Глава 11. Создание сети небольшого размера

Материалы для инструктора

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Материалы для инструкторов. Глава 11. Руководство по планированию

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 13

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

Глава 11. Создание сети небольшого размера

Introduction to Networks 6.0.
Руководство по планированию

Глава 11. Упражнения

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
11.2.1.4	Задание	Угрозы безопасности и уязвимости	Рекомендуется
11.2.2.5	Задание	Типы атак	Рекомендуется
11.2.2.6	Лабораторная работа	Изучение угроз безопасности сети	Необязательно
11.2.4.5	Packet Tracer	Настройка безопасного пароля и протокола SSH	Рекомендуется
11.2.4.6	Лабораторная работа	Доступ к сетевым устройствам по протоколу SSH	Необязательно
11.2.4.7	Лабораторная работа	Изучение сеансов связи по протоколам Telnet и SSH с помощью программы Wireshark	Необязательно
11.2.4.8	Лабораторная работа	Обеспечение безопасности сетевых устройств	Рекомендуется
11.2.5.7	Packet Tracer	Резервное копирование файлов конфигурации	Необязательно
11.2.5.8	Лабораторная работа	Управление файлами конфигурации маршрутизатора с помощью программы Tera Term	Рекомендуется
11.2.5.9	Лабораторная работа	Управление файлами конфигурации устройства с помощью TFTP-сервера, флеш-памяти и USB-накопителя	Необязательно

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 11. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
11.2.5.10	Лабораторная работа	Изучение процедур восстановления пароля	Необязательно
11.3.2.3	Cisco Packet Tracer	Проверка задержки сети с помощью ping-запроса и команды traceroute	Рекомендуется
11.3.2.4	Лабораторная работа	Проверка задержки сети с помощью команд ping и traceroute	Рекомендуется
11.3.3.2	Видео	Команда show version	
11.3.3.3	Cisco Packet Tracer	Использование команд show	Рекомендуется
11.3.4.5	Задание	Команды show	Рекомендуется
11.3.4.6	Лабораторная работа	Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах	Необязательно
11.4.1.4	Задание	Определите порядок действий для поиска и устранения неполадок	Рекомендуется
11.4.3.5	Лабораторная работа	Поиск и устранение неполадок, связанных с кабелями и интерфейсами	Рекомендуется

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 11. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
11.4.3.6	Packet Tracer	Поиск и устранение неполадок подключения	Рекомендуется
11.5.1.1	Упражнение в аудитории	Проектирование и построение сети малого предприятия	Необязательно
11.5.1.2	Packet Tracer	Отработка комплексных практических навыков	Рекомендуется
11.5.1.3	Packet Tracer	Поиск и устранение неполадок	Рекомендуется

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 11. Проверочная работа

- После прохождения главы 11 учащиеся должны пройти проверку на знание материала главы 11.
- Для неформальной оценки успехов студентов можно использовать контрольные работы, лабораторные работы, работу с Cisco Packet Tracer и другие упражнения.

Глава 11. Практические рекомендации

Прежде, чем излагать материал главы 11, обратите внимание на следующее:

- Инструктор должен пройти проверку на знание материала главы 11.
- Цели этой главы:
  - Определить устройства, используемые в сети небольшого размера.
  - Определить протоколы, используемые в сети небольшого размера.
  - Объяснить, каким образом сеть небольшого размера можно использовать в качестве основы для построения более крупных сетей.
  - Объяснить необходимость применения основных мер безопасности на сетевых устройствах.
  - Определить уязвимости системы безопасности.
  - Определить основные методы устранения угроз.
  - Настроить сетевые устройства с помощью функций их стабилизации для устранения угроз безопасности.
  - Использовать выходные данные команды ping для определения относительной производительности сети.
  - Использовать выходные данные команды tracert для определения относительной производительности сети.
  - Использовать команды show для проверки конфигурации и состояния сетевых устройств.
  - Использовать команды хоста и системы IOS для получения сведений об устройствах в сети.

Глава 11. Практические рекомендации (продолжение)

- Использовать выходные данные команды ping для определения относительной производительности сети.
- Использовать выходные данные команды tracert для определения относительной производительности сети.
- Использовать команды show для проверки конфигурации и состояния сетевых устройств.
- Использовать команды хоста и системы IOS для получения сведений об устройствах в сети.

- 11.1.2.2. Дополнительные примечания относительно различных протоколов.
  - *DNS — служба, которая предоставляет IP-адрес веб-сайта или доменное имя, чтобы хост мог подключиться к нему* ***без использования числового IP-адреса****.*
  - *DHCP-сервер — служба, назначающая клиентам IP-адрес, маску подсети, шлюз по умолчанию и другие параметры****, чтобы их не нужно было вводить вручную****.*
  - Веб-сервер может использовать протокол HTTP или его защищенную версию, протокол HTTPS.
- 11.1.3.2. Ссылки на некоторые анализаторы протоколов, такие как программа Wireshark
  - https://www.wireshark.org/download.html

Глава 11. Практические рекомендации (продолжение)

- Раздел 11.2.2.2
  - Следующий веб-сайт продемонстрирует атаки в Интернете в реальном времени: http://map.norsecorp.com/#/
    - Веб-сайт Norse Attack Map поддерживает самую большую в мире сеть аналитики угроз и отображает ее графически на первой странице.
- Раздел 11.2.4.4
  - PuTTY — это бесплатный SSH-клиент, который можно использовать для связи по протоколу SSH с маршрутизаторами и коммутаторами.
  - Последняя версия программы PuTTY доступна по адресу: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
- Раздел 11.3.4.2
  - Предложите студентам просмотреть записи ARP с помощью команды **arp –a**. Затем предложите студентам отправить ping-запрос на широковещательный адрес их локальной сети и затем еще раз просмотреть записи ARP с помощью команды arp –a. Должны появиться дополнительные устройства. Это один из способов, который можно использовать для поиска всех устройств в локальной сети.
  - Объясните студентам, как и зачем это используется.

Глава 2. Дополнительная помощь

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных компанией Cisco сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить ее на сайте сообщества сертифицированных компанией Cisco сетевых специалистов (CCNA).
- Студенты могут записаться на курс **Introduction to Packet Tracer** (для самостоятельного изучения)

CISCO

Глава 11. Создание сети небольшого размера

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Глава 11. Разделы и задачи

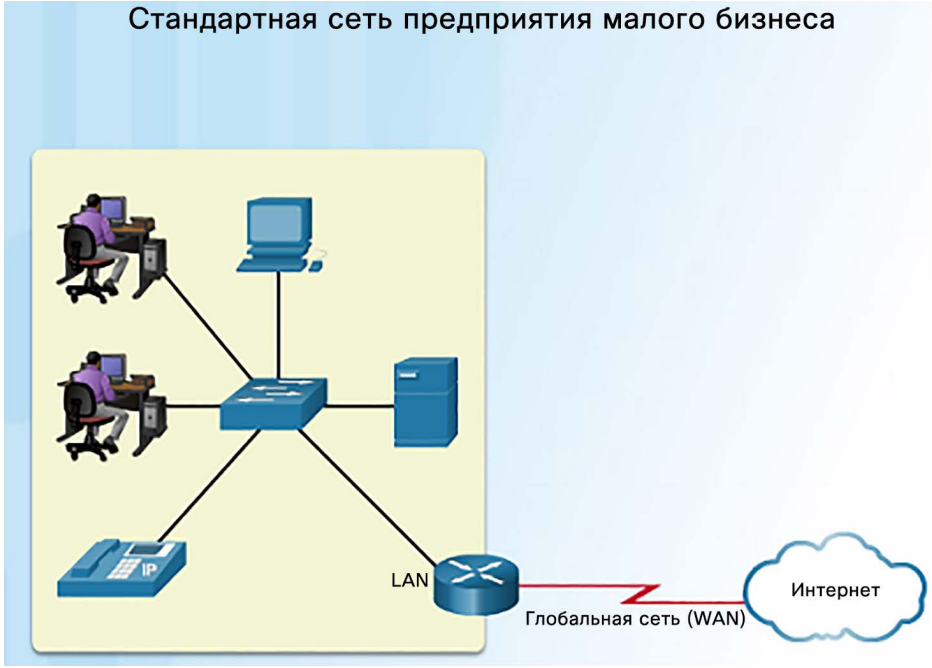
- 11.1. Проектирование сетей
  - Описать способы создания, настройки и проверки небольшой сети, состоящей из напрямую подключенных сегментов.
    - Определить устройства, используемые в сети небольшого размера.
    - Определить протоколы, используемые в сети небольшого размера.
    - Объяснить, каким образом сеть небольшого размера можно использовать в качестве основы для построения более крупных сетей.
- 11.2. Безопасность сети
  - Выполнить настройку функций, повышающих уровень безопасности, на коммутаторах и маршрутизаторах.
    - Объяснить необходимость применения основных мер безопасности на сетевых устройствах.
    - Определить уязвимости системы безопасности.
    - Определить основные методы устранения угроз.
    - Настроить сетевые устройства с помощью функций их стабилизации для устранения угроз безопасности.

Глава 11. Разделы и цели (продолжение)

- 11.3. Производительность базовой сети
  - Использовать стандартные команды show и утилиты для определения относительного базового уровня производительности сети.
    - Использовать выходные данные команды ping для определения относительной производительности сети.
    - Использовать выходные данные команды tracert для определения относительной производительности сети.
    - Использовать команды show для проверки конфигурации и состояния сетевых устройств.
    - Использовать команды хоста и системы IOS для получения сведений об устройствах в сети.
- 11.4. Поиск и устранение неполадок сети
  - Находить и устранять неполадки в сети.
    - Описывать распространенные методики поиска и устранения неполадок в сети.
    - Находить и устранять неполадки в работе кабелей и интерфейсов.
    - Находить и устранять неполадки, связанные с устройствами в сети.

11.1. Проектирование сетей

Топологии небольших сетей



- Большинство предприятий имеют небольшой размер, и обычно им необходимы небольшие сети, состоящие из одного маршрутизатора с одним или несколькими коммутаторами и, возможно, одной или нескольких точек беспроводного доступа. На предприятии также могут быть IP-телефоны.
  - Для подключения к Интернету на маршрутизаторе, как правило, будет выделено одно подключение к глобальной сети с помощью DSL, кабеля или Ethernet-соединения.
- Управление небольшой сетью аналогично управлению крупной сетью:
  - Обслуживание и поиск и устранение неполадок существующего оборудования
  - Обеспечение безопасности устройств и данных в сети

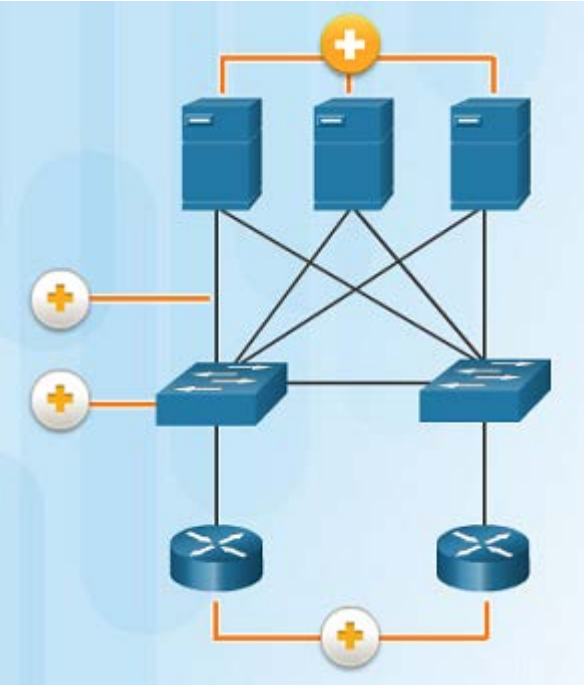
Выбор устройств для небольшой сети

- Независимо от размера сети, чтобы учесть все требования, стоимость и варианты развертывания, необходимо предварительное планирование и проектирование.
  - Стоимость — стоимость коммутатора или маршрутизатора зависит от его производительности и функций.
  - Скорость и типы из портов/интерфейсов — очень важно правильно выбрать количество и тип портов на маршрутизаторе или коммутаторе.
  - Расширяемость — сетевые устройства выпускаются как в фиксированной, так и в модульной конфигурации для обеспечения расширяемости и гибкости.
  - Функции и службы операционной системы — необходимо учитывать различные функции и службы, включая безопасность, QoS, VoIP, коммутацию уровня 3, NAT и DHCP.

IP-адресация в рамках небольшой сети

- При развертывании сети небольшого размера необходимо спланировать пространство IP-адресации.
- Все узлы в пределах сети организации должны иметь уникальный адрес.
- При проектировании схемы IP-адресации учитываются различные типы устройств:
  - Устройства для конечных пользователей
  - Серверы и периферийные устройства
  - Узлы, доступные из Интернета
  - Промежуточные устройства.
- Планирование и документирование схемы IP-адресации позволяет администраторам отслеживать устройства по типам. Например, если всем серверам назначается адрес узла в диапазоне 50–100, трафик сервера можно будет легко отследить по IP-адресу.

Резервирование в небольшой сети

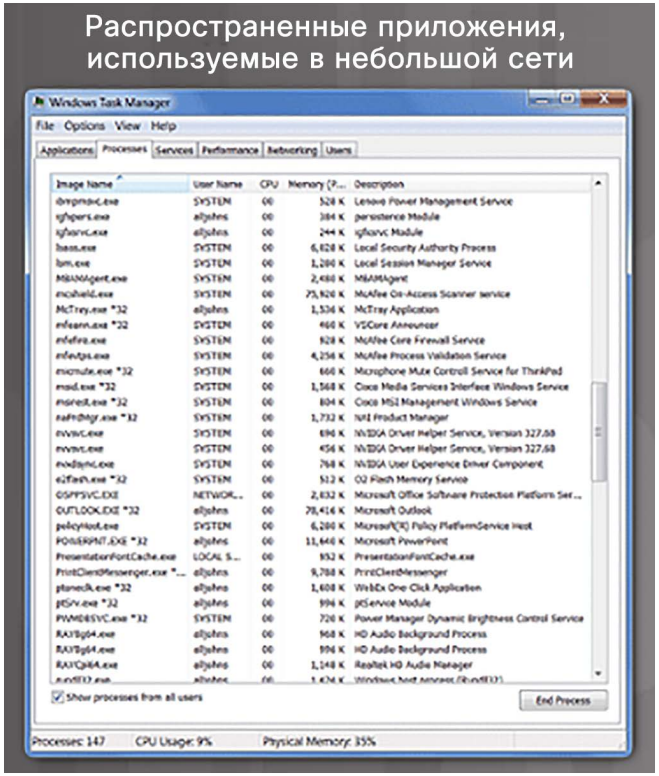


- Надежность является еще одним важным элементом проектирования сети — сбой в работе сети может принести значительные убытки.
- На рисунке слева представлена сеть центра обработки данных.
- На этом рисунке показаны 4 типа резервирования:
  - Резервные серверы
  - Резервные каналы
  - Резервные коммутаторы
  - Резервные маршрутизаторы
- Сбой сервера, канала связи, коммутатора или маршрутизатора не приведет к отказу сети.

Управление трафиком

- При проектировании сети необходимо учесть различные типы трафика и способы их обработки.
- Маршрутизаторы и коммутаторы в сети небольшого размера должны быть настроены для поддержки передачи трафика в реальном времени, например видео и голоса. Например:
  - Голос → высокий приоритет
  - Видео → высокий приоритет
  - SMTP → средний приоритет
  - Мгновенный обмен сообщениями → обычный приоритет
  - FTP → низкий приоритет
- Сетевой трафик следует классифицировать в соответствии с приоритетом для повышения эффективности работы сотрудников и минимизации простоев сети.

Наиболее распространенные приложения



- Существует два вида программ или процессов, обеспечивающих доступ к сети.
  - Сетевые приложения — это компьютерные программы, используемые для обмена данными по сети. Некоторые приложения конечных пользователей зависят от сети и могут осуществлять обмен данными непосредственно с нижними уровнями стека протоколов. Примеры таких приложений — клиенты электронной почты и веб-обозреватели.
  - Службы уровня приложений — другие программы могут прибегать к помощи служб уровня приложений при использовании сетевых ресурсов (например, передача файлов и временное хранение данных сетевой печати).
- Все приложения и сетевые сервисы используют протоколы, которые определяют действующие стандарты и форматы данных, которые следует использовать для форматирования и передачи данных.

Общие протоколы

- *DNS — служба, которая предоставляет IP-адрес веб-сайта или доменное имя, чтобы хост мог подключиться к нему без использования числового IP-адреса.*
- *DHCP-сервер — служба, назначающая клиентам IP-адрес, маску подсети, шлюз по умолчанию и другие параметры, чтобы их не нужно было вводить вручную.*

- Большинство сетевых специалистов работают с сетевыми протоколами, которые необходимы для поддержки сетевых приложений и служб, используемых сотрудниками в постоянной работе.
- На рисунке слева перечислены некоторые распространенные сетевые протоколы, которые используются в большинстве сетей, в том числе в небольших сетях.
- Каждый сетевой протокол определяет:
  - Процессы на каждой из сторон сеанса обмена данными.
  - Типы сообщений
  - Синтаксис сообщений
  - Значение информационных полей
  - Способы отправки сообщений и предполагаемый ответ
  - Взаимодействие с последующим более низким уровнем.

Приложения обработки речи и видео

- Современные компании все активнее используют для связи с заказчиками и деловыми партнерами IP-телефонию и потоковую передачу мультимедийного содержимого.
- Сетевой администратор должен убедиться, что сеть может поддерживать эти приложения и службы, включая наличие вспомогательной инфраструктуры с использованием соответствующих коммутаторов и кабелей.
- Устройства VoIP преобразуют аналоговые сигналы в цифровые IP-пакеты. После того как сигналы преобразованы в IP-пакеты, маршрутизатор рассылает их по соответствующим расположениям.

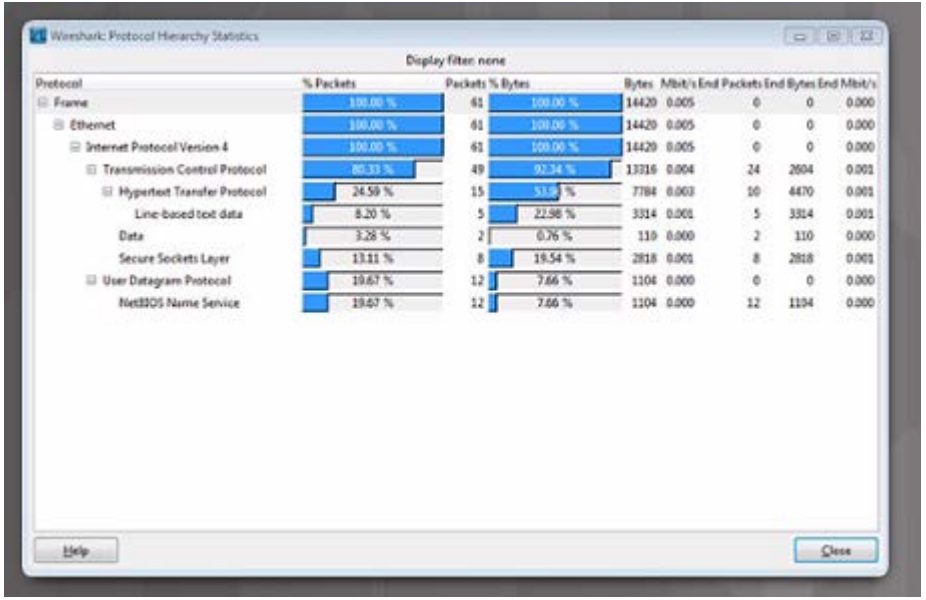
Приложения обработки речи и видео (продолжение)

- В рамках IP-телефонии преобразование голосовых данных в IP-пакеты выполняется непосредственно IP-телефоном. При наличии интегрированного решения IP-телефонии установка в сети маршрутизаторов с поддержкой голосовых данных не требуется. Для управления вызовами и отправки сигналов IP-телефоны используют специализированный сервер.
- Приложения реального времени — сеть должна поддерживать приложения, требующие минимальной задержки при передаче данных. Существует два протокола, удовлетворяющих этому требованию, — транспортный протокол реального времени (Real-Time Transport Protocol, RTP) и управляющий транспортный протокол реального времени (Real-Time Transport Protocol, RTCP).

Расширение небольшой сети

- Сетевой администратор должен предусмотреть расширение малой компании и ее сети.
- Желательно, чтобы сетевой администратор располагал достаточным временем для расширения сети в соответствии с развитием компании.
- Для масштабирования сети требуется ряд элементов:
  - сетевая документация (физическая и логическая топология);
  - реестр устройств (список устройств, которые используют сеть или являются ее частью);
  - бюджет (детализированный бюджет на ИТ, включая годовой бюджет на закупку оборудования на финансовый год);
  - анализ трафика (необходимо задокументировать протоколы, приложения и службы, а также соответствующие требования к трафику).

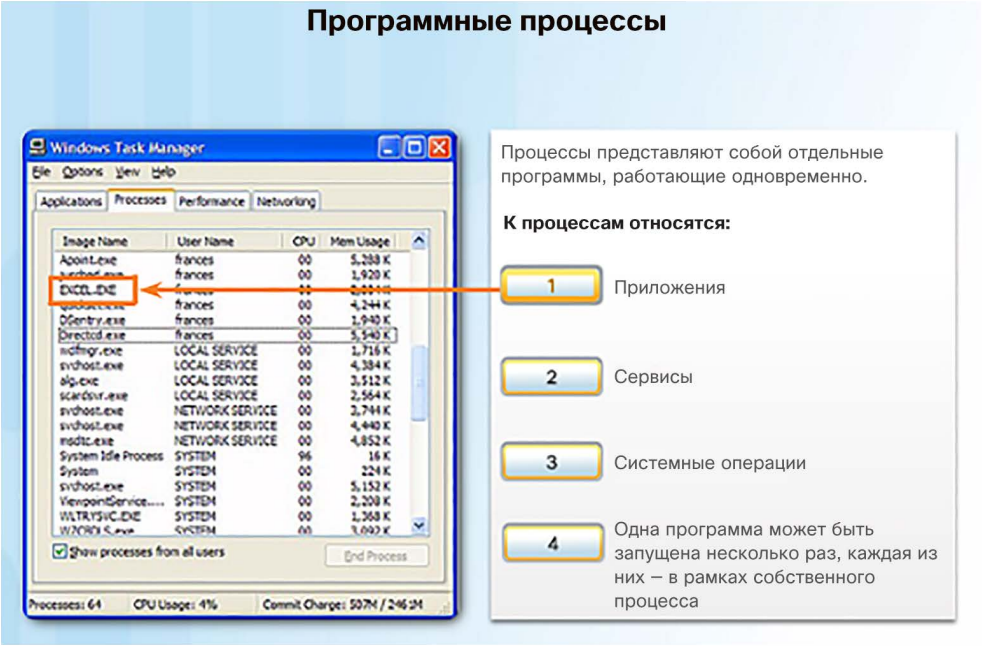
Анализ протоколов



- По мере роста сети очень важно понимать тип и поток трафика, проходящего по сети.
- Анализатор протоколов — основной инструмент, используемый для этой цели. Он также помогает определять неизвестный трафик и его источник.
- Чтобы определить шаблоны потока трафика, необходимо выполнить ряд задач:
  - захватывать трафик во время пиковых периодов загрузки;
  - выполнять захват в различных сегментах сети, так как некоторые типы трафика будут ограничены определенными сегментами.
- Результаты анализа можно использовать при принятии решений об эффективном управлении трафиком.

Использование сети сотрудниками

- Примеры процессов, запущенных в операционной системе Windows



- Помимо понимания изменений в тенденциях трафика администратор сети также должен знать, как именно изменяется использование сети.
- Сетевой администратор может получать персональные «снимки» загрузки ИТ-приложений сотрудниками за заданное время. Эта информация позволяет сетевому администратору регулировать выделение сетевых ресурсов по мере необходимости. Эти снимки обычно содержат следующую информацию:
  - ОС и ее версия
  - Приложения, не являющиеся сетевыми
  - Сетевые приложения
  - Использование ЦП
  - Использование дискового пространства
  - Использование ОЗУ

11.2. Безопасность сети

Типы угроз

- Компьютерные сети играют важнейшую роль в нашей повседневной деятельности. Физические лица и организации в равной степени зависят от своих компьютеров и сетей.
- Несанкционированное вторжение в сеть может привести к большим убыткам из-за нарушений в работе сети и к потере ценных результатов работы.
- Атака на сеть может иметь разрушительные последствия и привести к потере времени и денег.
- Злоумышленники, которых называют хакерами, могут получить доступ к сети через уязвимости программного обеспечения, атаки на аппаратное обеспечение или же путем простого подбора пароля.

Типы угроз (продолжение)

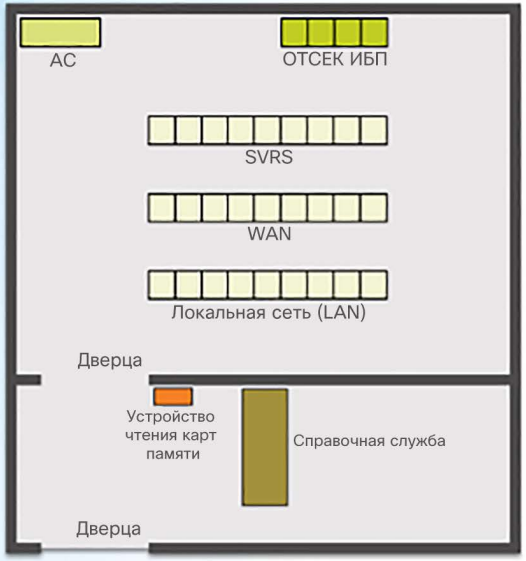
- Есть четыре типа угроз:
  - Хищение информации — происходит, когда кто-либо проникает в компьютер с целью кражи конфиденциальной информации.
  - Потеря данных или манипуляции с ними — проникновение в компьютер с целью уничтожения или изменения записей данных. Примеры потери данных: вирус, форматирующий жесткий диск чьего-либо компьютера. Пример манипуляции с данными: проникновение в систему, например, с целью изменения цены изделия.
  - Хищение персональных данных — вид кражи информации, при котором украденные личные данные используются с целью обмана.
  - Прекращение обслуживания — лишение зарегистрированных пользователей доступа к услугам, которыми они имеют право пользоваться.

Физическая безопасность

Планирование физической системы безопасности

Планирование физической системы безопасности в целях ограничения ущерба для оборудования

- Блокирование оборудования и предотвращение несанкционированного доступа через двери, потолок, съемный пол, окна, вентиляционные и канализационные шахты
- Мониторинг и управление доступом к серверному шкафу с помощью электронной системы учета
- Использование камер системы безопасности



Поэтажный план безопасного компьютерного зала

- Физическая безопасность сетевых устройств также очень важна для управления безопасностью.
- Существует четыре класса физических угроз, которые следует учитывать.
  - Угрозы для аппаратного обеспечения — физическое повреждение серверов, маршрутизаторов, коммутаторов, кабельных линий и рабочих станций.
  - Угрозы со стороны окружающей среды — предельные температуры (слишком высокие или слишком низкие) или слишком высокая влажность.
  - Угрозы, связанные с электропитанием — пики напряжения, недостаточное напряжение в сети (провалы напряжения), колебания напряжения и полное отключение питания.
  - Эксплуатационные угрозы — ненадлежащее обращение с ключевыми электрическими компонентами (электростатический разряд), нехватка важных запасных деталей и ненадлежащая маркировка.

Типы уязвимостей

Уязвимости = технологии

Уязвимости в системе безопасности сети

Уязвимости протоколов TCP/IP

- Протоколы HTTP, FTP и ICMP отличаются низким уровнем безопасности.
- Протоколы SNMP и SMTP относятся к изначально небезопасной структуре, на базе которой был разработан протокол TCP.

Уязвимости операционной системы

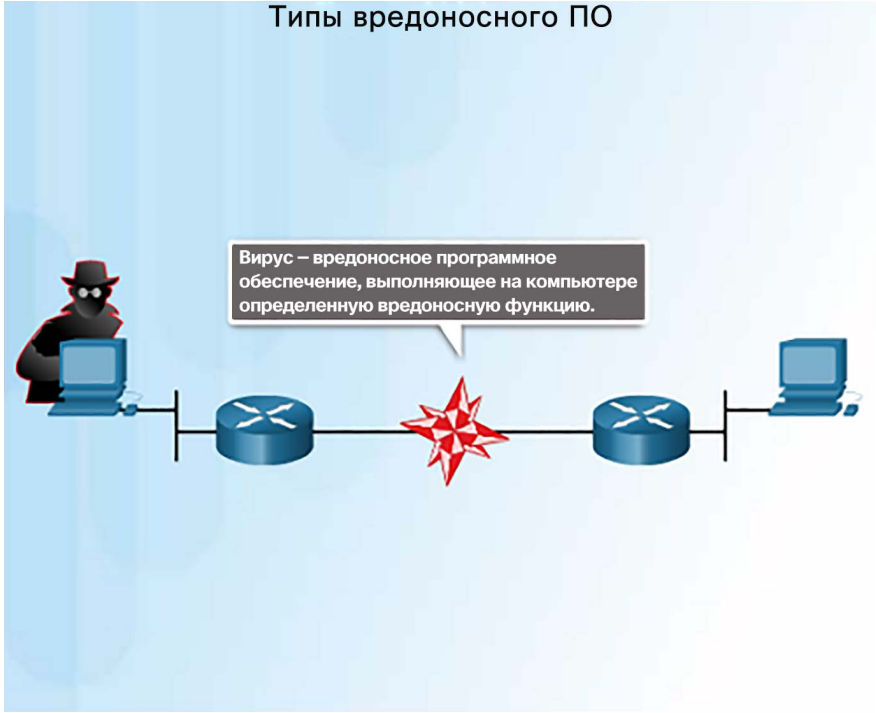
- Во всех операционных системах существуют проблемы безопасности, которые необходимо устранить.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- Эти проблемы задокументированы в архивах компьютерной группы реагирования на чрезвычайные ситуации CERT на веб-сайте http://www.cert.org.

Уязвимости сетевого оборудования

Различные типы сетевого оборудования (маршрутизаторы, межсетевые экраны и коммутаторы) имеют свои уязвимые места, которые необходимо находить, чтобы обеспечить их защиту. К таким слабым местам относятся: защита паролем, отсутствие аутентификации, протоколы маршрутизации и пробелы в межсетевых экранах.

- Уязвимость — степень незащищенности, свойственная каждой сети и устройству, включая маршрутизаторы, коммутаторы, настольные компьютеры, серверы и устройства обеспечения безопасности.
- Как правило, атаки направлены на серверы и настольные компьютеры.
- Существует три основных типа уязвимостей, которые могут приводить к различным атакам. Можно привести несколько примеров
  - Технологические уязвимости — уязвимости в незащищенных протоколах, операционной системе и сетевом оборудовании.
  - Уязвимости конфигурации — незащищенные учетные записи пользователей, системные учетные записи с легко угадываемыми паролями, неправильно настроенное сетевое оборудование.
  - Политика безопасности — отсутствие письменных инструкций по безопасности, недостаточный мониторинг и аудит сети и ресурсов.

Типы вредоносных программ



- Вредоносные программы или вредоносный код (сокращенное название вредоносного программного обеспечения) — это программное обеспечение или код, который предназначен для нанесения ущерба, прерывания работы, кражи или повреждения данных, узлов или сетей.
- Примерами вредоносных программ являются вирусы, интернет-черви и трояны.
  - Вирусы — тип вредоносных программ (исполняемый файл), который распространяется путем внедрения своей копии в другую программу и ее заражения. Они распространяются от одного компьютера к другому.
  - Интернет-черви аналогичны вирусам, но им не нужна программа-носитель. Интернет-червь — автономная программа, использующая функции системы для перемещения по сети.
  - Программы-трояны — пользователя обманом заставляют загрузить и запустить такую вредоносную программу на своем компьютере. Они обычно создают лазейки, позволяющие злоумышленникам получить доступ к системе.

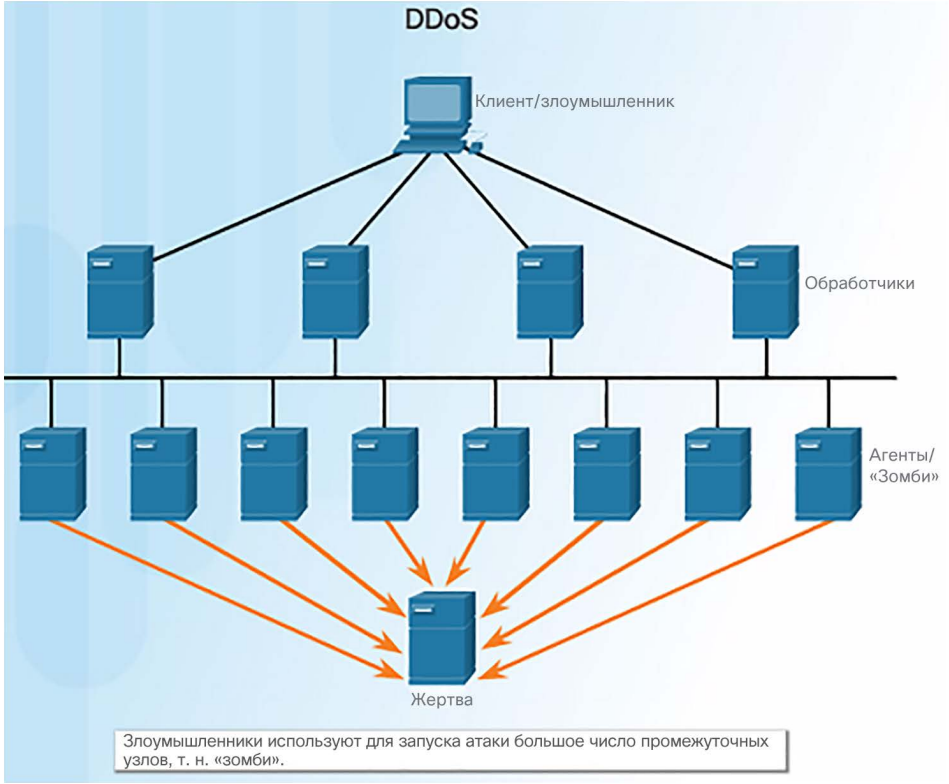
Разведывательные атаки

- Помимо атак с использованием вредоносного кода сети также могут стать объектом различных сетевых атак. Существует три основные категории сетевых атак:
  - Разведывательные атаки — обнаружение и сопоставление систем, служб или уязвимостей.
  - Атаки доступа — несанкционированные действия с данными, доступ к системе или использование прав пользователя.
  - Отказ в обслуживании — отключение или повреждение сетей, систем или служб.
- В ходе разведывательной атаки хакер может использовать команду **nslookup** или **whois** для определения IP-адресов, назначенных объекту. Получив IP-адрес, он может использовать команду **fping** для отправки ping-запроса диапазону IP-адресов, чтобы выяснить, который из них ответит. Узнав отвечающий IP-адрес, хакер может использовать команду **nmap,** чтобы узнать порты прослушивания.

Атаки доступа

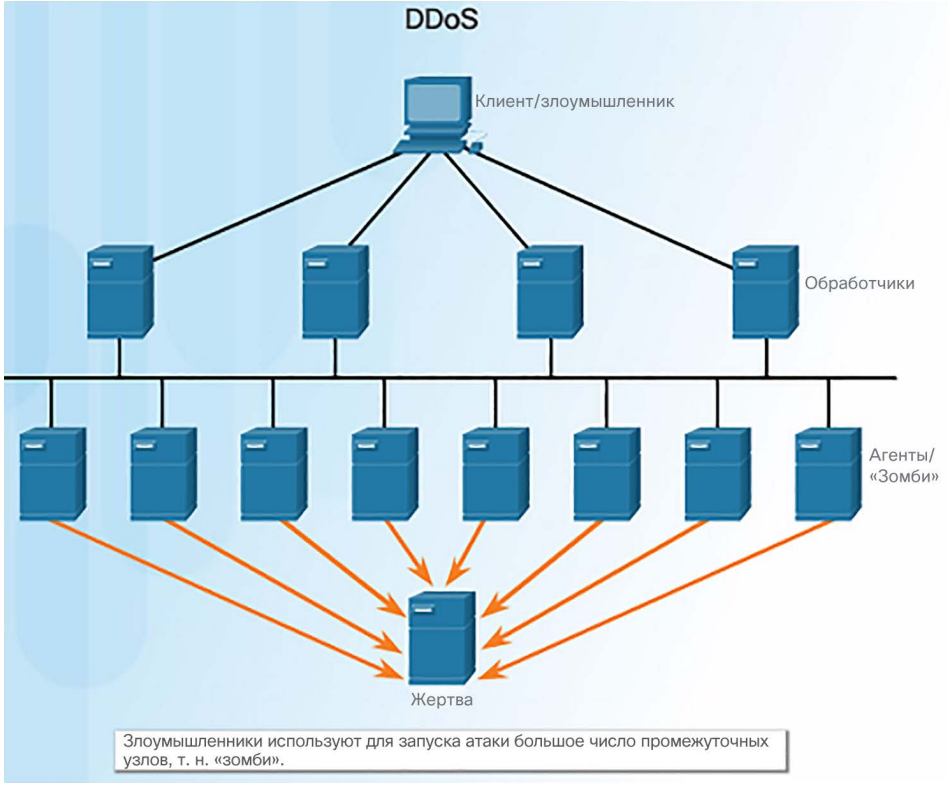
- Атаки доступа используют известные уязвимости в службах аутентификации, FTP- и веб-сервисах, чтобы получить доступ к учетным записям в Интернете, конфиденциальным базам данных и другим ресурсам. Существует четыре класса атак доступа.
  - Подбор пароля — хакеры могут использовать различные методы, в том числе метод прямого подбора, программы-трояны и анализаторы пакетов.
  - Злоупотребление доверием — злоумышленник может получить доступ к целевой системе, используя доверительные отношения между целевой и скомпрометированной системами.
  - Перенаправление портов — злоумышленник устанавливает программу на скомпрометированный узел и использует его для получения доступа к целевому узлу через другой порт.
  - Человек посередине — злоумышленник добавляет себя в сеанс связи. Распространены атаки с использованием фишингового сообщения электронной почты, в котором жертва нажимает на определенную ссылку.

Атаки типа «отказ в обслуживании» (DoS-атаки)



- Атаки типа «отказ в обслуживании» (DoS-атаки) препятствуют доступу авторизованных пользователей к различным службам, используя системные ресурсы, такие как дисковое пространство, пропускная способность и буферы. Такая атака может быть вызвана перегрузкой ресурсов или недопустимым форматом данных.
- DoS-атаки применяются наиболее часто, и им очень сложно противодействовать. Вот несколько примеров DoS-атак.
  - Смертельный эхо-запрос — злоумышленник отправляет искаженный или очень крупный ping-пакет.
  - SYN-флуд — злоумышленник отправляет множество запросов SYN на веб-сервер. Веб-сервер ожидает завершения трехэтапного квитирования TCP. Законный пользователь пытается отправить запрос SYN на веб-сервер, однако тот оказывается недоступен.

Атаки типа «отказ в обслуживании» (DoS-атаки) (продолжение)



- DDoS-атаки — злоумышленник использует большое число промежуточных узлов, «зомби», чтобы начать атаку на целевой узел или сервер. Промежуточные узлы, используемые для запуска атаки, обычно заражаются вредоносным ПО, передавая управление злоумышленнику.
- Smurf-атаки — атаки на основе ICMP, когда злоумышленник рассылает большое количество ICMP-пакетов, используя исходный IP-адрес жертвы. Узлы-«зомби» отвечают целевой жертве в попытке переполнить WAN-канал к месту назначения.

Лабораторная работа. Изучение угроз безопасности сети

Лабораторная работа. Изучение угроз сетевой безопасности

Задачи

Часть 1. Изучение веб-сайта SANS

Часть 2. Определение новых угроз безопасности сети

Часть 3. Подробное описание отдельной угрозы безопасности сети

Общие сведения/сценарий

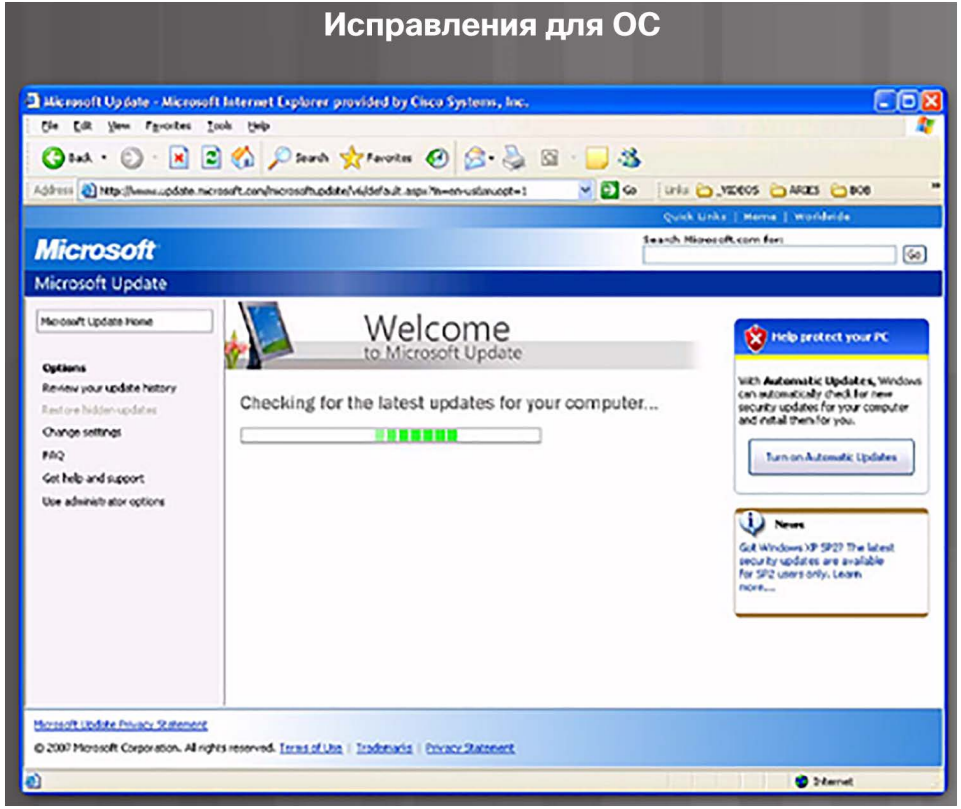
Чтобы защитить сеть от атак, администратор должен определить, какие внешние угрозы представляют опасность для сети. Для определения возникающих угроз и способов их устранения можно пользоваться специализированными веб-сайтами.

Одним из наиболее известных и проверенных ресурсов для защиты компьютера и сети является веб-сайт института SANS (Институт системного администрирования, сетей и безопасности). На веб-сайте SANS доступны несколько разных ресурсов, включая список 20 основных средств контроля безопасности для эффективной киберзащиты и еженедельную новостную рассылку по вопросам безопасности @Risk: The Consensus Security Alert. В рассылке подробно рассказывается о новых сетевых атаках и уязвимостях.

В этой лабораторной работе вам необходимо открыть и изучить веб-сайт SANS, определить новые угрозы сетевой безопасности с его помощью, посетить другие аналогичные веб-ресурсы и подготовить подробное описание отдельной сетевой атаки.

- Для отражения атак на сеть администратор должен иметь возможность обнаруживать внешние угрозы, которые могут представлять опасность для сети.
- В этой лабораторной работе вы изучите угрозы безопасности сети. Для этого вы обратитесь к очень важному веб-сайту, связанному с безопасностью, а также изучите недавние угрозы и подробно опишете конкретную угрозу безопасности сети.

Резервное копирование, обновление и установка исправлений



- Владение актуальной информацией о современных разработках — это важная часть обеспечения безопасности сети и защиты от сетевых атак.
- По мере появления новых вредоносных программ предприятиям рекомендуется постоянно следить за обновлением антивирусного программного обеспечения до последних версий
- Наиболее действенный метод минимизации последствий атаки вируса-червя и других атак — загрузить обновления для системы безопасности с сайта поставщика операционной системы и установить соответствующие обновления на все уязвимые копии систем.
- Использование центрального сервера исправлений для автоматической установки важных исправлений — очень полезное решение этой задачи.

Аутентификация, авторизация и учет

- Такие службы по обеспечению сетевой безопасности, как аутентификация, авторизация и учет (Authentication, authorization, accounting, AAA), являются базовой структурой для настройки средств контроля доступа на каком-либо сетевом устройстве.
- Службы аутентификации, авторизации и учета позволяют контролировать доступ к сети разрешенных пользователей (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также следить за их действиями во время доступа к сети (учет).

Межсетевые экраны

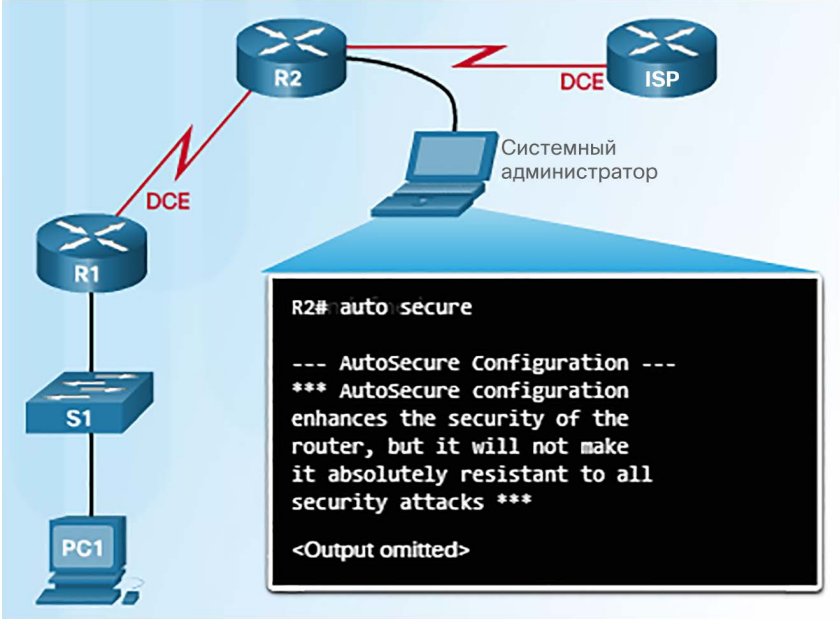
- Межсетевые экраны являются одним из самых эффективных инструментов безопасности, предназначенных для защиты пользователей от внешних угроз.
- Межсетевой экран ставится между двумя (или более) сетями и контролирует трафик между ними, а также позволяет предотвратить несанкционированный доступ. На оконечные системы устанавливают межсетевые экраны на основе узлов или персональные межсетевые экраны.
- В межсетевых экранах используются различные методы для определения разрешения или запрета доступа к сети.
  - Фильтрация пакетов — запрет или разрешение доступа на основе IP- или MAC-адресов.
  - Фильтрация по приложениям — запрет или разрешение доступа для конкретных типов приложений на основе номеров портов.
  - Фильтрация по URL-адресам — запрет или разрешение доступа к веб-сайтам на основе конкретных URL-адресов или ключевых слов.
  - Анализ пакетов с учетом состояний соединений (SPI) — входящие пакеты должны представлять собой разрешенные отклики на запросы внутренних узлов. Трафик, проходящий через межсетевой экран снаружи, должен происходить из внутренней сети либо иметь явное разрешение.

Безопасность оконечных устройств

- Оконечное устройство, или узел, представляет собой отдельную компьютерную систему или устройство, которое выступает в роли клиента сети.
- К наиболее распространенным оконечным устройствам относятся ноутбуки, настольные компьютеры, серверы, смартфоны и планшеты.
- Компании необходимо внедрить правильно задокументированную политику, которой должны следовать сотрудники, поскольку защита оконечных устройств — одна из наиболее сложных задач сетевого администратора.
- Политика зачастую подразумевает использование антивирусного ПО и меры предотвращения несанкционированного доступа к узлу.

Обзор обеспечения безопасности устройств

- Блокировка маршрутизатора:



- При установке на устройство новой операционной системы настройки системы безопасности имеют значения по умолчанию.
- Обычно это создает угрозы безопасности, и следует изменить настройки по умолчанию, включая пароли.
- Необходимо устанавливать исправления безопасности и обновления системы.
- В маршрутизаторах Cisco для обеспечения безопасности системы можно использовать функцию Cisco AutoSecure.
- Вот ряд простых шагов, которые можно применить для большинства операционных систем:
  - Установленные по умолчанию имена пользователей и пароли необходимо немедленно изменить.
  - Доступом к системным ресурсам должны обладать только лица, которым они необходимы.
  - Невостребованные службы и приложения при возможности необходимо отключить или удалить.

Безопасность устройств
Пароли

Надежные и ненадежные пароли

Ненадежный пароль	Почему пароль ненадежный
secret	Простое словарное слово
smith	Девичья фамилия матери
toyota	Марка автомобиля
bob1967	Имя и год рождения пользователя
Blueleaf23	Простые слова и цифры

Надежный пароль	Почему пароль надежный
b67n42d39c	Сочетание букв и цифр
12^h u4@1p7	Сочетание букв и цифр, специальных символов, а также пробела

- Очень важно для защиты сетевых устройств использовать надежные пароли.
- Ниже приведены некоторые рекомендации по выбору пароля.
  - Используйте пароль длиной от 8 до 10 символов (предпочтительно 10 и более символов). Чем длиннее, тем лучше.
  - Пароль должен быть сложным. Включайте в пароль комбинацию букв в верхнем и нижнем регистре, цифр, специальных символов и пробелов (если допускается их использование).
  - Не используйте пароли, основанные на повторениях, распространенных словах, последовательностях букв или цифр, именах пользователей, именах родственников или кличках домашних животных, биографических сведениях или любой легко идентифицируемой информации.
  - Допускайте намеренные ошибки в словах, используемых в паролях.
  - Периодически меняйте пароли.
  - Никогда не записывайте пароли и не оставляйте их в местах, где кто-нибудь сможет их найти.
  - При возможности используйте парольные фразы.

Основные правила обеспечения безопасности

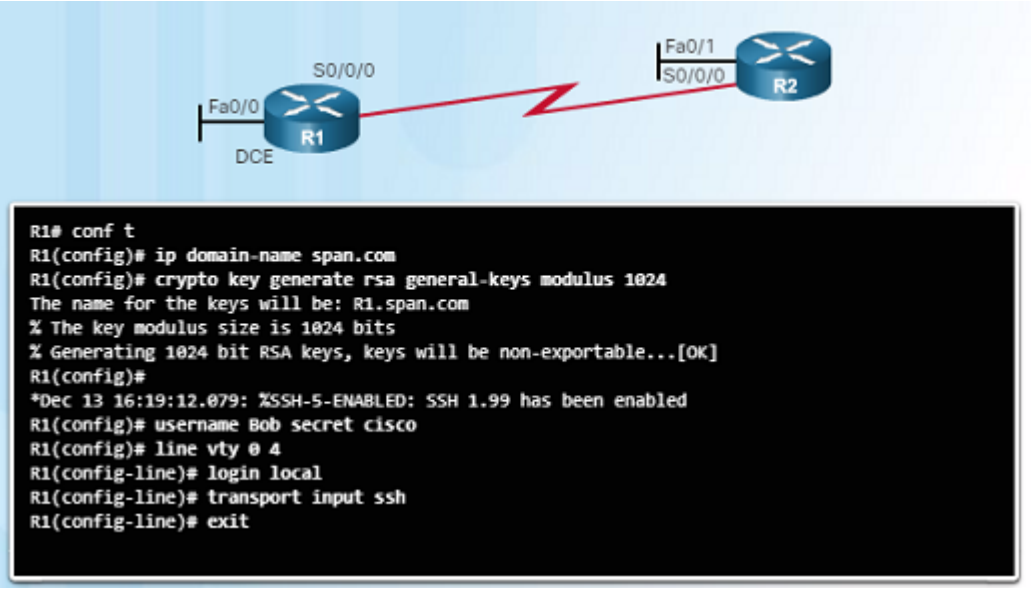
- Используйте команду глобальной настройки **service password-encryption** для шифрования паролей в файле конфигурации и предотвращения просмотра паролей в виде обычного текста неавторизованными пользователями.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 10
Router(config-line)# end
Router# show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

- Чтобы все настроенные пароли имели длину не менее заданного значения, следует использовать команду **security passwords min-length** в режиме глобальной настройки.
- Хакеры часто используют атаку методом полного перебора для расшифровки зашифрованных паролей. Блокируйте попытки входа в систему устройства, если число неудачных попыток за указанное время превысит определенное значение. Для этого используйте команду **login block-for 120 attempts 3 within 60.**
  - Эта команда блокирует попытки входа на 120 секунд, если в течение 60 секунд выполнены три неудачные попытки входа
- Настройка на маршрутизаторе параметра exec timeout автоматически отключает пользователей, если они не выполняли никаких действий в течение времени ожидания.

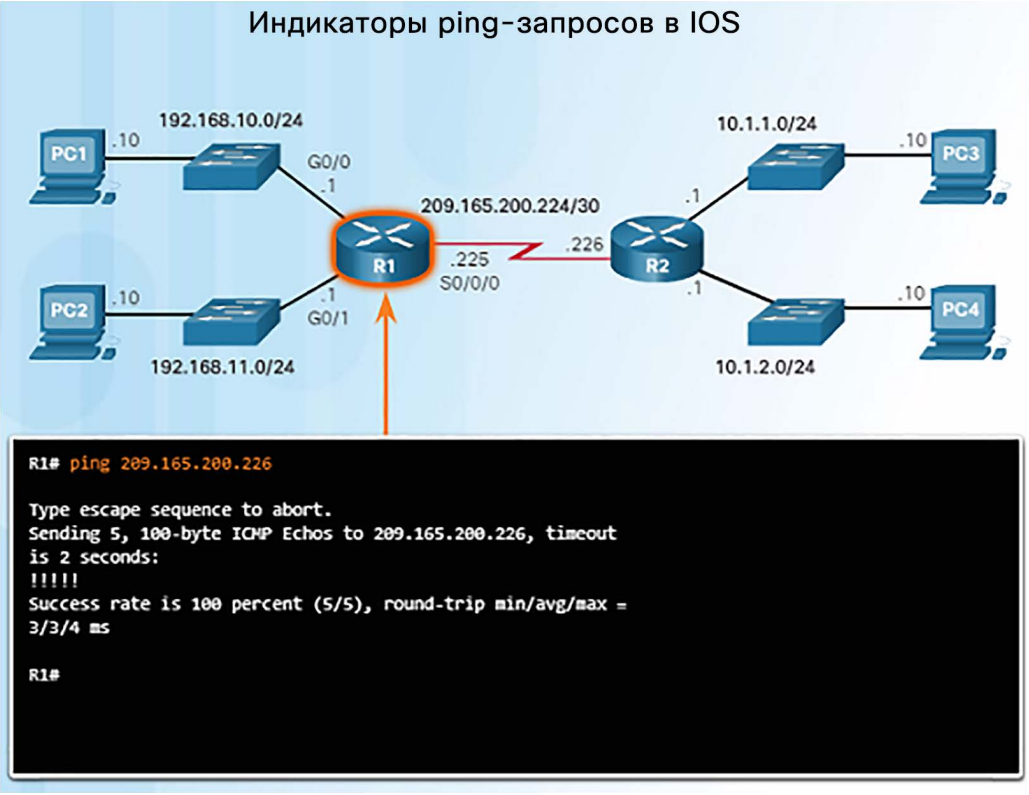
Активация подключения по SSH

- Когда



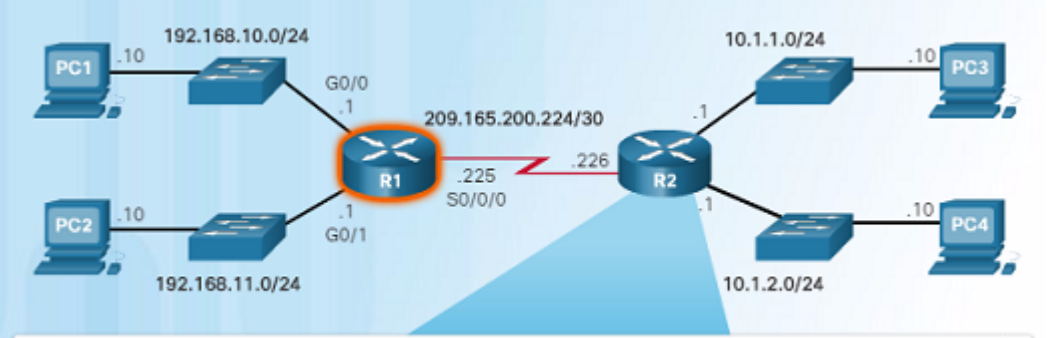
11.3. Производительность базовой сети

Интерпретация результатов выполнения ping-запроса



- Использование **ping-запроса** — очень эффективный способ проверки сетевых подключений к конкретному узлу, серверу или устройству. Это первый важный шаг в процессе поиска и устранения неполадок в работе сети.
- Для отправки команды **ping**-запроса используется протокол ICMP, а сама команда служит для проверки подключений уровня 3.
- Ping-запросы, отправленная из IOS, например на маршрутизаторе Cisco, возвращает несколько параметров. Ниже приведены наиболее типичные.
  - ! — указывает на получение эхо-сообщения ICMP. Это именно то, что вам нужно.
  - . — указывает на то, что истекло время ожидания эхо-ответа ICMP.
  - U — получено сообщение ICMP Unreachable (Недостижимо)

Расширенная команда ping




```
R2# ping
Protocol [ip]:
Target IP address: 192.168.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
```

- В Cisco IOS есть «расширенный» режим команды ping, который может предоставить дополнительные параметры, как показано на рисунке слева.
- Для перехода в этот режим необходимо ввести текст **ping** в привилегированном режиме EXEC, не указывая IP-адрес назначения, а затем нажать ВВОД.
- В примере на рисунке слева показано, как принудительно задать или изменить IP-адрес источника. Это очень удобно при устранении неполадок.

Базовый уровень производительности сети

Выполните ту же проверку

FEB 8, 2013 08:14:43

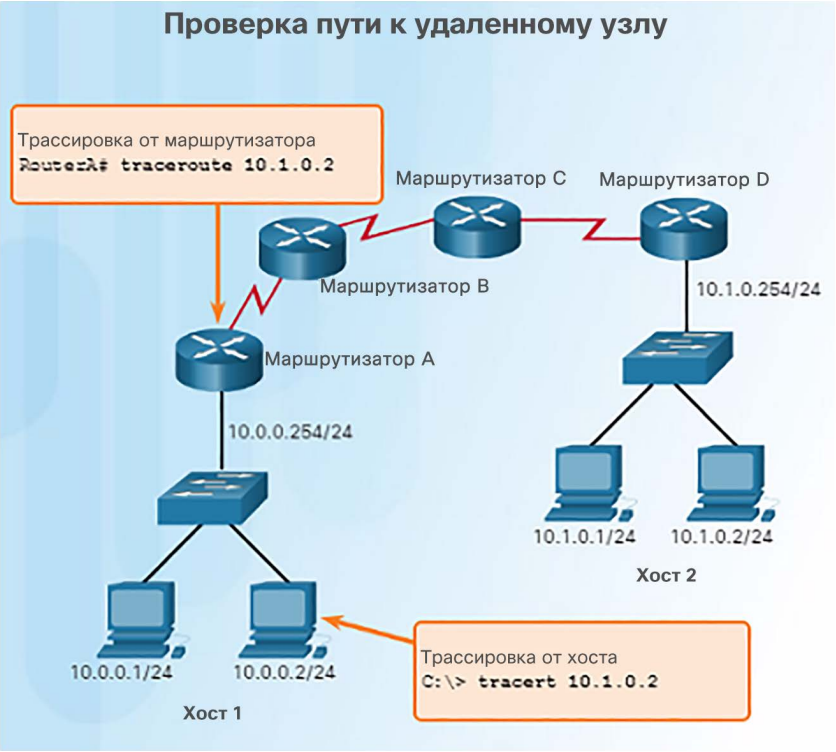
```
C:\> ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.66.254.159:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

MAR 17, 2013 14:41:06

```
C:\> ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

- Определение базового уровня производительности сети — это один из наиболее эффективных средств мониторинга и поиска и устранения неполадок в работе сети.
- Определение эффективного базового уровня реализуется путем измерения производительности в разные моменты времени за некоторый период.
- Одним из способов является копирование и вставка результатов выполнения команды **ping**, **trace** или любой другой соответствующей команды в текстовый файл, включая метку времени.
- В корпоративных сетях необходимо собирать обширную статистику базовых показателей, используя профессиональные программные средства.

Интерпретация сообщений трассировки



- Команда trace возвращает список переходов по мере маршрутизации пакета по сети Каждый маршрутизатор — это переход.
- В системе Windows используйте команду **tracert**.
- При выполнении трассировки из интерфейса командной строки маршрутизатора используйте команду **traceroute**.
- Ответ "Request timed out" (Время ожидания запроса истекло) указывает, что маршрутизатор не ответил. Возможно, произошел сбой в работе сети, или маршрутизаторы настроены не отвечать на эхо-запросы, используемые при трассировке.

Расширенная команда traceroute

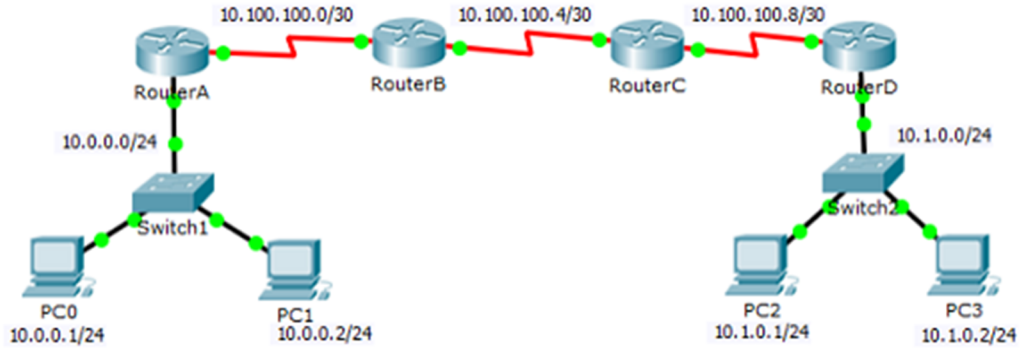
Параметры расширенной команды traceroute

Параметр	Описание
Protocol [ip]:	Запрос используемого протокола. Значение по умолчанию – IPv4.
Target IP address:	Необходимо ввести имя узла или IPv4-адрес. Нет значения по умолчанию.
Source address:	Интерфейс или IPv4-адрес маршрутизатора, которые будут использованы в качестве адреса источника для тестовых пакетов. Обычно маршрутизатор выбирает для использования IPv4-адрес исходящего интерфейса.
Numeric display [n]:	По умолчанию используется символическое и цифровое представление; однако символическое представление можно отключить.
Timeout in seconds [3]:	Количество секунд ожидания ответа на тестовый пакет. Значение по умолчанию – 3 секунды.
Probe count [3]:	Количество тестовых пакетов, которые необходимо отправить на каждом уровне времени существования. Количество по умолчанию – 3.
Minimum Time to Live [1]:	Значение времени существования для первых тестовых пакетов. Значение по умолчанию – 1, однако можно установить более высокое значение, чтобы не показывать известные переходы.
Maximum Time to Live [30]:	Максимальное значение времени жизни, которое может быть использовано. Значение по умолчанию – 30. Выполнение команды traceroute завершается при достижении адреса назначения или достижении этого значения.
Port Number [33434]:	Порт назначения, используемый тестовыми сообщениями UDP. Значение по умолчанию – 33434.
Loose, Strict, Record, Timestamp, Verbose [none]:	Параметры IP-заголовка. Можно указать любое сочетание. Команда traceroute отображает запросы для настройки обязательных полей. Учтите, что команда traceroute будет добавлять запрошенные параметры в каждый тестовый пакет, однако нет гарантии, что все маршрутизаторы (или конечные узлы) обработают эти параметры.

- Расширенная команда traceroute позволяет сетевому администратору настроить параметры, связанные с этой командой.
- Эта команда может пригодиться при поиске и устранении петель маршрутизации, определении точного маршрутизатора следующего перехода либо определении места, в котором пакет отбрасывается маршрутизатором или отклоняется межсетевым экраном.
- Расширенная команда traceroute помогает выявить неполадку. Чтобы использовать эту команду, введите **traceroute** и нажмите клавишу ВВОД.
- Команда **ping** отправляет ICMP-пакеты, а **traceroute** — IP-пакеты со значением TTL (30 по умолчанию).

Packet Tracer. Проверка подключения с помощью команды traceroute

Packet Tracer. Проверка подключения с помощью инструмента Traceroute Topology



Задачи

Часть 1. Проверка сквозного подключения при помощи команды tracert

Часть 2. Сопоставление с командой traceroute на маршрутизаторе

Общие сведения

Цель этого задания – помочь вам при поиске и устранении проблем сетевого соединения с помощью служебных команд для отслеживания маршрута от источника к адресату. Вам необходимо проверить выходные данные команд **tracert** (команда Windows) и **traceroute** (команда IOS) в процессе перемещения пакетов по сети и определить причину сетевых неполадок. Когда проблема будет решена, убедитесь в ее окончательном устранении при помощи команд **tracert** и **traceroute**.

- В этом упражнении Packet Tracer вы будете выполнять поиск и устранение неполадок сетевых подключений с помощью команд трассировки.
- Вы должны будете изучить выходные данные команды **tracert** и **traceroute**, чтобы выявить неполадку.
- Когда проблема будет устранена, потребуется убедиться в правильности работы, используя те же команды.

Лабораторная работа. Проверка задержек в сети с помощью команд ping и traceroute

Лабораторная работа. Проверка задержек сети с помощью ping-запроса и команды traceroute

Топология

Задачи

Часть 1. Регистрация задержки сети с помощью команды ping

Часть 2. Регистрация задержки сети с помощью команды traceroute

Общие сведения/сценарий

Для получения достоверной информации о задержке сети это задание необходимо выполнять в рабочей сети. Вместе с инструктором проверьте, существуют ли ограничения на использование **ping**запроса в локальной сети.
Цель этой лабораторной работы — измерить и оценить задержку сети за определенное время и составить наглядные примеры типовой активности сети в различное время суток. Для этого вы проанализируете задержку ответа на **ping**запрос удаленного компьютера. Используя время задержки эхо-ответа в миллисекундах, вычислите среднюю задержку и диапазон (минимальное и максимальное значения) продолжительности задержки.

- В этой лабораторной работе вы проверите задержку в работающей сети с помощью команд **ping** и **traceroute**.
- Чтобы получить реалистичную статистику задержек в сети, необходимо использовать работающую сеть.

Повторное рассмотрение наиболее распространенных команд show

```
R1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
```

- Технические специалисты по сетям широко используют команды show для проверки конфигурации и работы устройства или для поиска и устранения неполадок.
- Наиболее распространенные команды show:
  - show running-config
  - show interfaces
  - show arp
  - show ip route
  - show protocols
  - show version

Демонстрационное видео. Команда show version

```
Router>enable
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M2, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 06-Feb-15 17:01 by prod_rel_team

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

Router uptime is 33 minutes
System returned to ROM by reload at 18:46:50 UTC Mon Jun 1 2015
System image file is "flash0:c1900-universalk9-mz.SPA.154-3.M2.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command


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.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
 --More--
```

- Это видео демонстрирует выходные данные команды **show version** при ее запуске на маршрутизаторе Cisco 1941.
- На рисунке слева выделена версия программного обеспечения IOS.
- Рассматриваются сведения о выходных данных, в том числе следующие:
  - Время, в течение которого работал маршрутизатор
  - Информация о версии
  - Сведения об интерфейсе и памяти

Packet Tracer. Использование команд show

Packet Tracer. Использование команд show

Задачи

Часть 1. Анализ выходных данных команды show

Часть 2. Вопросы для повторения

Общие сведения

Это упражнение предназначено для закрепления знаний о командах **show** маршрутизатора. Вам не нужно будет выполнять настройку, вы просто изучите выходные данные отдельных команд **show**.

Часть 1. Анализ выходных данных команды show

Шаг 1. Подключитесь к маршрутизатору ISPRouter.

a. Щелкните **ISP PC** (ПК интернет-провайдера), откройте вкладку **Desktop** (Рабочий стол) и выберите **Terminal** (Терминал).

b. Войдите в привилегированный режим EXEC.

c. Используйте следующие команды **show**, чтобы ответить на вопросы для закрепления из части 2:

```
show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
show version
```

- В этом упражнении Packet Tracer вы поработаете с различными командами **show** и изучите их выходные данные.

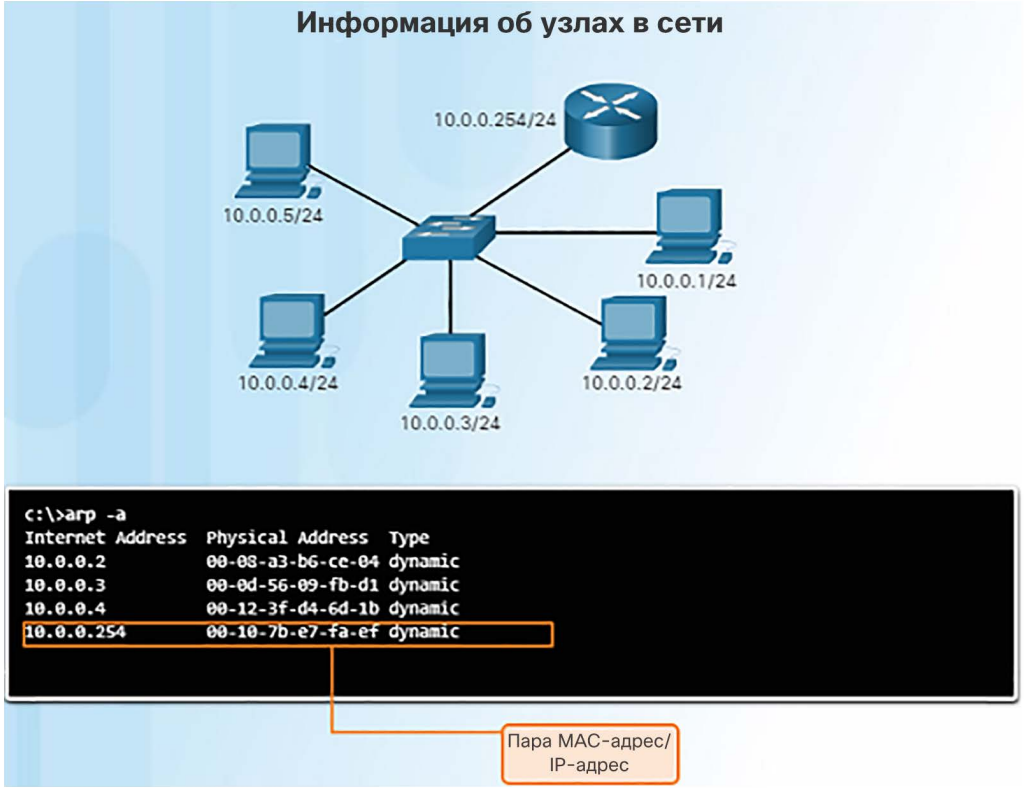
Команда ipconfig

ipconfig /all

```
C:\>ipconfig /all
Ethernet adapter Network Connection:
        Connection-specific DNS Suffix: example.com
        Description . . . . . . . . . . . : Intel(R)
        PRO/Wireless 3945ABG Network Connection
        Physical Address. . . . . . . . . : 00-18-DE-C7-F3-FB
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.2.3.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.2.3.254
        DHCP Server . . . . . . . . . . . : 10.2.3.69
        DNS Servers . . . . . . . . . . . : 192.168.226.120
        Lease Obtained. . . . . . . . . . : Thursday, May 03,
                                            2007 3:47:51 PM
        Lease Expires . . . . . . . . . . : Friday, May 04,
                                            2007 6:57:11 AM
C:\>
```

- На компьютере с ОС Windows можно просмотреть IP-адрес шлюза по умолчанию с помощью команды **ipconfig**.
- Команду **Ipconfig /all** можно использовать для просмотра MAC-адреса, а также других важных сведениях об адресации уровня 3 для устройства.
- На ПК с операционной системой Windows команда **ipconfig /displaydns** выводит на экран все кэшированные записи DNS.

Команда arp



- На компьютере с ОС Windows команда **arp -a** выводит список всех устройств, хранящихся в ARP-кэше конкретного хоста.
- Для каждого устройства отображается IPv4-адрес, физический адрес и тип адресации (статическая или динамическая).
- ARP-кэш можно очистить с помощью команды **arp-d**.

Команда show cdp neighbors

```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge,
                  B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP,
                  r - Repeater, P - Phone

Device ID  Local Intrfce  Holdtme  Capability  Platform  Port ID
S3         Fas 0/0        151      S I         WS-C2950  Fas 0/6
R2         Ser 0/0/1      125      R           1841      Ser 0/0/1

R3#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M),
Version 12.4(10b), RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
```

- Протокол Cisco Discovery Protocol (CDP) — это собственный протокол Cisco, функционирующий на канальном уровне, который позволяет соседним устройствам Cisco узнать друг о друге даже в отсутствие подключения уровня 3.
- Во время загрузки устройства Cisco протокол CDP запускается по умолчанию. CDP автоматически обнаруживает соседние устройства, на которых работает протокол CDP.
- Протокол CDP предоставляет следующие сведения о каждом из соседних устройств CDP: идентификаторы устройств, список адресов, идентификатор порта, список функций и платформу.
- Команда **show cdp neighbors detail** отображает IP-адрес соседнего устройства.

Команда show ip interface brief

Тестирование интерфейса

```
R1# show ip interface brief
Interface              IP-Address       OK?  Method  Status              Protocol
FastEthernet0/0        192.168.254.254  YES  NVRAM   up                   up
FastEthernet0/1        unassigned       YES  unset   down                 down
Serial0/0/0            172.16.0.254     YES  NVRAM   up                   up
Serial0/0/1            unassigned       YES  unset   administratively  down
                                                     down
```

- Одна из наиболее часто используемых команд для проверки конфигурации интерфейса и состояния всех интерфейсов — это команда **show ip interface brief**.
- Эта команда выводит сокращенные сведения по сравнению с командой **show ip interface** и предоставляет обзор основной информации по всем сетевым интерфейсам на маршрутизаторе.
- Команда предоставляет различные сведения, включая IP-адрес, назначенный каждому интерфейсу, и рабочее состояние интерфейса.

Лабораторная работа. Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах

Лабораторная работа. Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах

Топология

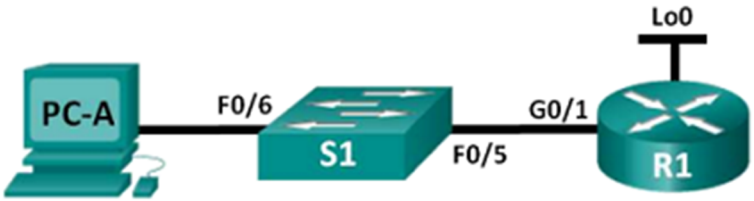


Таблица адресации

Устройство	Интерфейс	IP-адреса	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	Lo0	209.165.200.225	255.255.255.224	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Часть 2. Настройка устройств и проверка подключения

Часть 3. Сбор сведений о сетевых устройствах

- Одна из наиболее важных задач, выполняемых сетевыми специалистами, состоит в документировании сети.
- В этой лабораторной работе вы построите небольшую сеть, выполните настройку устройств, добавите некоторые основные средства защиты, а затем создадите документацию для полученной конфигурации, выполняя на маршрутизаторе, коммутаторе и компьютере различные команды.

Команда debug

Выходные данные команды debug ip icmp

```
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
*Nov 13 12:56:08.147: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
R1# undebug all
All possible debugging has been turned off
R1#
```

- Процессы, протоколы, механизмы и события IOS генерируют сообщения для индикации их состояния.
- Эти сообщения могут оказаться ценным источником информации при поиске и устранении неполадок, а также при проверке работы системы.
- Команда **debug** в IOS, введенная в привилегированном режиме EXEC, позволяет администратору отобразить эти сообщения в реальном времени для анализа.
- Это позволяет включить в выходные данные команды **debug** только необходимую функцию или подфункцию.

Команда terminal monitor

Введите команду, разрешающую передачу сообщений журнала в ваш удаленный сеанс.

```
R1# terminal monitor
R1#
```

Введите следующие команды поиска и устранения неполадок:

- Введите команду debug, которая будет контролировать состояние сообщений ICMP маршрутизатора R1.
- Отправьте эхо-запрос на устройство с IP-адресом 10.0.0.10.
- Отключите отладку.

```
R1#
```

- Соединения для предоставления доступа к интерфейсу командной строки IOS могут устанавливаться локально или удаленно.
  - Для выполнения локального подключения требуется физический доступ к маршрутизатору или коммутатору по кабельному соединению.
  - Удаленные подключения по протоколам SSH или Telnet выполняются по сети. Для них необходимо настроить сетевой протокол, например IP.
- Длинные сообщения отладки по умолчанию отправляются на консоль, а не по виртуальным каналам.
- Для отображения сообщений журнала на терминале или в виртуальной консоли используется команда привилегированного режима EXEC **terminal monitor**, а для выключения — команда **terminal no monitor**.

11.4. Поиск и устранение неполадок в работе сети

Основные подходы к поиску и устранению неполадок

Шесть шагов процедуры поиска и устранения неполадок

Шаг	Название	Описание
1	Определение неполадки	Первым этапом процедуры поиска и устранения неполадок является определение проблемы. На этом этапе можно использовать различные методы, в том числе, можно расспросить пользователя, что может оказаться очень полезным.
2	Формирование предположений о возможных причинах неполадки	После разговора с пользователем и определения проблемы можно попытаться сформировать предположения о ее возможных причинах. Обычно на этом этапе выявляется несколько возможных причин неполадки.
3	Проверка предположений о причине неполадки	Проверьте свои предположения о вероятных причинах проблемы, чтобы определить истинную причину. Технический специалист может попытаться устранить неполадку, применив быструю процедуру. Если с помощью быстрой процедуры не удается устранить неполадку, следует продолжить поиск точной причины.
4	Разработка плана действий по устранению неполадки и его реализация	Установив точную причину неполадки, разработайте план действий для ее устранения и выполните его.
5	Полная проверка функционального состояния системы и принятие профилактических мер	После устранения неполадки выполните полную проверку функционального состояния системы и при необходимости примите профилактические меры.
6	Документирование полученных данных, принятых мер и результатов	На последнем этапе процедуры поиска и устранения неполадок выполняется документирование полученных данных, выполненных действий и результатов. Эта информация очень важна для использования в будущем.

- Технические специалисты должны уметь проанализировать причины неполадки в работе сети, чтобы устранить ее.
- Этот процесс называется поиском и устранением неполадок.
- Общепринятая эффективная процедура основана на научном подходе и может быть разбита на шесть основных этапов, представленных на рисунке слева.
- На скольких устройствах в сети возникла проблема?
  - Если на одном устройстве, начните поиск и устранение неполадок на нем.
  - Если на всех устройствах, начните поиск и устранение неполадок на устройстве, к которому подключаются все эти устройства.

Что следует сделать: решить проблему или эскалировать ее?

- В некоторых случаях невозможно незамедлительно устранить неполадку в работе сети и может потребоваться передать ее на уровень выше, если необходимо решение руководителя.
- Например, осуществив поиск неполадок, технический специалист может прийти к выводу о том, что нужно заменить модуль маршрутизатора. Эта проблема требует передачи на более высокий уровень для утверждения руководителем, поскольку могут потребоваться финансовые расходы.

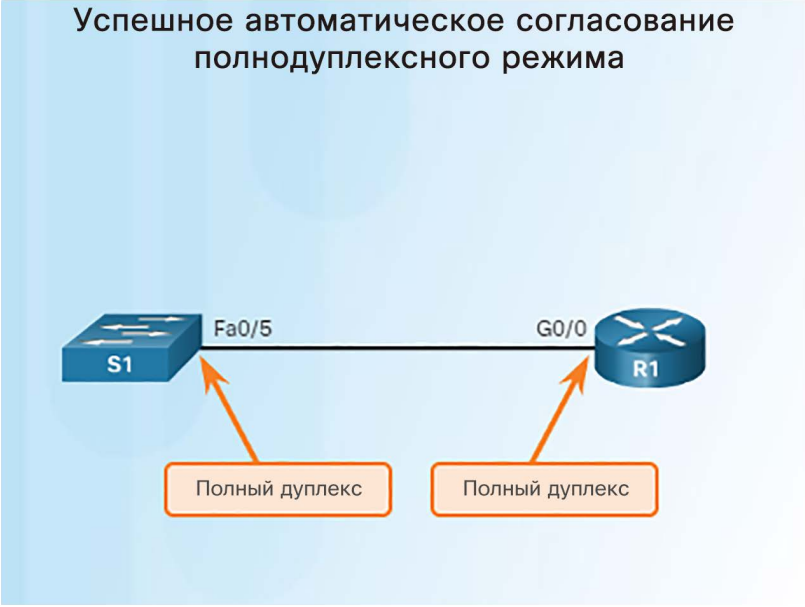
Проверка и контроль решения проблемы

Трассировка пути к месту назначения с помощью команды **traceroute**


```
R1# traceroute 10.3.0.1
Type escape sequence to abort.
Tracing the route to 10.3.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.0.2 12 msec 12 msec 16 msec
  2 10.2.0.2 24 msec *  24 msec
R1#
```

- В состав Cisco IOS входят мощные инструменты, которые упрощают поиск и устранение неполадок, а также помогают убедиться, что проблема решена:
- команда **ping** позволяет подтвердить успешное подключение к сети;
- команда **traceroute** показывает путь, который используется пакетами при перемещении к месту назначения, и помогает определить, где на этом пути пакеты останавливаются;
- команды show, включая **show ip int brief,** которые обеспечивают обзорное представление интерфейсов на устройстве.

Работа в дуплексном режиме

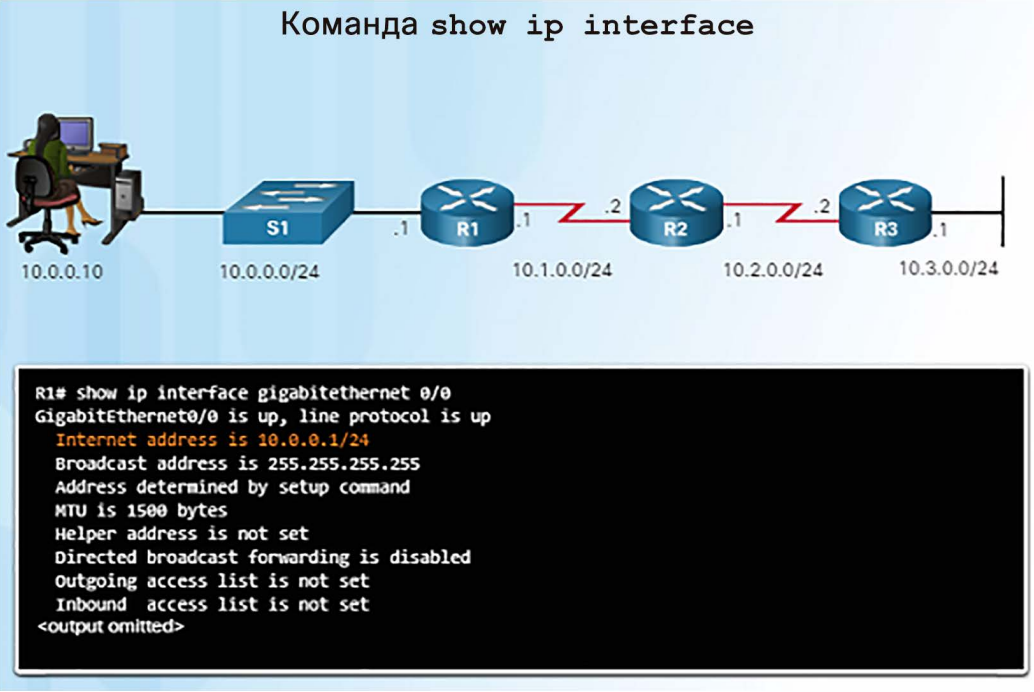


- В процессе передачи данных дуплексный режим относится к направлению передача данных между двумя устройствами, такими как маршрутизатор и коммутатор.
  - Полудуплексный режим — передача данных разрешена одновременно только в одном направлении.
  - Полнодуплексный режим — данные могут передаваться в обоих направлениях одновременно.
- Для повышения производительности связи у обоих подключенных сетевых интерфейсов Ethernet должны быть одинаковые настройки дуплексного режима.
  - Они должны быть настроены на работу или в полудуплексном, или в полнодуплексном режиме.
  - Чтобы помочь в настройке, было разработано автоматическое согласование Ethernet. Однако это может приводить к неполадкам, если на одном конце связи выбран автоматический режим, а на другой — нет.

Несовпадение дуплексных режимов

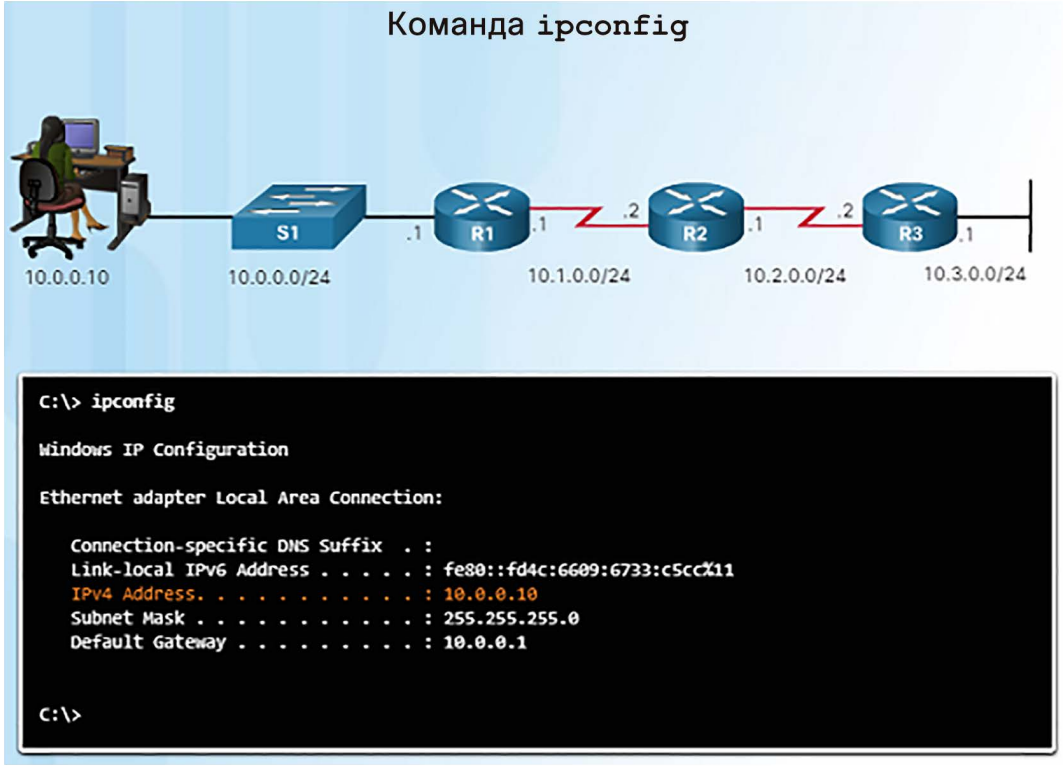
- Неполадки, связанные с несовпадением дуплексных режимов, сложно обнаружить, поскольку обмен данными между устройствами по-прежнему выполняется, но обычно намного медленнее.
  - Команда **ping** может не выявлять неполадку.
  - Ответ на эхо-запрос может приходить, несмотря на несоответствие режимов.
- Протокол Cisco Discovery Protocol (CDP) позволяет обнаружить несоответствие дуплексных режимов двух устройств Cisco, как показано на рисунке слева.
- Эти сообщения журнала отображаются только на консоли или при удаленном подключении, если используется команда **terminal monitor**.

Проблемы IP-адресации на устройствах IOS



- Проблемы, связанные с IP-адресами, с большой вероятностью приводят к сбоям подключения.
- Поскольку IP-адреса имеют иерархическую структуру, любой IP-адрес, назначенный сетевому устройству, должен соответствовать диапазону адресов своей сети.
- Двумя основными причинами неверного назначения IPv4-адресов являются ошибки ручной настройки конфигурации и неполадки, связанные с протоколом DHCP.
- Если во время назначения допущена ошибка, то велика вероятность того, что при связи с устройством возникнет проблема.
- Используйте команду **show ip interface brief** для проверки IPv4-адресов, назначенных сетевым интерфейсам.

Проблемы IP-адресации на оконечных устройствах



- Если компьютеру под управлением ОС Windows не удается связаться с сервером DHCP, Windows автоматически назначает компьютеру адрес в диапазоне 169.254.0.0/16, чтобы он мог обмениваться данными в пределах локальной сети.
- Как правило, это указывает на неисправность, и устройство, которому назначен такой адрес или диапазон адресов, не сможет обмениваться данными с другими устройствами в сети.
- Большинство оконечных устройств настраиваются с помощью DHCP на автоматическое назначение IPv4-адреса.
- Используйте команду **ipconfig** для проверки IP-адреса, назначенного компьютеру с ОС Windows.

Неполадки, связанные со шлюзом по умолчанию

- Шлюзом по умолчанию для оконечного устройства является ближайшее сетевое устройство, которое способно пересылать трафик в другие сети. Обычно это маршрутизатор.
- В отсутствие допустимого адреса шлюза по умолчанию узел не сможет обмениваться данными с устройствами за пределами локальной сети.
  - Шлюз по умолчанию для узла должен относиться к той же сети, в которой находится оконечное устройство.
  - Шлюз по умолчанию может быть настроен вручную или получен от сервера DHCP.
- Используйте команду **ipconfig** для проверки шлюза по умолчанию на компьютере с ОС Windows.
- Используйте команду **show ip route**, чтобы убедиться в правильности настройки шлюза по умолчанию.

Поиск и устранение неполадок, связанных с DNS

- Используйте команду **ipconfig/all** для получения сведений о DNS-сервере на ПК под управлением ОС Windows.

```
C:\> ipconfig /all


Ethernet adapter Local Area Connection:
<some output omitted>
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : F0-4D-A2-DD-A7-B2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 09, 2015 7:49:48 PM
   Lease Expires . . . . . . . . . . : Thursday, November 19, 2015 7:49:51 AM
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCP Server . . . . . . . . . . . : 10.0.0.1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- Служба доменных имен (DNS) используется для сопоставления имен, таких как www.cisco.com, с числовыми IP-адресами.
- В результате пользователь может ввести www.cisco.com в веб-обозревателе вместо ввода IP-адреса компании Cisco для своего веб-сервера.
- Если служба DNS не работает, некоторые пользователи могут столкнуться с «отключением сети», хотя на самом деле просто может быть недоступен DNS-сервер.
- Адреса сервера DNS могут быть заданы вручную или назначены автоматически с помощью DHCP.

Лабораторная работа. Поиск и устранение неполадок подключения

Топология

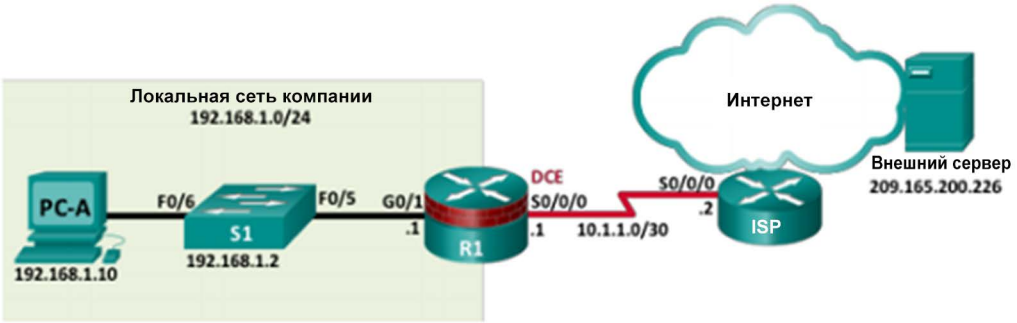


Таблица адресации

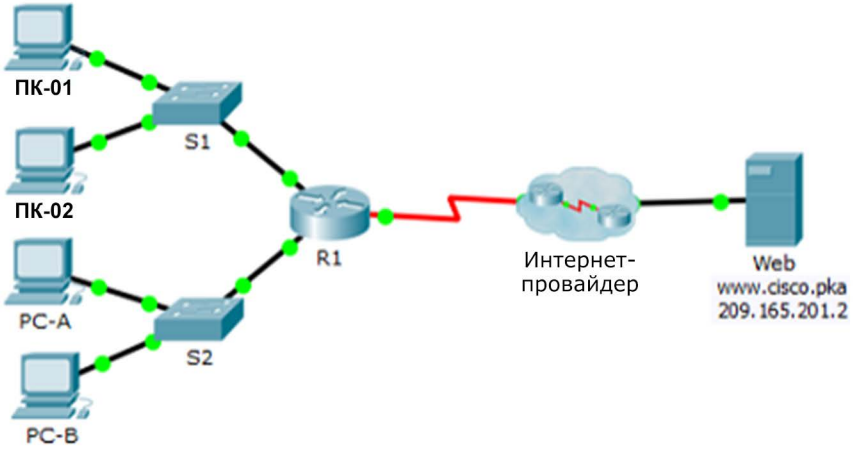
Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0	10.1.1.1	255.255.255.252	—
ISP	S0/0/0	10.1.1.2	255.255.255.252	—
	Lo0	209.165.200.226	255.255.255.255	—
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

- В этой лабораторной работе вы будете выполнять поиск и устранение неполадок в работе сети, используя навыки и инструменты, изученные вами в этой главе.
- Вы будете подключаться к устройствам и использовать различные средства для выявления неполадок в работе сети, высказывать предположения о возможных причинах, проверять свои предположения и устранять проблему.

Packet Tracer. Поиск и устранение неполадок подключения

Packet Tracer. Поиск и устранение неполадок подключения

Топология



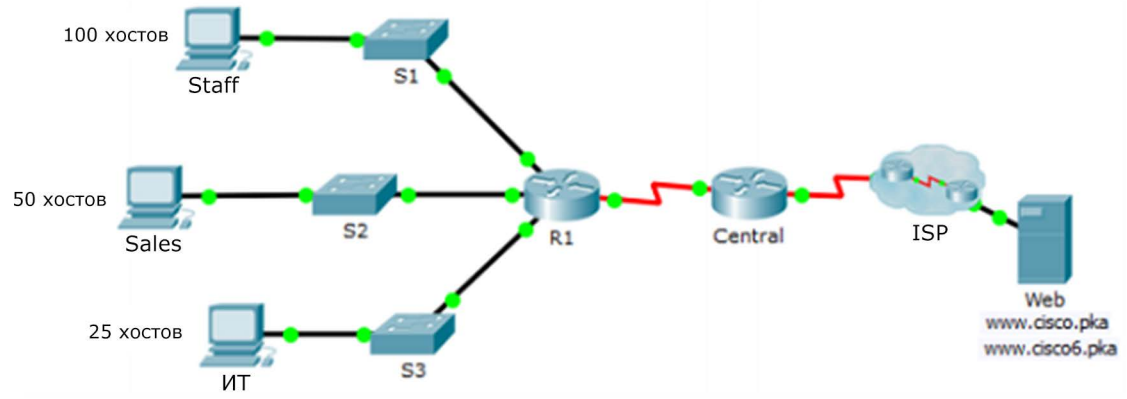
- В ходе этого упражнения в программе Packet Tracer вы будете выполнять поиск и устранение неполадок сетевых подключений, а если это невозможно, передавать их на более высокий уровень.
- Вам также потребуется подробно задокументировать неполадки и способы их устранения.

11.5. Выводы

Packet Tracer. Отработка комплексных практических навыков

Cisco Packet Tracer. Отработка комплексных практических навыков

Топология

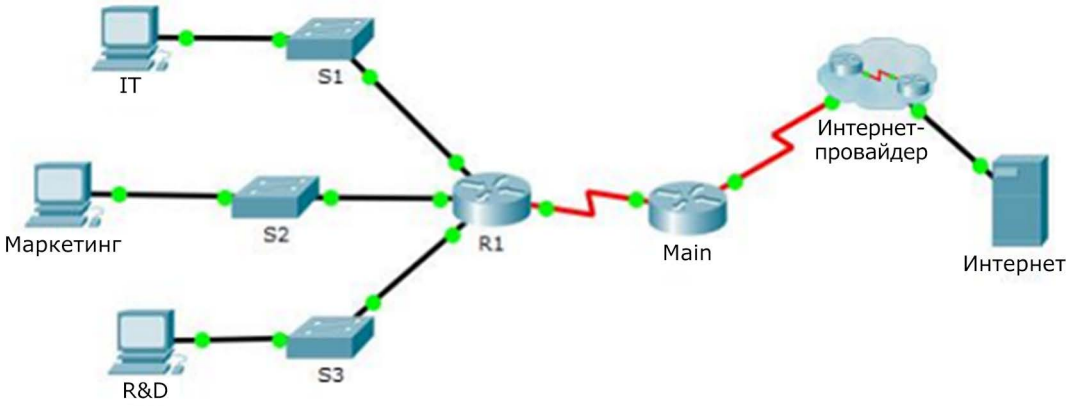


- В ходе этого упражнения Packet Tracer вам потребуется создать новую схему адресации IPv4, включающую четыре подсети с использованием сети 192.168.0.0/24.
- Вы также выполните базовую настройку безопасности и конфигурацию интерфейсов на маршрутизаторе R1.
- Кроме того, вы настроите интерфейс SVI и базовые параметры безопасности на коммутаторах S1, S2 и S3.

Packet Tracer. Поиск и устранение неполадок

Packet Tracer. Поиск и устранение неполадок

Топология



- В этом упражнения Packet Tracer вам потребуется исправить ошибки в конфигурации и проверить подключение между компьютерами и веб-сайтами, маршрутизаторами и коммутаторами.
- Компьютеру должен быть разрешен доступ к маршрутизатору R1 по протоколу SSH.

Глава 11. Создание сети небольшого размера

- Объясните функции и возможности ПО Cisco IOS.
- Настройте исходные параметры на сетевом устройстве с помощью ПО Cisco IOS.
- С учетом схемы IP-адресации настройте параметры IP-адресов на оконечных устройствах, чтобы обеспечить сквозное подключение в сети малого и среднего бизнеса.

Новые термины и команды

- В этой главе нет новых терминов и команд.

CISCO