- **Локальная сеть (LAN)** — сетевая инфраструктура, которая обеспечивает доступ пользователям и оконечным устройствам в небольшой географической области.

Локальные сети связывают оконечные устройства в ограниченной области, например, в доме, школе, офисном здании или комплексе зданий.
Локальная сеть обычно администрируется одной организацией или частным лицом. Администратор управляет политикой безопасности и контролем доступа на сетевом уровне.
Локальные сети предоставляют высокоскоростной доступ к внутренним оконечным и промежуточным устройствам.

- **Глобальная сеть (WAN)** — сетевая инфраструктура, которая предоставляет доступ к другим сетям на обширной географической области.

Основные компоненты WAN

WAN связывают локальные сети в обширных географических областях, таких как города, регионы, страны или континенты.
Управление глобальными сетями обычно осуществляется различными операторами связи.
Глобальные сети обычно обеспечивают более низкоскоростные соединения между локальными сетями.

Концепция BYOD

«Принеси на работу своё собственное устройство» (Bring Your Own Device, BYOD) значит, что конечные пользователи имеют свободу использования личных инструментов доступа к информации на предприятии или в сети учебного заведения. По мере увеличения популярности устройств и соответствующего падения цен ожидается, что каждый из сотрудников и учащихся может иметь в личном пользовании самые совершенные вычислительные и сетевые инструменты. Эти персональные средства включают в себя ноутбуки, нетбуки, смартфоны, планшетные ПК и электронные книги. BYOD означает возможность использования в любом месте любого устройства, независимо от его владельца. в средах BYOD сотрудники используют преимущества передачи голоса, видео и проведения конференций во время совместной работы. Не менее важно учитывать внутренние угрозы. . В концепции BYOD корпоративные данные намного более уязвимы.

TCP/IP

Семейство протоколов IP — это набор протоколов, необходимых для передачи и приёма информации с использованием Интернета. Этот протокол более известен как TCP/IP, потому что двумя первыми сетевыми протоколами, определёнными для этого стандарта, являлись TCP и IP.
Модель TCP/IP часто используется для описания стека протоколов. Где под стеком протоколов можно понимать множество взаимодействующих протоколов, обеспечивающих функциональность сети.
Первой сетью с коммутацией пакетов и предшественником современного Интернета была (ARPANET) TCP/IP на 4 уровня
Уровень приложений Транспортный Межсетевой Уровень сетевого доступа Уровень приложений – Представляет данные пользователю, а также кодирование и управление диалоговыми окнами
Транспортный уровень – Поддерживает связь между различными устройствами в разных сетях
Межсетевой уровень – Определяет наилучший путь через сеть
Уровень сетевого доступа – Управляет устройствами и средами, формирующими сеть

Модели OSI & TCP/IP имеют идентичные уровни Transport и Internet (Network), на которые возложены соответственно одинаковые задачи

1.1 - Опишите концепт конвергентной сети.

Конвергентная сеть - это вычислительная сеть, сочетающая передачу голосовой информации (включая, но не ограничиваясь телефонными переговорами) и данных (включая мультимедиа, видеосвязь и т.д.) по общему каналу, что обеспечивает:
упрощение корпоративных коммуникаций (замена нескольких независимых сетей единой сетью);
возможность работы с разнородной информацией (голос, видео, электронная почта, файлы и т.д.) на едином пользовательском терминале (при этом, обычный ПК вполне может выступать в этой роли);
дополнительную функциональность и упрощение работы при обмене разнородной информацией и ее обработке.
Среди них обязательно должна присутствовать система обеспечения безопасности коммуникаций, надежная сеть передачи данных, широкий набор коммуникационных сервисов, которые обеспечивают адекватную коммутацию для разных типов данных на разных уровнях.

Модель OSI

Сетевая модель OSI состоит из 7 уровней, причем принято начинать отсчёт с нижнего.
Перечислим их:
7. Прикладной уровень (application layer) Прикладной уровень или уровень приложений(application layer) – это самый верхний уровень модели. Он осуществляет связь пользовательских приложений с сетью. Эти приложения нам всем знакомы: просмотр веб-страниц (HTTP), передача и приём почты (SMTP, POP3), приём и получение файлов (FTP, TFTP), удаленный доступ (Telnet)
6. уровень представления (presentation layer) уровень представления данных (presentation layer) – он преобразует данные в соответствующий формат. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером протокола, работающего на уровне представления, является протокол Secure Socket Layer (SSL)
5. Сеансовый уровень (session layer) Сеансовый уровень или уровень сессий(session layer) – как видно из названия, он организует сеанс связи между компьютерами. примером может служить протокол SMPP (Short message peer-to-peer protocol), с
4. Транспортный уровень (transport layer) этот уровень обеспечивает надёжность передачи данных от отправителя к получателю Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням стека - прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP
3. Сетевой уровень (network layer) Этот уровень служит для образования единой транспортной системы, объединяющей несколько сетей с различными принципами передачи информации между конечными узлами
2. Канальный уровень (data link layer) одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит в начало и конец каждого кадра,
1. Физический уровень (physical layer) осуществляющий передачу потока данных..Этот уровень имеет дело с передачей битов по физическим каналам, таким, например, как коаксиальный кабель, витая пара или оптоволоконный кабель.

Структура команд cisco ios

№1: "?" используйте ?, если не знаете какую команду написать. Например, вы можете написать ? в командной строке для вывода всех возможных команд.
№2: show running-configuration Команда *show running-config* показывает текущую конфигурацию устройства. Running-configuration – это конфигурация, загруженная в данный момент в оперативную память
роутера конфигурация не сохраняется пока не выполнить c*opy running-configuration startup-configuration*.
№3: copy running-configuration startup-configuration Эта команда сохранит текущие модификации в настройках (running-configuration, которая хранится в RAM), в энергонезависимую RAM (NVRAM). Если внезапно исчезнет электропитание, то данные в NVRAM сохранятся
№4: show interface Команда *show interface* отображает состояние интерфейсов маршрутизатора.
№6: config terminal, enable, interface, and router в user mode (пользовательский режим, где приглашение выглядит как >). В этом режиме можно написать *enable* для переключения в привилегированный режим (приглашение выглядит как #). В привилегированном режиме отображается любая информация, но нельзя вносить никакие изменения. Для того, чтобы попасть в режим глобальной конфигурации введите *config terminal* (или *config t*), приглашение станет выглядеть как (config)# . В этом режиме можно изменять любые настройки. Для изменения параметра интерфейса (например, IP-адреса) переключитесь в режим конфигурирования командой *interface* (приглашение выглядит как (config-if)#).
№7: no shutdown Команда *no shutdown* включает интерфейс. для того, чтобы выключить интерфейс введите *shutdown*.

Защита

Компоненты безопасности сетей для дома или в сетях малых офисов должны содержать как минимум:

- **Антивирусное и антишпионское программное обеспечение** — защита устройства конечных пользователей от вирусов и от вредоносного ПО
- **Фильтрация на межсетевом экране** — блокирование попыток несанкционированного доступа к сети Они могут включать в себя систему реализованных на узле межсетевых экранов, которая используется для предотвращения несанкционированного доступа к устройству узла, или базовый сервис фильтрации на домашнем маршрутизаторе для предотвращения несанкционированного доступа из внешнего мира в сеть.

Кроме вышеперечисленного, в более крупных сетях и корпоративных сетях часто имеются другие требования безопасности:

- **Выделенные системы межсетевых экранов** — обеспечение более совершенных функциональных возможностей межсетевого экрана, который может фильтровать большое количество трафика с большей детализацией
- **Списки контроля доступа (ACL)** — дальнейшая фильтрация доступа, а также обеспечение пересылки трафика
- **Системы предотвращения вторжений (IPS)** — определение быстро распространяющихся угроз, таких как атаки нулевого дня или атаки нулевого часа
- **Виртуальные частные сети (VPN)**— обеспечение безопасного доступа для удалённых сотрудников

Методы доступа

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

- Консоль
  Консольный порт — это порт управления, обеспечивающий возможность внеполосного доступа к устройству Cisco. Внеполосный доступ — это доступ через выделенный административный канал, который используется исключительно в целях технического обслуживания устройства. Преимущество использования порта консоли состоит в том, что доступ к устройству возможен даже без настройки сетевых услуг, например, начальной конфигурации сетевого устройства
  Консольный порт также можно использовать, когда работа сетевых сервисов нарушена и удалённый доступ к устройству на базе CISCO IOS невозможен
- Telnet или SSH
  Telnet — это способ удалённого установления сеанса интерфейса командной строки (CLI) через виртуальный интерфейс по сети. В отличие от консольного подключения, для сеансов Telnet требуются активные сетевые сервисы на устройстве. В сетевом устройстве должен быть настроен хотя бы один активный интерфейс с интернет-адресом, например, с адресом IPv4.
  Протокол Secure Shell (SSH) предоставляет удалённый вход в систему аналогично Telnet, за исключением того, что он использует более безопасные сетевые службы. Протокол SSH предоставляет более высокий уровень аутентификации на основе пароля, чем протокол Telnet
- Порт AUX
  Устаревший метод установления сеанса интерфейса командной строки (CLI) — с помощью коммутируемого соединения по телефону к вспомогательному порту (AUX) маршрутизатора Порт AUX может также использоваться локально, как и консольный порт, с прямым подключением к компьютеру, на котором работает программа эмуляции терминала

Инкапсуляция и декапсуляция

Инкапсуляция данных — процесс, который добавляет к данным содержимое заголовка дополнительного протокола перед передачей. В большинстве форм передачи данных первоначальные данные подвергаются инкапсуляции нескольких протоколов до начала передачи
чтобы иллюстрировать процесс отправки клиенту веб-страницы в формате HTML.
Протокол прикладного уровня (HTTP) запускает процесс, предоставляя отформатированные данные HTML веб-страницы транспортному уровню. В нём данные приложения разбиваются на сегменты TCP. Каждому сегменту TCP присваивается метка, называемая заголовком и содержащая информацию о том, какой процесс, запущенный на компьютере назначения, должен получить сообщение. Кроме того, он содержит информацию, которая помогает процессу назначения собрать данные обратно в исходный формат.
Транспортный уровень инкапсулирует данные веб-страницы в формате HTML в сегменте и передаёт его на межсетевой уровень, где реализован протокол IP. В нём весь сегмент TCP инкапсулируется в IP-пакет, и к нему добавляется еще одна метка, называемая заголовком IP. В заголовке IP указываются IP-адреса узлов отправителя и получателя, а также данные, необходимые для доставки пакета соответствующему процессу назначения.
Далее этот пакет IP передаётся на уровень сетевого доступа, где он инкапсулируется — к нему добавляются заголовок кадра и Концевик.
Обратный процесс на принимающем узле называется деинкапсуляцией. Деинкапсуляция — процесс, который выполняется приёмным устройством, чтобы удалить один или несколько заголовков протоколов. Данные деинкапсулируются по мере продвижения по стеку к приложениям для конечных пользователей

Типы кабелей

- **Прямой кабель Ethernet**: наиболее распространённый тип сетевого кабеля; как правило, используется для подключения узла к коммутатору и коммутатора к маршрутизатору. Стандарт T586A T586B оба конца
- **Перекрёстный кабель Ethernet**: Соединяет 2 узла сети. не распространённый тип кабеля; используется для соединения аналогичных устройств друг к другу, например, для подключения коммутатора к коммутатору, узла к узлу или маршрутизатора к маршрутизатору.
  Один конец T586A др T586B
- **Инверсный кабель**: кабель, запатентованный компанией Cisco; Соединяет последовательный порт рабочей станции к порту консоли маршрутизатора с помощью адаптера

Топологии сети

Топология сети — расположение или взаимоотношение сетевых устройств, а также взаимозависимость между ними. Топологии локальных и глобальных сетей можно рассматривать в двух видах.

- **Физическая топология**: термин, используемый для обозначения физических подключений, определяет, каким образом подключены оконечные устройства и устройства сетевой инфраструктуры, такие как маршрутизаторы, коммутаторы и беспроводные точки доступа. Физическая топология может быть двухточечной («точка-точка») или звездообразной.

Точка –точка Физические двухточечные топологии напрямую связывают два узла двум узлам не нужно совместно использовать одну среду передачи с другими узлами. Кроме того, узлу не нужно определять, адресован ли входящий кадр именно для него или адресован на другой узел Один узел размещает кадры на одном конце, а другой узел получает эти кадры на другом конце двухточечного соединения.

Топология типа «звезда»: оконечные устройства подключаются к центральному промежуточному устройству теперь в топологиях типа «звезда» используются коммутаторы. Топология типа «звезда» - это наиболее распространённая физическая топология локальной сети, главным образом потому, что она проста в установке, модификации (легко добавлять и удалять оконечные устройства) и удобна в устранении неполадок.

Расширенная звездообразная или гибридная. В расширенной звездообразной топологии центральные промежуточные устройства соединяют остальные звездообразные топологии. В гибридной топологии звездообразные сети могут соединяться с использованием топологии шины.

Топология шины: все конечные системы связаны друг с другом общей шиной (проводником, кабелем) и имеют оконцовку на концах шины. Шинные топологии использовались в устаревших сетях Ethernet, поскольку были дешёвыми и легко устанавливались.

Кольцевая топология: конечные системы подключены к соседнему узлу, формируя связь в форме кольца. В отличие от шинной топологии, кольцевая не требует оконцовки

- **Логическая топология**: термин, используемый для обозначения способа передачи кадров от одного узла к следующему. Такое расположение состоит из виртуальных соединений между узлами сети. Эти логические пути сигнала определены протоколами канального уровня. Логическая топология двухточечных каналов сравнительно проста. При этом общая среда предлагает детерминированные и недетерминированные методы контроля доступа.

Точка-точка Конечные узлы, сообщающиеся по двухточечной сети, могут быть физически подключены с помощью нескольких промежуточных устройств В некоторых случаях логическое соединение между узлами формирует так называемый виртуальный канал. Виртуальный канал — это логическое соединение, созданное в сети между двумя сетевыми устройствами. Два узла по обоим концам виртуального канала обмениваются кадрами между собой. Это происходит и в том случае, если кадры передаются через промежуточные устройства.