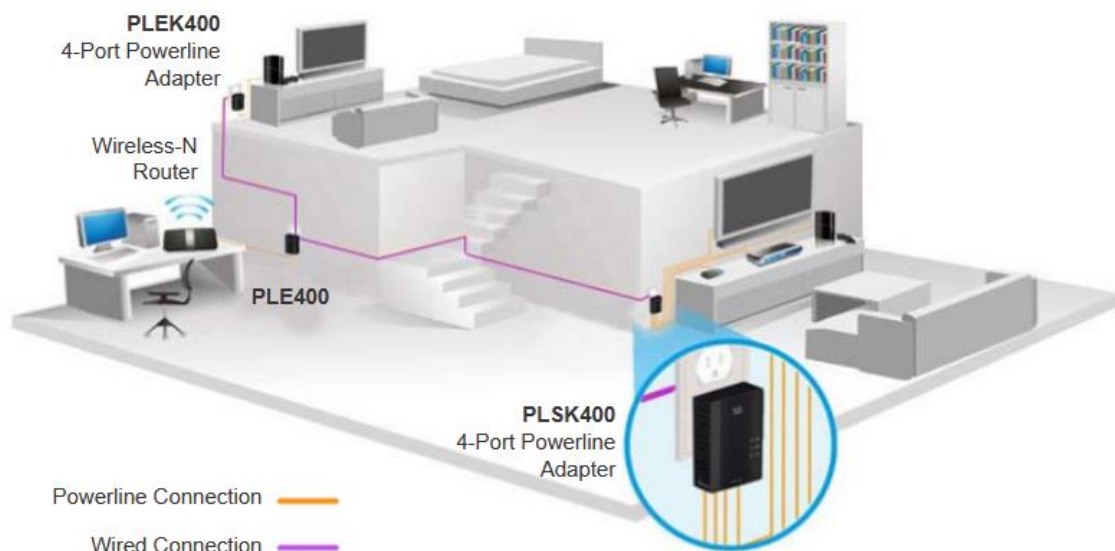


- Технология «умный дом» — это развивающаяся тенденция, которая позволяет интегрировать технологии в бытовые устройства, позволяя им связываться с другими устройствами.
- Микроволновая печь может узнать, в какое время нужно начинать готовить, сверившись с календарем, в котором отмечено, когда вы планируете вернуться домой.
- Технология «Умный дом» в настоящее время разрабатывается для всех комнат в доме.



Тенденции развития сетей

# Организация сети по линиям электропередачи



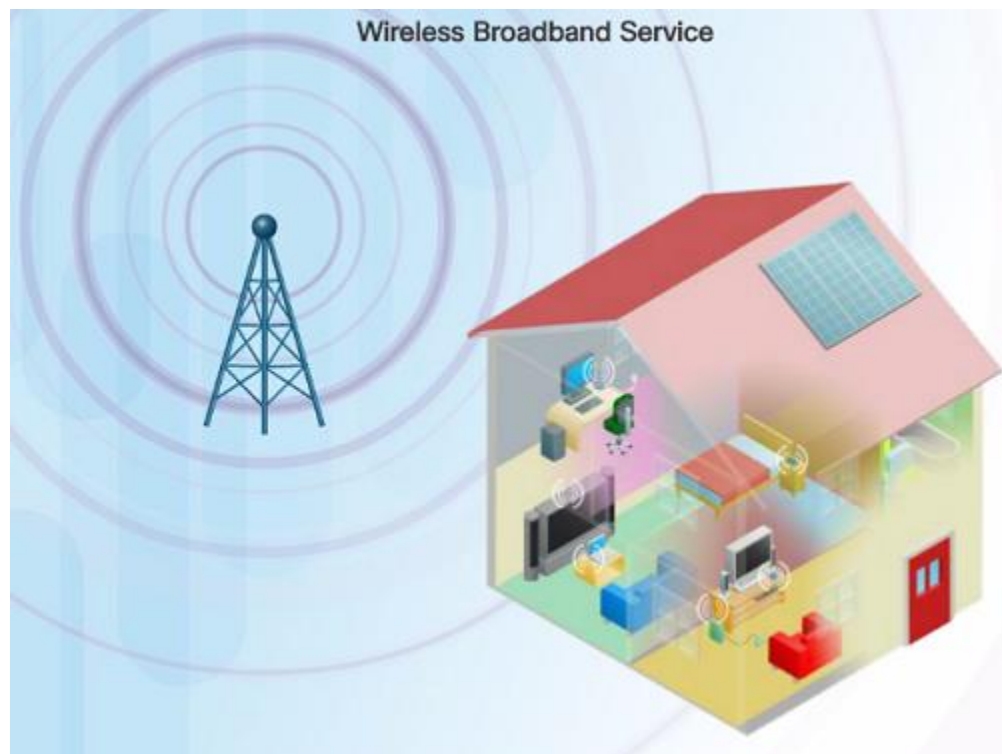
Организация сети по линиям электропередачи позволяет устройствам подключаться к локальной сети в тех случаях, когда нецелесообразно использовать кабельные или беспроводные сети передачи данных.

При помощи стандартного адаптера сети электропитания устройства могут подключаться к локальной сети везде, где есть электрические розетки, отправляя данные на определенных частотах.

Организация сети по линиям электропитания особенно полезна там, где невозможно использовать точки беспроводного доступа или они не обеспечивают доступ для всех устройств в доме.

# Беспроводной широкополосный доступ

Для подключения к сети Интернет домов и небольших компаний, помимо кабельных или DSL-подключений, также используются беспроводные сети.



- Провайдеры беспроводного интернет-доступа (WISP), которые чаще всего работают в сельской местности, — это поставщики услуг Интернета, которые подключают абонентов к назначенным точкам доступа.
- Беспроводной широкополосный доступ — это еще одно решение для домашних сетей и небольших компаний.
  - Используется та же сотовая технология, что и для смартфонов.
  - Антенна устанавливается снаружи дома, обеспечивая беспроводное или проводное подключение устройств в любой точке дома.



# Базовая конфигурация коммутатора и оконечного устройства

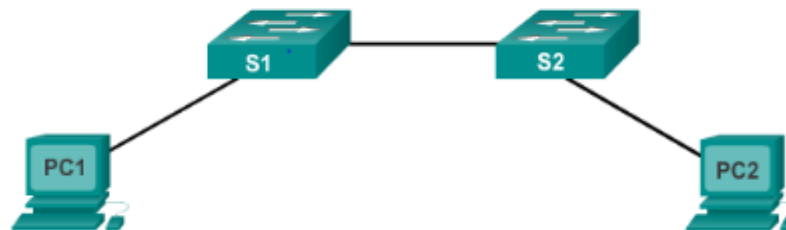


## Введение в сетевые технологии

# Операционные системы

Всё сетевое оборудование, зависящее от операционных систем

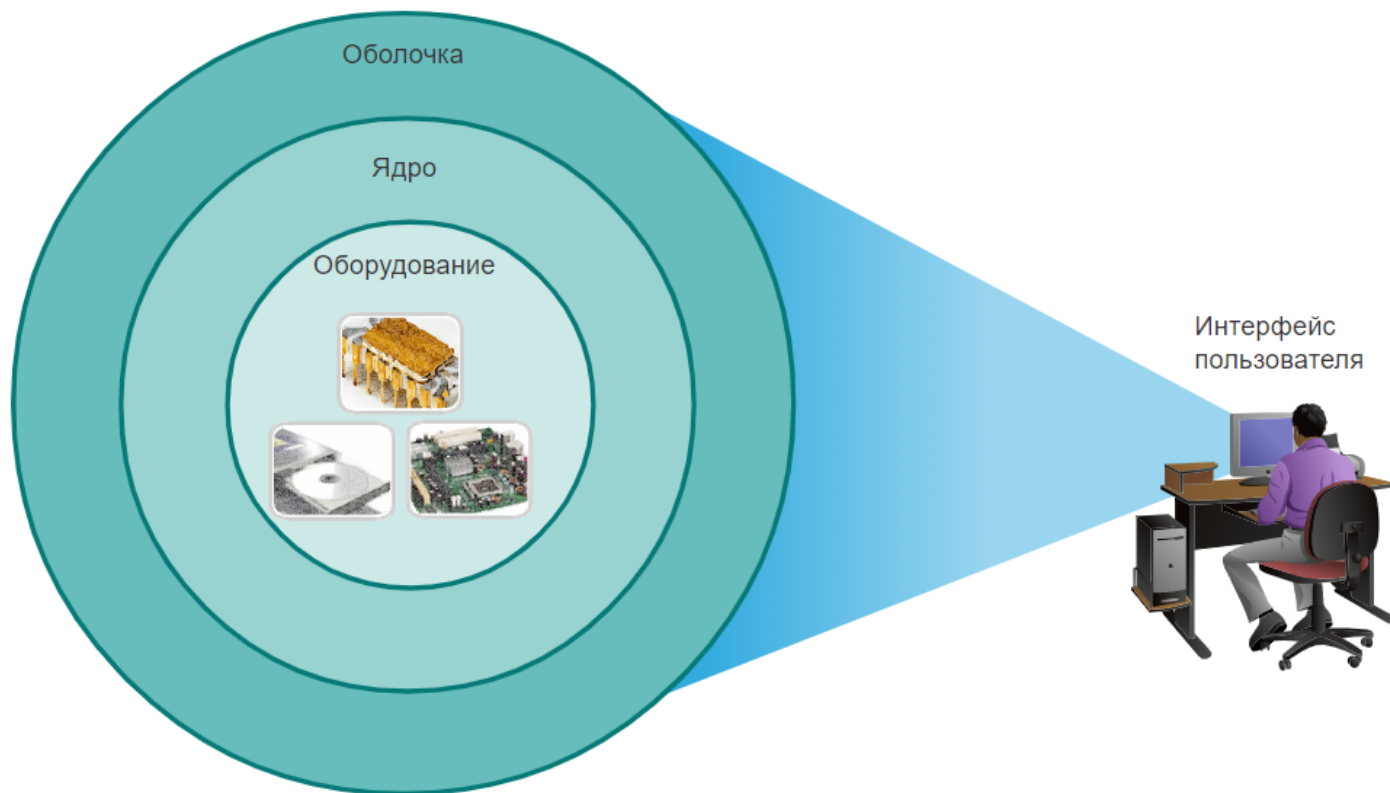
- Конечные пользователи (ПК, ноутбуки, смартфоны, планшетные компьютеры)
- Коммутаторы
- Маршрутизаторы
- Точки беспроводного доступа
- Межсетевые экраны



## Операционная система сетевого взаимодействия Cisco (IOS)

- Общее наименование различных вариантов сетевых операционных систем, используемых на устройствах Cisco

# Операционные системы



- **Оболочка** – пользовательский интерфейс, позволяющий пользователям запрашивать определенные задачи с компьютера. Эти запросы могут быть сделаны либо через интерфейс CLI, либо через интерфейс GUI.
- **Ядро** – часть операционной системы, обеспечивающая взаимодействие аппаратных средств и программного обеспечения компьютера, распределение системных ресурсов и т.д.
- **Оборудование** – электронные и иные «физические» компоненты компьютера.

# Доступ к Cisco IOS

## Назначение ОС

При помощи GUI пользователь операционной системы ПК может выполнять следующие задачи.

- Выбирать различные объекты и запускать программы, используя мышь.
- Вводить текст и текстовые команды.
- Просматривать выходные данные на экране монитора.

Примеры: Windows, macOS, Linux KDE, Apple iOS и Android.



Сетевая операционная система IOS на основе интерфейса командной строки позволяет сетевому специалисту выполнять следующие действия:

- Запускать сетевые программы на базе CLI, используя клавиатуру.
- Вводить текст и текстовые команды с клавиатуры.
- Просматривать выходные данные на экране монитора.

Сетевые устройства Cisco работают под управлением определенных версий Cisco IOS. Версия IOS зависит от типа используемого устройства и необходимых функций. Все сетевые устройства по умолчанию поставляются с ОС IOS.

Можно обновить версию IOS и получить дополнительные возможности.

```
analyst@secOps ~]$ ls
Desktop Downloads lab.support.files second_drive
[analyst@secOps ~]$
```





## Доступ к Cisco IOS

# Способы доступа к сетевому устройству

- Коммутатор будет пересылать трафик по умолчанию, и его не нужно явно настраивать для работы. Например, два настроенных узла, подключенных к одному и тому же новому коммутатору, смогут обмениваться данными.
- Независимо от поведения нового коммутатора по умолчанию, все коммутаторы должны быть настроены и защищены.

Метод	Описание
Консоль	Это физический порт управления, обеспечивающий внеполосный доступ к устройству Cisco. Внеполосный доступ осуществляется 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 сервисов, например, во время начальной настройки сетевого устройства. Для подключения к консоли требуется компьютер с программным обеспечением эмуляции терминала и специальный кабель консоли для подключения к устройству.
Протокол Secure Shell (SSH)	Secure Shell (SSH)— метод, позволяющий удаленно установить защищенное подключение CLI через виртуальный интерфейс по сети. В отличие от консольного подключения для SSH-подключений на устройстве должны быть активны сетевые службы, включая активный интерфейс с настроенным адресом. Большинство версий Cisco IOS содержит SSH-сервер и SSH-клиент, который можно использовать для SSH-соединения с другими устройствами.
Telnet	Telnet— это незащищенный протокол, позволяющий удаленно начать сеанс CLI через виртуальный интерфейс по сети. В отличие от SSH, Telnet не обеспечивает безопасное зашифрованное соединение и должен использоваться только в лабораторной среде. Данные для аутентификации пользователя, пароли и команды передаются по сети в виде простого текста. Лучше всего использовать SSH вместо Telnet. Cisco IOS включает в себя как сервер Telnet, так и клиент Telnet.

## Доступ к Cisco IOS

# Программы эмуляции терминала

Существует несколько программ эмуляции терминала, используемых для подключения к сетевым устройствам при помощи последовательного подключения через консольный порт либо посредством подключения по протоколам SSH/Telnet. Эти программы позволяют работать эффективнее за счет регулировки размера окон, изменения размера шрифтов и цветовых схем.

PuTTY

Tera Term

SecureCRT

PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
- Selection
- Colours
- Connection
  - Data
  - Proxy
  - Telnet
  - Rlogin
  - SSH
  - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type:

☐ Raw ☐ Telnet ☐ Rlogin ☒ SSH ☐ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:

☐ Always ☐ Never ☒ Only on clean exit

About Help Open Cancel

# Основные командные режимы

## Пользовательский режим

Ограниченная проверка маршрутизатора. Удалённый доступ.

Switch>  
Router>

Пользовательский режим разрешает выполнять ограниченный круг базовых команд для мониторинга. Также его часто называют режимом «только для просмотра».

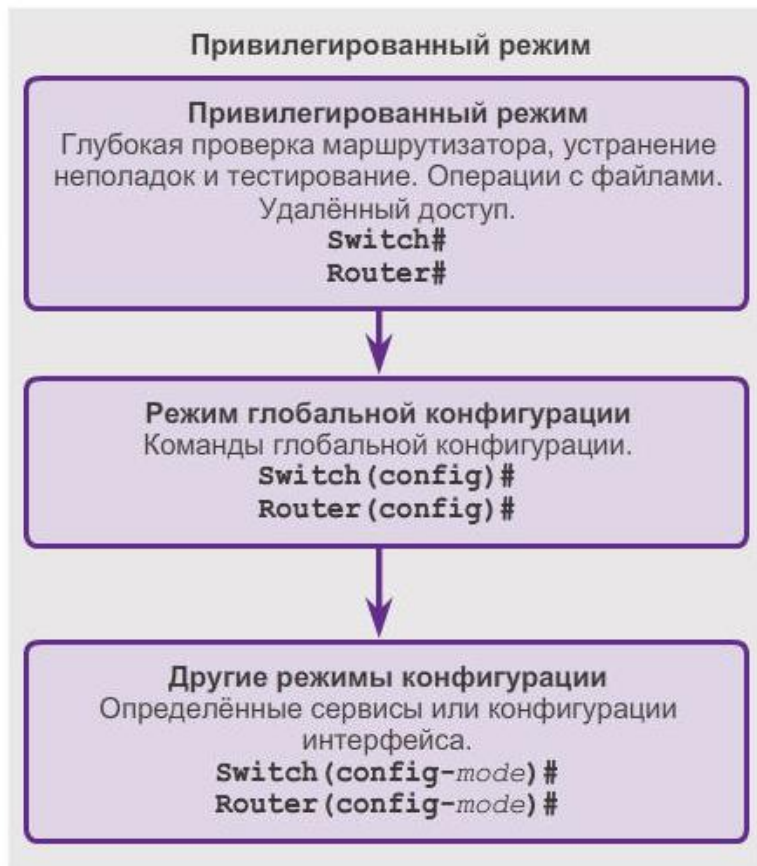
В Привилегированном режиме по умолчанию можно выполнять все команды для мониторинга, управления и изменения конфигурации.

## Привилегированный режим

Глубокая проверка маршрутизатора. Устранение неполадок и тестирование. Операции с файлами. Удалённый доступ.

Switch#  
Router#

# Режим глобальной конфигурации и его дополнительные режимы



- Switch# **configure terminal**
- Switch(config)#

## Режим глобальной конфигурации и дополнительные режимы

Структура запроса IOS

```
Router>ping 192.168.10.5

Router#show running-config

Router (config) #Interface FastEthernet 0/0

Router (config-if) #ip address 192.168.10.1 255.255.255.0
```

Запрос изменяется для назначения текущего интерфейса командной строки (CLI).

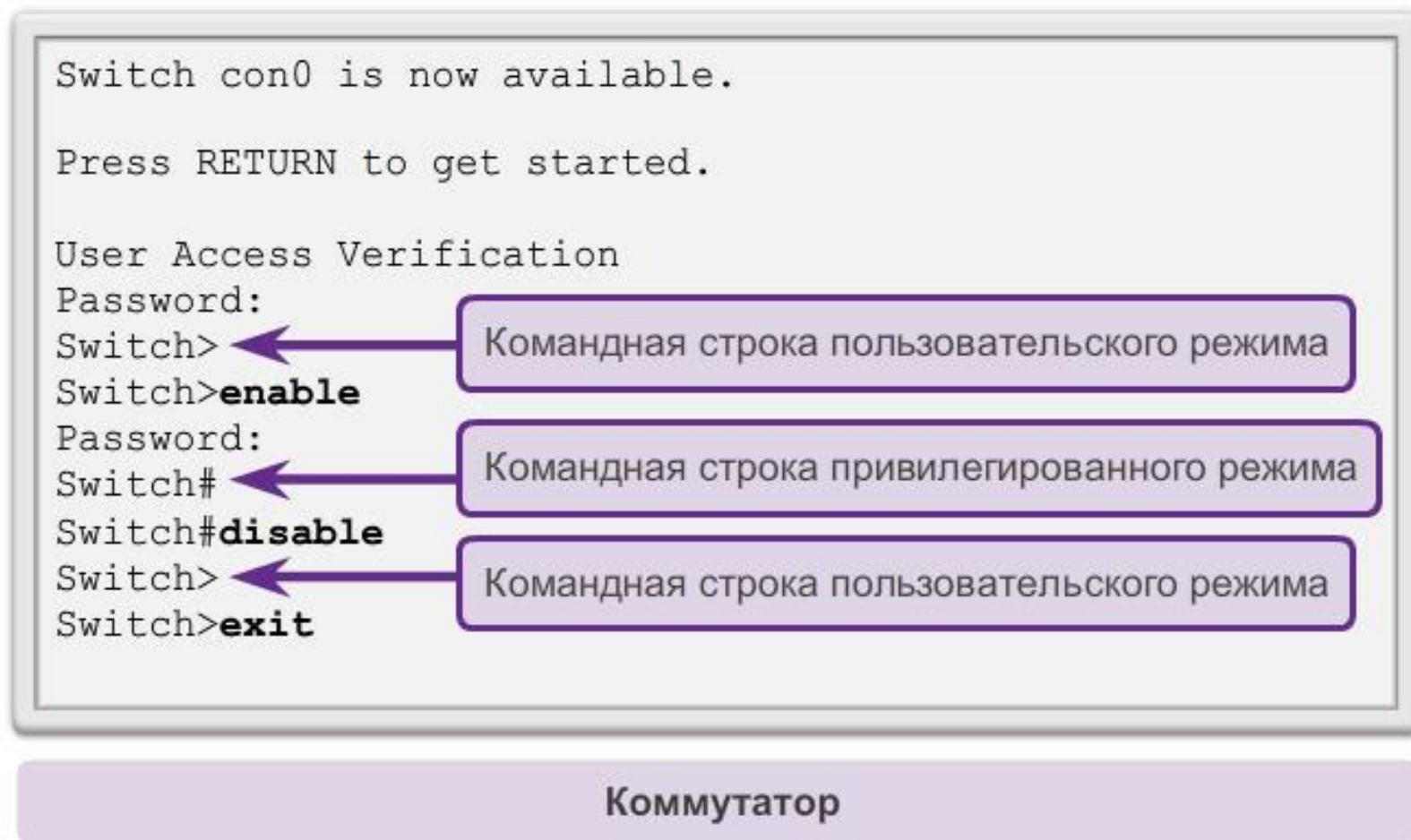
```
Switch>ping 192.168.10.9

Switch#show running-config

Switch (config) #Interface FastEthernet 0/1

Switch (config-if) #Description connection to WEST LAN4
```

# Переключение между режимами IOS



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



# Переключение между режимами IOS (продолж.)

Чтобы перейти из режима глобальной конфигурации в привилегированный режим, или из любого дополнительного режима глобальной конфигурации в режим на один уровень выше в иерархии режимов, необходимо ввести команду **exit**.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

```
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#end
Switch#
```

Чтобы перейти из любого дополнительного режима глобальной конфигурации в привилегированный режим, введите команду **end** или используйте сочетание клавиш **Ctrl+Z**.

```
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#line vty 0 4
Switch(config-line)#interface fastethernet 0/1
Switch(config-if)#end
Switch#
```



# Базовая структура команд IOS



Каждая команда IOS имеет определённый формат или синтаксис. Каждая команда выполняется только из соответствующего режима.

Команды не чувствительны к регистру. Вслед за текстом команды вводится одно или несколько **ключевых слов** и **аргументов (параметров)**.

**Ключевое слово** — это особый параметр, определенный в операционной системе (на рисунке — **ip protocols**).

**Аргумент** — не задан заранее, это значение или переменную определяет пользователь (на рисунке — **192.168.10.5**).

## Структура команды

# Контекстная справка

```
Switch#cl?  
clear clock
```

Параметры команд:  
отображают список команд  
или ключевых слов,  
которые начинаются с  
символов **cl**

```
Switch#clock set ?  
hh:mm:ss Current Time
```

Объяснение команд: IOS  
отображает список  
последующих параметров  
или переменных и  
приводит к ним пояснение.

```
Switch#clock set 19:50:00 ?  
<1-31> Day of the month  
MONTH Month of the year
```

Объяснение команд с  
несколькими параметрами  
или переменными

```
Switch#clock set 19:50:00 25 June 2012  
Switch#
```

В операционной  
системе IOS  
доступно  
несколько видов  
справки:

- контекстная справка;
- проверка синтаксиса команды;
- горячие клавиши и клавиши быстрого вызова.

## Структура команды

# Проверка синтаксиса команды

## Неполная команда

```
Switch#>clock set  
% Incomplete command.  
Switch#clock set 19:50:00  
% Incomplete command.
```

IOS открывает сообщение справки, в котором указано, что в конце команды нет необходимых ключевых слов или параметров.

## Неоднозначная команда

```
Switch#c  
% Ambiguous command: 'c'
```

IOS открывает сообщение справки, когда командный процессор не может прочитать неправильно введенную команду.

## Неверная команда

```
Switch#clock set 19:50:00 25 6  
                        ^  
% Invalid input detected at '^'  
marker.
```

IOS показывает знак "^", чтобы указать место, которое не может прочитать командный процессор.

Существует три различных типа сообщений об ошибках:

- неоднозначная команда;
- неполная команда;
- неверная команда

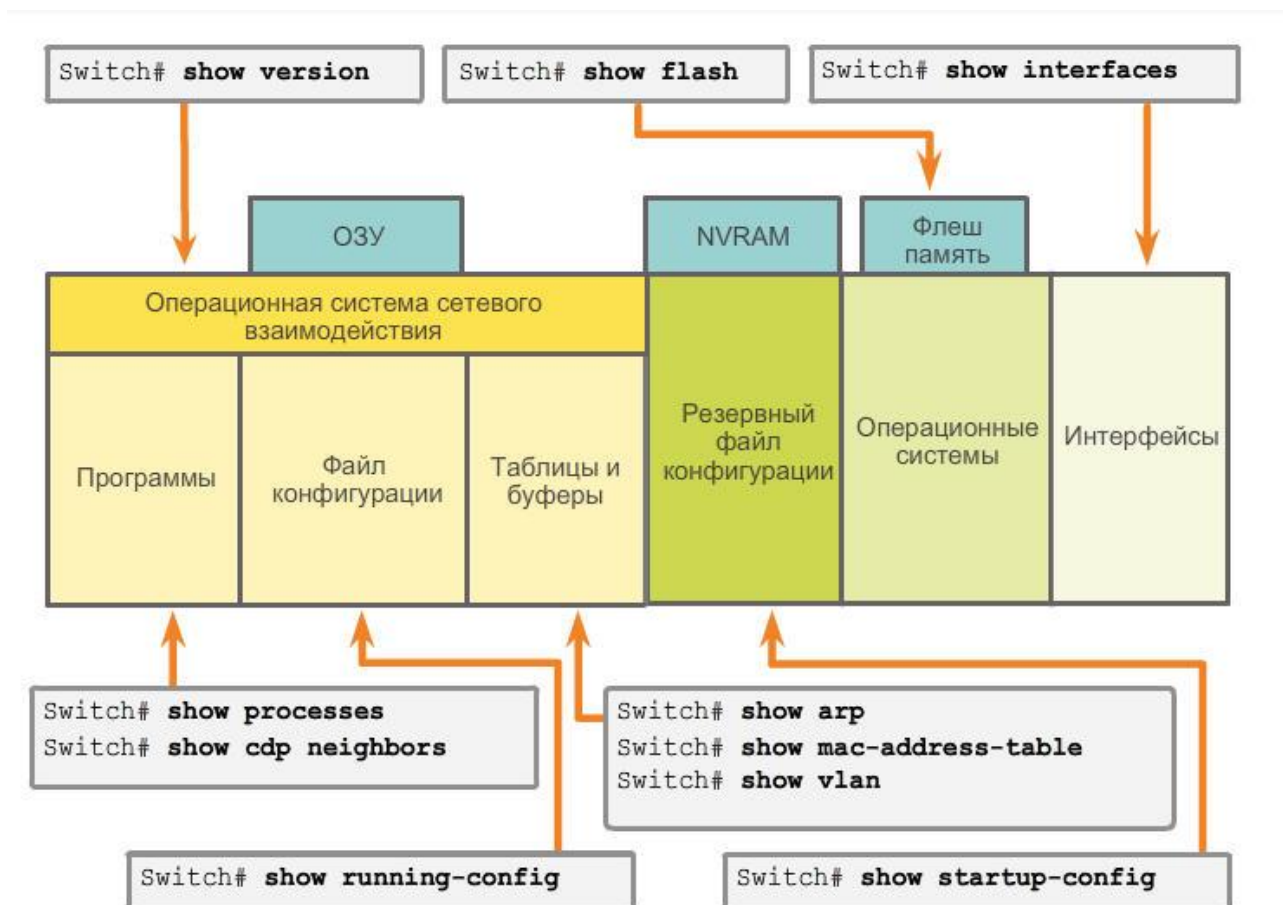


# Горячие клавиши и клавиши быстрого вызова

- **Tab**: заполняет оставшуюся часть частично введённой команды или ключевого слова
- **Ctrl-R**: повторно отображает строку
- **Ctrl-A**: перемещает курсор в начало строки
- **Ctrl-Z**: выполняет выход из режима конфигурации и возврат в пользовательский режим
- **СТРЕЛКА ВНИЗ**: позволяет пользователю выполнять прокрутку вперёд по последним командам
- **СТРЕЛКА ВНИЗ**: позволяет пользователю выполнять прокрутку вперёд по последним командам
- **Ctrl-Shift-6**: позволяет пользователю прервать процесс IOS (например, **ping** или **traceroute**).
- **Ctrl-C**: прерывает текущую команду и выполняет выход из режима конфигурации

## Структура команды

# Команды для изучения IOS



Команды IOS **show** предоставляют информацию о конфигурации, эксплуатации и состоянии компонентов коммутатора или маршрутизатора Cisco.



## Структура команды

# Команда «show version»

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
cisco1941 uptime is 41 minutes
```

```
System returned to ROM by power-on
```

```
System image file is ""flash0:c1900-universalk9-mz.SPA.152-4.M1.bin""
```

```
Last reload type: Normal Reload
```

```
Last reload reason: power-on
```

```
This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
```

версия программного  
обеспечения IOS

версия программы  
начальной загрузки

время с момента  
последней  
перезагрузки

имя файла образа  
IOS

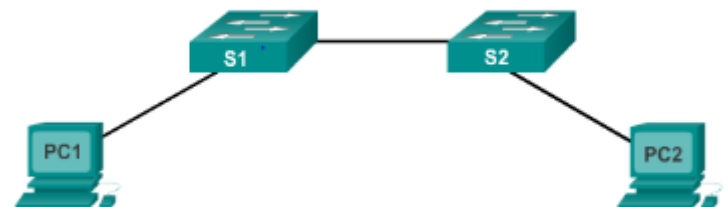
```
Router#show version
```

# Назначение коммутатора

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

Основное внимание будет уделено следующим пунктам.

- Создание сети из двух ПК, соединённых посредством коммутатора
- Настройка имени коммутатора
- Ограничение доступа к конфигурации устройства
- Настройка баннерных сообщений
- Сохранение конфигурации



## Базовая настройка устройств

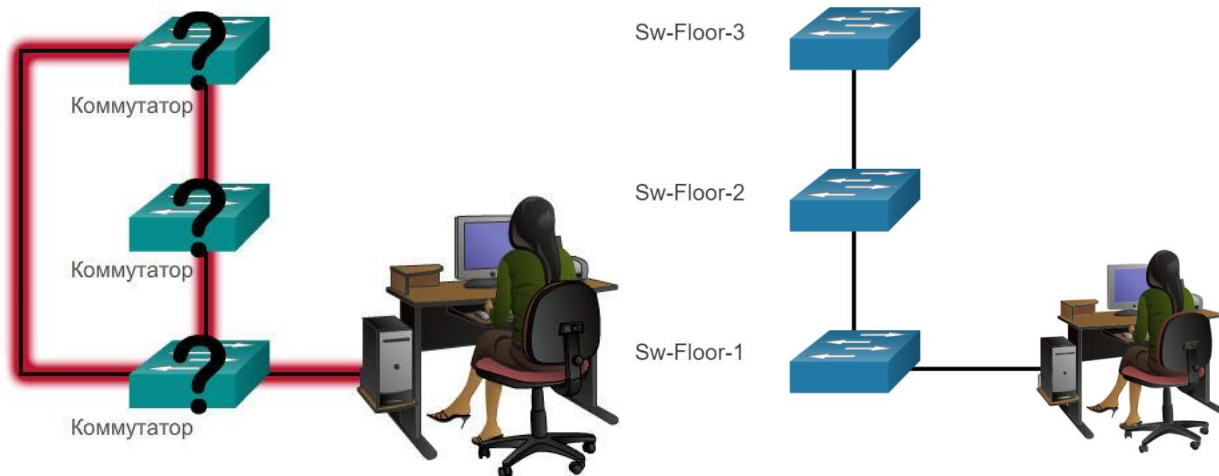
# Имена устройств

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;**
- состоять не более чем из 64 символов.

Организация должна выработать общее правило об именах устройств, которое позволяет легко и интуитивно идентифицировать конкретное устройство.

Безымянные сетевые устройства сложнее распознать для последующей настройки.



# Настройка имён узлов

- Первая команда конфигурации на любом устройстве должна дать ему уникальное имя хоста.
- По умолчанию всем устройствам присваивается заводское имя по умолчанию. Например, коммутатором Cisco IOS является "Switch."

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

- Инструкция по именованию устройств:
  - начинаться с буквы
  - не содержать пробелов
  - оканчиваться на букву или цифру
  - содержать только буквы, цифры и тире
  - состоять не более чем из 64 символов

**Примечание.** Чтобы удалить настроенное имя узла и вернуть стандартный диалог командной строки для коммутатора, используйте команду глобальной конфигурации **no hostname**.

# Типы и правила выбора паролей

Ниже приведены типы паролей.

- **Enable password:** ограничивает доступ к привилегированному режиму, без шифрования
- **Enable secret:** ограничивает доступ к привилегированному режиму, с шифрованием
- **Console password:** ограничивает доступ к устройству, используя консольное соединение
- **VTY password:** ограничивает доступ к устройству по протоколу Telnet

**Примечание.** Используйте пароли длиной более 8 символов. Используйте сочетание прописных и заглавных букв, чисел, специальных знаков и/или цифровых последовательностей. На разных устройствах рекомендуется использовать разные пароли.



## Защита доступа к привилегированному режиму

- используйте команду **enable secret**, а не более раннюю версию команды **enable password**
- **enable secret** обеспечивает повышенный уровень безопасности, поскольку для пароля используется шифрование

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

# Защита доступа к пользовательскому режиму

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

- Необходимо обеспечить безопасность консольного порта
  - снижает вероятность физического подключения кабеля к устройству и получения доступа к устройству неправомерными пользователями
- vty-линии обеспечивают доступ к устройству Cisco по протоколу Telnet
  - количество поддерживаемых vty-линий варьируется в зависимости от типа устройства и версии IOS

При первоначальном подключении к устройству Вы находитесь в пользовательском режиме EXEC. Этот режим защищен с помощью консоли.

Линии виртуального терминала (VTY) обеспечивают удаленный доступ к устройству через Telnet или SSH.

## Шифрование паролей при выводе на экран

- Файлы конфигурации startup-config и running-config отображают большинство паролей в виде простого текста.
- Чтобы зашифровать пароли, используйте команду глобальной конфигурации **service password-encryption**.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- С помощью команды **show running-config** убедитесь, что пароли зашифрованы.

```
Sw-Floor-1# show running-config
!
!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

# Базовая настройка устройств

## Баннерные сообщения

### Ограничение доступа к устройствам — сообщение текущего дня

```
Sw1-Floor-1(config)#banner motd # This is a secure system. Authorized Access ONLY!!! #
```

Данная конфигурация приводит к появлению данного сообщения.

Разделительные символы не входят в это сообщение.

```
Sw1-Floor-1 con0 is now available
Press RETURN to get started.
This is a secure system. Authorized
Access ONLY!!!
User Access Verification
password:
Sw1-Floor-1>enable
Password:
Sw1-Floor-1#
```

# Сохранение конфигураций

## Файлы конфигурации

```
Switch#show running-config
```

Демонстрирует все  
параметры  
конфигурации в ОЗУ  
на текущий момент.

```
Switch#show running-config
Building configuration...
Current configuration : 2904 bytes
!
! Last configuration change at 00:02:32
UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
<выходные данные опущены>
!
```

Текущую  
конфигурацию можно  
скопировать в  
NVRAM.

```
Switch#copy running-config startup-config
```

файл текущей конфигурации обновляет файл  
загрузочной конфигурации

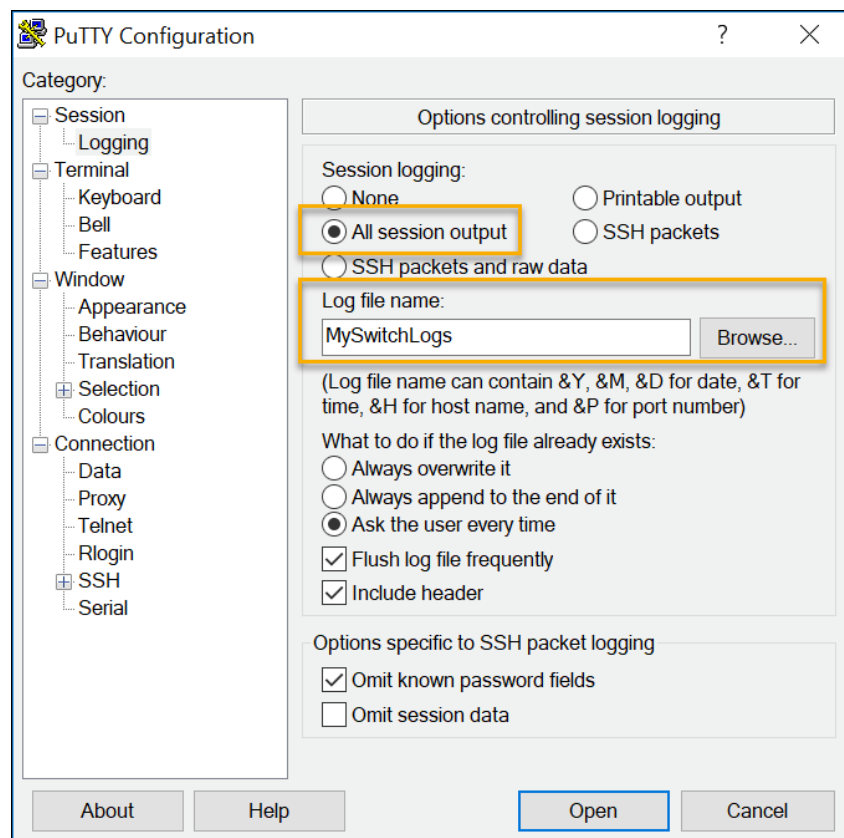
- Перезапуск устройства  
Switch# **reload**  
  
System configuration has been modified. Save? [yes/no]: **n**  
  
Proceed with reload? [confirm]
- Начальную конфигурацию можно удалить с помощью команды **erase startup-config**  
  
Switch# **erase startup-config**
- Чтобы вернуть конфигурацию, «встроенную» по умолчанию, выполните команду **delete vlan.dat**  
  
Switch# **delete vlan.dat**  
Delete filename [vlan.dat]?  
Delete flash:vlan.dat? [confirm]



# Запись конфигурации в текстовый файл

Файлы конфигурации можно также сохранить в виде текстового документа.

- **Шаг 1.**Откройте программу эмуляции терминала, например PuTTY или Tera Term, связанную с коммутатором.
- **Шаг 2.**Активируйте ведение журнала в программе терминала и назначьте файлу журнала имя и место сохранения. На рисунке показано, что **All session output** (Все выходные данные сеанса) будут записываться в указанный файл (например, MySwitchLogs).

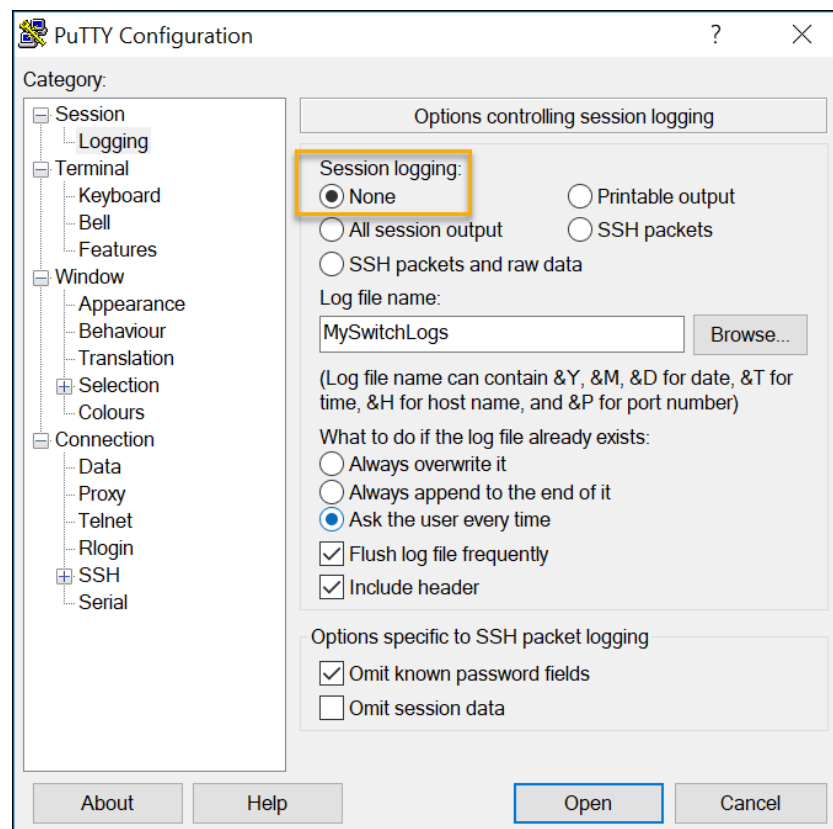


# Запись конфигурации в текстовый файл

- **Шаг 3.** В командной строке привилегированного режима EXEC выполните команду **show running-config** или **show startup-config**. Текст, отображенный в окне терминала, будет помещен в выбранный файл.
- **Шаг 4.** Отключите ведение журнала в программе терминала. На рисунке показано, как отключить ведение журнала сеанса, выбрав **None (Нет)**.

Созданный текстовый файл можно использовать как протокол текущей конфигурации устройства и для восстановления конфигурации. Возможно, файл придется отредактировать, прежде чем использовать его для восстановления сохраненной конфигурации на устройстве.

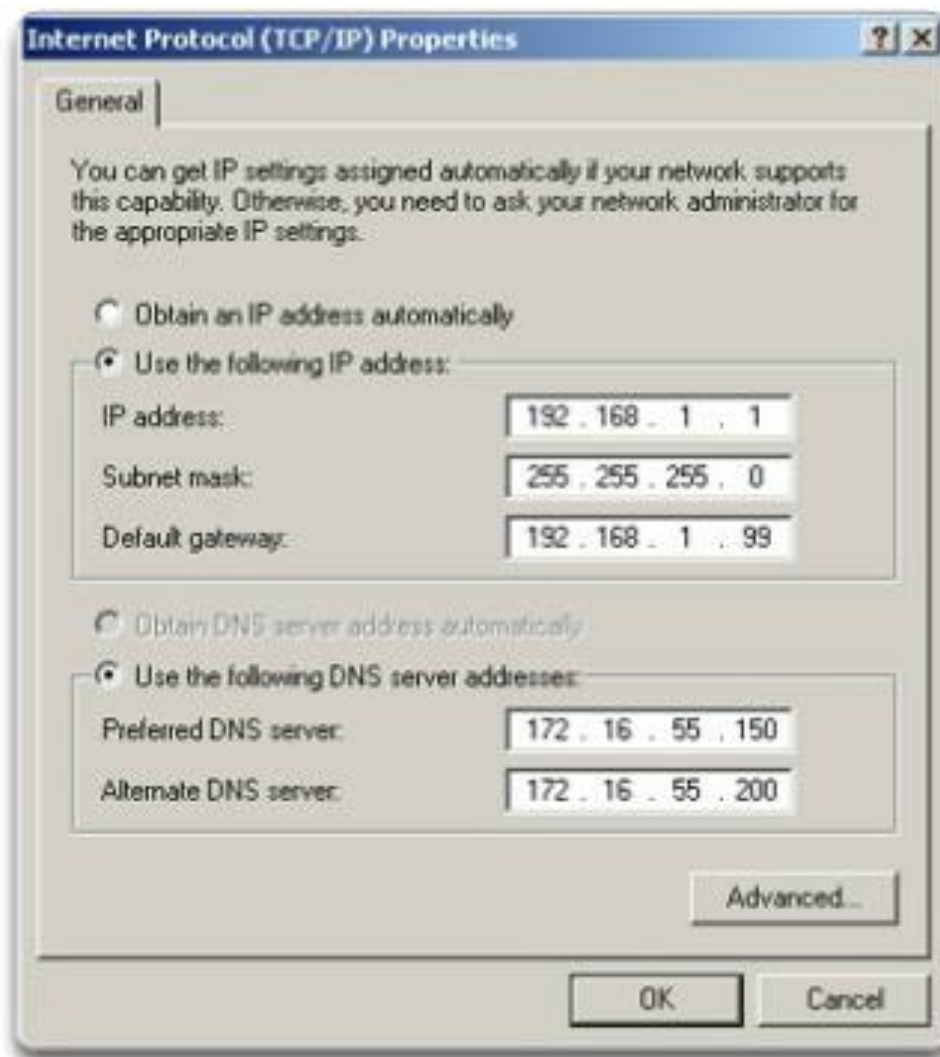
```
Switch# show running-config
Building configuration...
```



## Порты и адреса

# IP-адреса

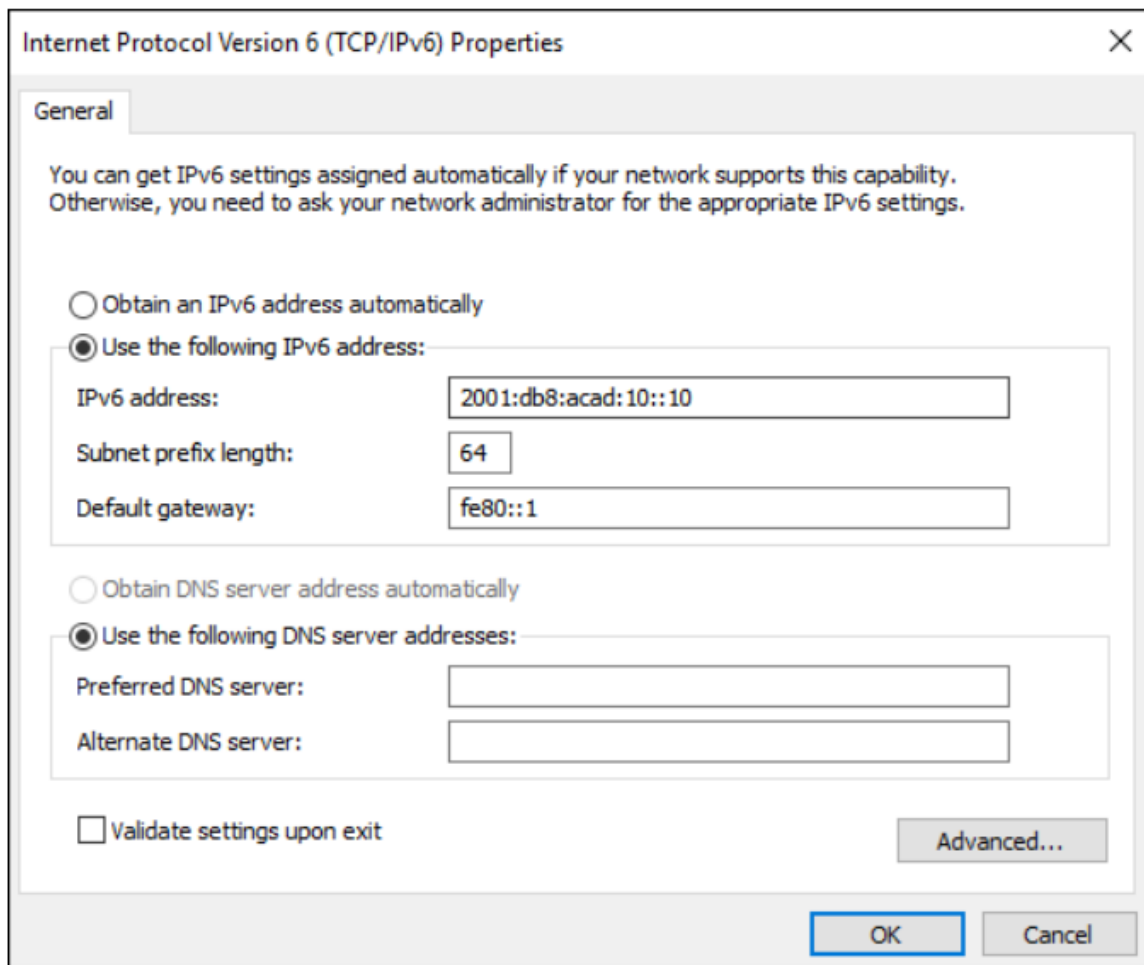
- Все оконечные устройства в сети необходимо настроить с использованием IP-адреса
- Структура IPv4-адреса называется *десятичной с разделительными точками*
- IPv4-адрес, отображаемый в десятичной нотации, содержит четыре десятичных числа в диапазоне от 0 до 255
- Наряду с IP-адресом также требуется указать маску подсети
- IP-адреса можно назначить и физическим портам, и виртуальным интерфейсам



## Порты и адреса

# IP-адреса

- Длина IPv6-адреса составляет 128 бит, написанных в виде строки шестнадцатеричных значений.
- Каждые 4 бита IPv6-адреса представлены одной шестнадцатеричной цифрой
- Общее количество шестнадцатеричных значений равно 32.
- Группы из четырех шестнадцатеричных цифр разделяются двоеточием (:).
- IPv6-адреса нечувствительны к регистру, их можно записывать как строчными, так и прописными буквами.



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:db8:acad:10::10

Subnet prefix length: 64

Default gateway: fe80::1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

# Интерфейсы и порты

- Сетевой обмен данными зависит от интерфейсов оконечных пользовательских устройств, интерфейсов сетевых устройств и кабелей, при помощи которых они соединены.
- Передача данных осуществляется посредством витых медных кабелей, оптоволоконных кабелей, коаксиальных кабелей или с помощью беспроводной связи.
- Типы сред передачи данных различаются возможностями и преимуществами. Вот некоторые различия между типами средств подключения:

Расстояние, на которое средство подключения может передавать сигнал

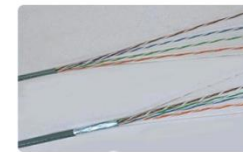
Среда установки средств подключения

Объемы данных и скорость передачи

Стоимость средства подключения и его установка



Copper



Fiber-optics



Wireless





# Настройка IP-адресации

## Настройка IP-адресов вручную для конечных устройств

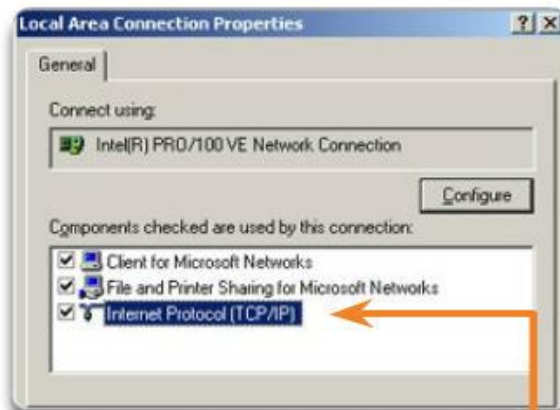
- Конечным устройствам в сети нужен IP-адрес для связи с другими устройствами в сети.

- IP-адрес можно ввести в оконечное устройство вручную или получить автоматически с помощью протокола DHCP.

Чтобы вручную настроить адрес IPv4 на узле ОС Windows, откройте **«Панель управления > Центр общего доступа к сети > Изменить параметры адаптера»** и выберите нужный адаптер. Затем щелкните его правой кнопкой мыши и выберите **«Свойства»**, чтобы **отобразить свойства подключения по локальной сети**.

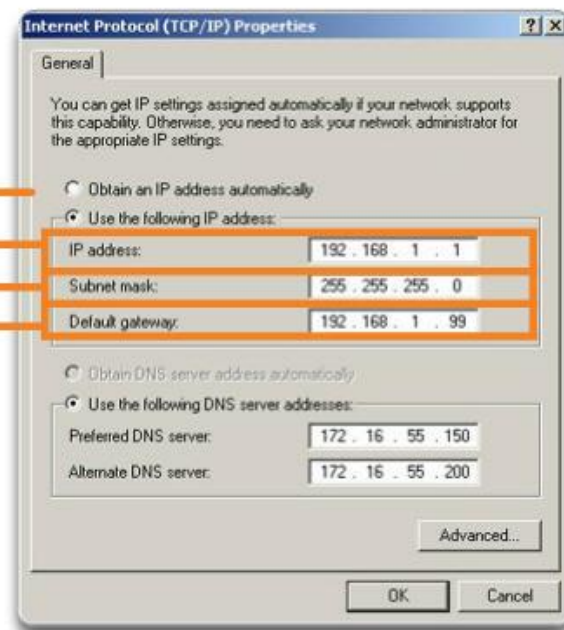
Откроется окно **Свойства: Протокол Интернета версии 4 (TCP/IPv4)**. Настройте адрес IPv4 и маску подсети, а также шлюз по умолчанию.

### Адресация оконечных устройств



Введите следующие адреса для ручных статических назначений:

IP-адрес  
Маска подсети  
Шлюз по умолчанию

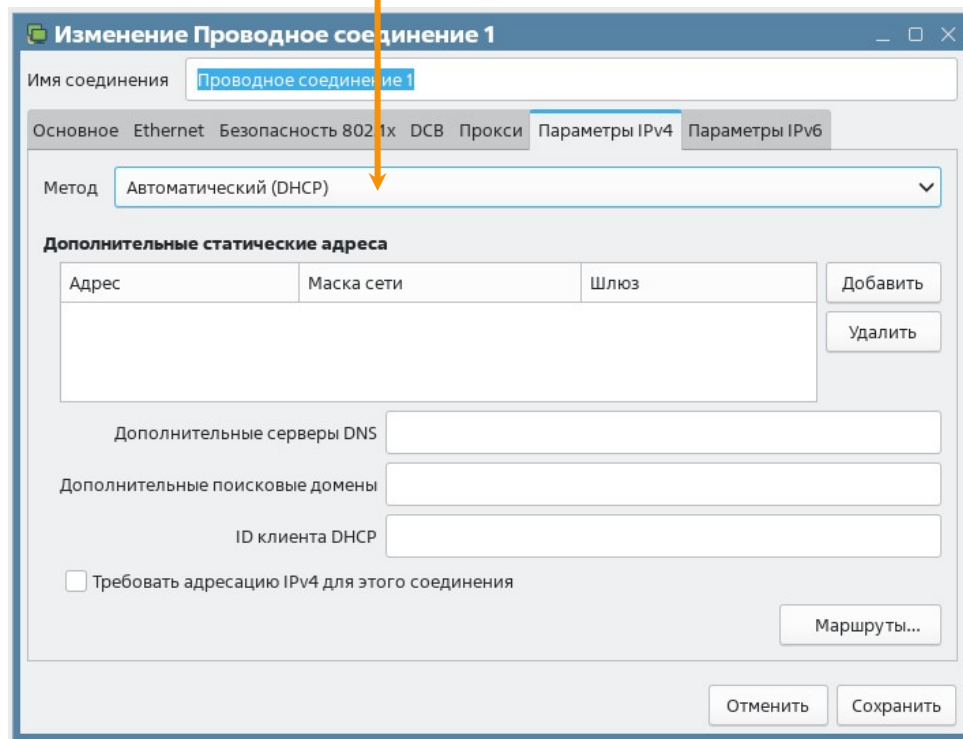


# Настройка IP-адресации

## Автоматическая настройка IP-адресов для конечных устройств



Это свойство настроит устройство для автоматического получения IP-адреса.



# Виртуальный интерфейс коммутатора

Для удаленного доступа к коммутатору на интерфейсе (SVI) нужно настроить IP-адрес и маску подсети.

Чтобы настроить SVI на коммутаторе, выполните следующие действия.

Введите команду **interface vlan 1** в режиме глобальной конфигурации.

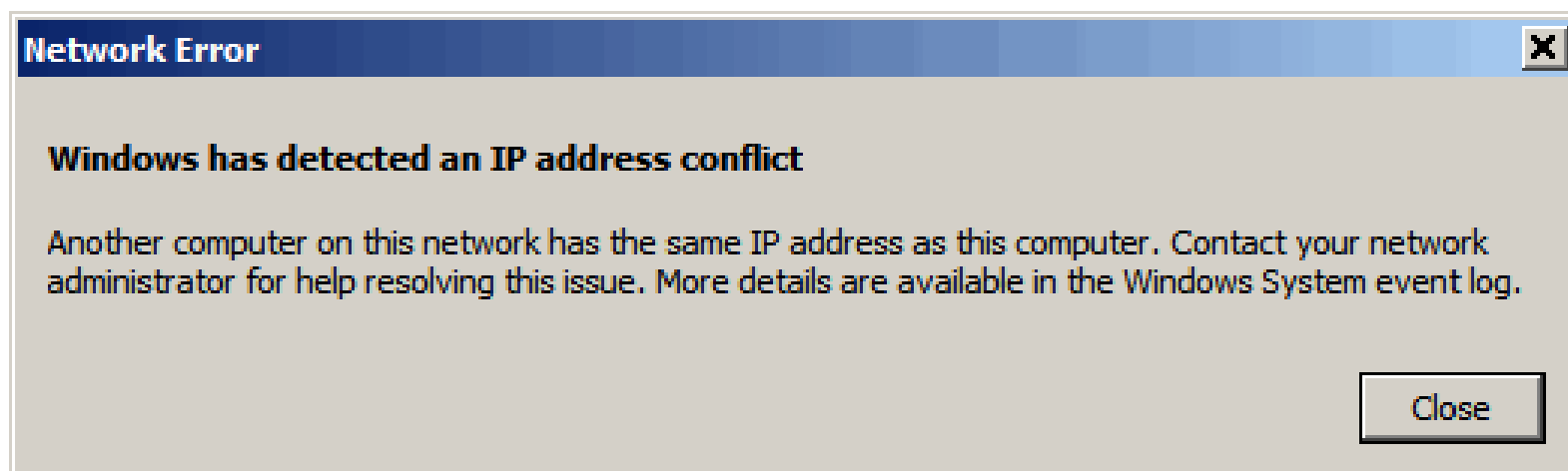
Затем назначьте адрес IPv4 с помощью команды конфигурации интерфейса **ip address** *IP-адрес, маска подсети*.

Наконец, включите виртуальный интерфейс с помощью команды конфигурации интерфейса **no shutdown**.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Настройка IP-адресации

# Конфликты IP-адресов



Проверка подключения

# Проверка адреса обратной связи на оконечном устройстве

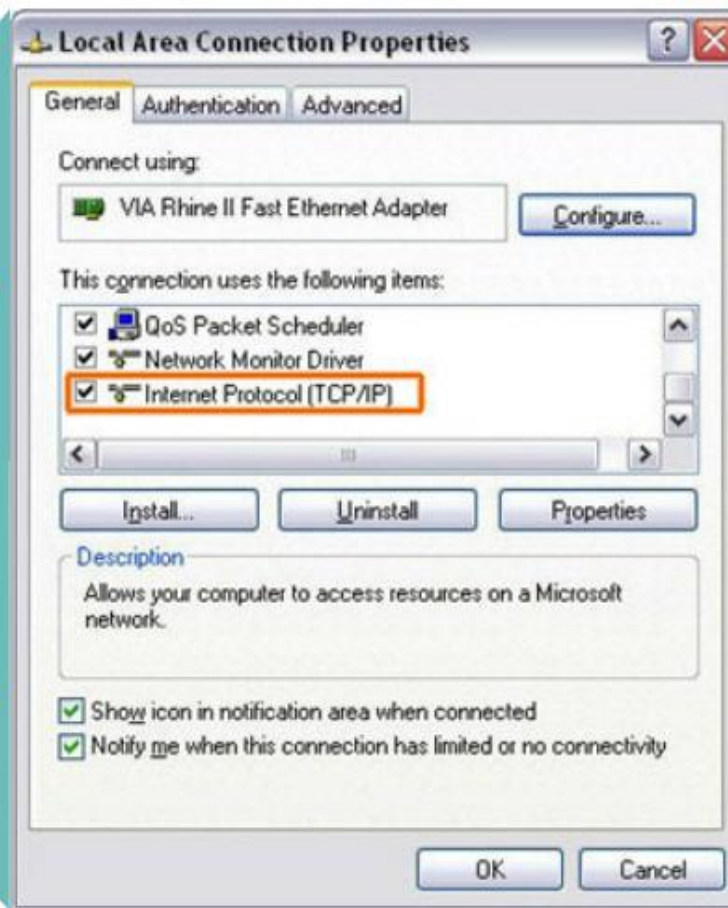
Проверка локального TCP/IP-стека

Эхо-тестирование локального узла подтверждает, что протокол TCP/IP установлен и исправно функционирует на адаптере локальной сети.



C:\>ping 127.0.0.1

Отправка эхо-запроса по IP-адресу **127.0.0.1** приведёт к тому, что устройство самостоятельно выполнит эхо-тестирование.





Проверка подключения

# Проверка сквозного подключения

```
C:\>ping 192.168.10.2
```

```
Pinging 192.168.10.2 with 32 bytes of data:
```

```
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
```

```
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
```

```
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
```

```
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36
```

```
Ping statistics for 192.168.10.2:
```

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

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 820ms, Maximum = 883ms, Average = 842ms
```

```
C:\>ping 192.168.10.11
```

```
Pinging 192.168.10.11 with 32 bytes of data:
```

```
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
```

```
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
```

```
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
```

```
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36
```

```
Ping statistics for 192.168.10.11:
```

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

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 820ms, Maximum = 883ms, Average = 842ms
```

```
C:\>
```



# Проверка назначения интерфейса

```
S1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	up	up

<output omitted>

vlan1	192.168.10.2	YES	manual	up	up
-------	--------------	-----	--------	----	----

```
S2#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	up	up

<output omitted>

vlan1	192.168.10.3	YES	manual	up	up
-------	--------------	-----	--------	----	----



## Удаленное подключение к сетевому устройству

# Активация подключения по SSH

Настройка поддержки протокола SSH выполняется в четыре этапа:

1. **Создайте ключ для шифрования SSH-трафика.** SSH шифрует трафик между источником и получателем. Однако для этого уникальный ключ проверки подлинности должен быть создан с помощью команды глобальной конфигурации **crypto key generate rsa general-keys modulus bits**. Следует лишь отметить, что модуль определяет размер ключа, который может быть в диапазоне от 360 *bit* до 2048 бит. Чем больше значение бита, тем безопаснее ключ. Однако большие значения битов также требуют больше времени для шифрования и расшифровки информации. Минимальная рекомендуемая длина модуля — 1024 бит.
2. **Проверьте или создайте запись локальной базы данных.** Создайте учетную запись пользователя в локальной базе данных с помощью команды **username**.
3. **Пользователи проходят аутентификацию в локальной базе данных.** Используйте команду конфигурации **login local** для проверки подлинности строки vty в локальной базе данных.
4. **Включите входящие сеансы SSH с использованием vty.** По умолчанию сеанс ввода не разрешен на линиях vty. Можно указать несколько протоколов, включая Telnet и SSH, используя команду **transport input [ssh | telnet]**.