Switch {

1. enable - переход в привилегированный режим

2. configure terminal - переход в режим настройки

3. interface [номер интерфейса] - выбор интерфейса для настройки

4. ip address [адрес] [маска] - назначение IP-адреса интерфейсу

5. no shutdown - включение интерфейса

6. shutdown - выключение интерфейса

7. show interfaces - отображение информации об интерфейсах

8. show ip route - отображение таблицы маршрутизации

9. show running-config - отображение текущей конфигурации устройства

10. copy running-config startup-config - сохранение текущей конфигурации в постоянную память устройства

11. ping [адрес] - отправка ICMP-запросов на указанный адрес для проверки доступности

12. traceroute [адрес] - отображение маршрута следования пакетов до указанного адреса

13. clock set [время] - установка времени на устройстве

14. exit/logout - выход из текущего режима настройки или привилегированного режима

15. reload - перезагрузка устройства

16. hostname [имя] - назначение имени устройства

17. banner motd [текст] - настройка баннера для вывода сообщения перед входом в систему

18. access-list [номер] permit/deny [протокол] [адрес источника] [маска источника] [адрес назначения] [маска назначения] - создание списка доступа для фильтрации трафика.

19. ip domain-name [имя домена] - настройка доменного имени.

20.username [имя пользователя ] privilege [уровень привелегий] secret [пароль] - создание пользователя

21.crypto key generate rsa - сгенерировать ключ rsa

22. transport input ssh - настройка интерфейса чтобы он мог принимать команды SSH-соединения

23. connect - открыть соединение с терминалом

24. desable[ранее введенная команда] - отменяет указанную команду

25. disconnect[номер сети от 1 до 16] - отключиться от сети.

26. resume [1-16] - активировать соединение с сетью

27. write memory - сохранить настройки

28. line vty 0 4- настройка консоли

28. transport input telnet - настройка подключения по telnet

}

Router{

1. enable - переход в привилегированный режим

2. configure terminal - переход в режим настройки

3. interface [номер интерфейса] - выбор интерфейса для настройки

4. ip address [адрес] [маска] - назначение IP-адреса интерфейсу

5. no shutdown - включение интерфейса

6. shutdown - выключение интерфейса

7. show interfaces - отображение информации об интерфейсах

8. show ip route - отображение таблицы маршрутизации

9. show running-config - отображение текущей конфигурации устройства

10. copy running-config startup-config - сохранение текущей конфигурации в постоянную память устройства

11. ping [адрес] - отправка ICMP-запросов на указанный адрес для проверки доступности

12. traceroute [адрес] - отображение маршрута следования пакетов до указанного адреса

13. telnet [адрес] - подключение к удаленному устройству по протоколу Telnet

14. ssh [адрес] - подключение к удаленному устройству по протоколу SSH

15. clock set [время] - установка времени на устройстве

16. exit - выход из текущего режима настройки или привилегированного режима

17. reload - перезагрузка устройства

18. hostname [имя] - назначение имени устройства

19. banner motd [текст] - настройка баннера для вывода сообщения перед входом в систему

20. access-list [номер] permit/deny [протокол] [адрес источника] [маска источника] [адрес назначения] [маска назначения] - создание списка доступа для фильтрации трафика.

21. router ospf [номер процесса OSPF] - включение протокола маршрутизации OSPF на роутере

22. network [адрес сети] [маска сети] area [номер зоны OSPF] - добавление сети в зону OSPF

23. show ip ospf neighbor - отображение соседей OSPF на роутере

24. show ip ospf interface - отображение информации об интерфейсах, подключенных к OSPF

25. ip route [адрес сети] [маска сети] [адрес следующего хопа или интерфейс] - добавление статического маршрута в таблицу маршрутизации.

26. ip nat inside source static [локальный адрес] [глобальный адрес] - настройка статического NAT для перевода локальных адресов в глобальные.

27. ip nat inside source list [номер списка доступа] interface [интерфейс] overload - настройка динамического NAT для перевода локальных адресов в глобальные с использованием перегрузки адресов.

28. access-list [номер] permit/deny [протокол] [адрес источника] [маска источника] [адрес назначения] [маска назначения] - создание списка доступа для фильтрации трафика при использовании NAT.

29. show ip nat translations - отображение текущих трансляций NAT на устройстве.

30. LASP (Local Address Selection Protocol) - протокол, позволяющий автоматически выбирать локальный адрес для исходящего трафика при использовании NAT. Он определяет наиболее подходящий локальный адрес на основе доступных интерфейсов и их параметров, таких как пропускная способность и задержка.

31. ip nat pool [имя пула] [глобальный начальный адрес] [глобальный конечный адрес] netmask [маска сети] - создание пула глобальных адресов для использования в динамическом NAT.

32. ip nat inside destination [адрес назначения] [маска назначения] [локальный адрес] - настройка NAT для перенаправления входящего трафика на локальный адрес.

33. ip nat outside source static [глобальный адрес] [локальный адрес] - настройка статического NAT для перевода глобальных адресов в локальные.

34. ip nat outside source list [номер списка доступа] interface [интерфейс] - настройка динамического NAT для перевода глобальных адресов в локальные без использования перегрузки адресов.

35. ip nat inside source static tcp/udp [локальный адрес] [номер порта] [глобальный адрес] [номер порта] - настройка статического NAT для перевода локальных портов в глобальные.

36. ip nat inside source list [номер списка доступа] pool [имя пула] - настройка динамического NAT с использованием пула глобальных адресов.

37. ip nat inside source static route-map [имя маршрутной карты] - настройка статического NAT с использованием маршрутной карты для выбора соответствующего глобального адреса.

38. route-map [имя маршрутной карты] permit [номер] match ip address [номер списка доступа] set ip next-hop [адрес следующего перехода] - создание маршрутной карты для использования в статическом NAT.

39. HSRP (Hot Standby Router Protocol) - протокол, позволяющий создать виртуальный IP-адрес, который будет использоваться в качестве шлюза по умолчанию для устройств в сети. Он также обеспечивает резервирование между несколькими маршрутизаторами, чтобы обеспечить непрерывность работы сети в случае отказа одного из маршрутизаторов.

40. interface [интерфейс] standby [номер группы HSRP] ip [виртуальный IP-адрес] - настройка интерфейса для работы с HSRP.

41. standby [номер группы HSRP] priority [приоритет] - настройка приоритета для маршрутизатора в группе HSRP.

42. standby [номер группы HSRP] preempt - настройка маршрутизатора для автоматического захвата роли активного маршрутизатора при его восстановлении после отказа.

43. standby [номер группы HSRP] track [интерфейс/объект] [приоритет] - настройка отслеживания состояния интерфейса или объекта и автоматического изменения приоритета HSRP в зависимости от его состояния.

44. standby [номер группы HSRP] authentication [тип] [ключ] - настройка аутентификации для HSRP с использованием предоставленного ключа.

45. show standby - команда для отображения информации о конфигурации и состоянии HSRP на маршрутизаторе.

}

Создние DHCP сервера на роутере{

en

conf t

ip dhcp pool dhcp100

network 192.168.1.0 255.255.255.0

default-router 192.168.1.254

dns-server 8.8.8.8

exit

service dhcp

ip dhcp excluded-address 192.168.1.254

ip dhcp excluded-address 192.168.1.253

}

Создание подключения по ssh{

en

conf t

enable secret admin

username admin secret admin

ip domain-name org.lan

crypto key generate rsa

line vty 0 4

login local

transport input ssh

}

Настройка NAT если Ethernet0/1/0 внешний порт{

en

conf t

int ethernet 0/1/0

ip nat outside

ex

int fa 0/0

ip nat inside

ex

ip access-list extended NAT

permit ip [адрес сети, которй нужно обеспечить доступ в интернет] [обратная маска сети] any

ip nat inside source list NAT interface eth 0/1/0

}

telnet{

en

conf t

hostname R1

en

enable secret qwerty

username admin privilege 15 secret cisco

line vty 0 4

login local

tr i t

exit

int fa 0/0

ip add 192.168.0.254 255.255.255.0

ex

}

Tunel{

Int tun 1

ip address 172.16.0.1 255.255.255.252

tunnel source [имя порта доступа в интернет]

tunnel destination [ip адрес порта назначения]

exit

ip route [сеть которую надо передавать] [маска сети которую надо передавать] [ip тунеля на другом роутере]

}

Port-security{

En

Conf t

Int fa 0/1

Sw m a

sw port-s mac st

sw port-sec

sw port-security violation shutdown

}

Ospf{

En

Conf t

Router ospf 1

Passive-interface default

No passive-interface

Fa 0/0

No passive-interface

Network [ip сети которой нужно поделиться] [обратная маска сети] area 1

(network вводить на тех роутерах, у которых есть доступ к указанной сети)

}

Spaning tree{

enable

configure terminal

spanning-tree vlan 1 priority 4096

(Настраивается для каждого vlan отдельно, чем ниже значение тем больший приоритет у устройства)

}

VTP{

vtp domain HOME

vtp password HOME

vtp mode server(раздает)/client(принимает)/ transparent(передаёт)

vtp version 2

}

CDP {

En

Conf t

Cdp run

Int ran fa 0/0-1

Cdp en

No sh

Exit

Do show cdp neighbors

}

NTP {

En

Conf t

ntp authenticate

ntp authentication-key 1 md5 cisco

ntp trusted-key 1

ntp server 117.25.2.100 key 1

ntp update-calendar

}

1. [ДАННЫЕ УДАЛЕНЫ]

2. Программные средства ЛВС включают в себя: 1. Протоколы управления сетью (SNMP, SSH, Telnet) - позволяют удаленно управлять сетью и настраивать устройства. 2. Протоколы маршрутизации (OSPF, RIP, BGP) - используются для выбора оптимального маршрута передачи данных в сети. 3.Программное обеспечение для мониторинга сети (Nagios, PRTG) - позволяют получать информацию о состоянии сети, анализировать трафик, идентифицировать проблемы и предотвращать их возникновение. 4. Программы для конфигурирования устройств (Cisco Configuration Professional, HP Network Configuration Utility) - упрощают процесс настройки оборудования в сети.

Аппаратные средства ЛВС включают в себя: 1. Коммутаторы - устройства, обеспечивающие коммутацию сетевых пакетов внутри сети. 2. Маршрутизаторы - устройства, обеспечивающие передачу данных между различными сетями. 3. Концентраторы - аппаратура, позволяющая объединять несколько устройств в одну сегментированную сеть. 4. Мосты - используются для соединения двух сегментов сети. 5. Кабели и разъёмы - используются для соединения устройств в сети.

3. В компьютерных сетях компьютеры могут совместно использовать такие ресурсы, как диски, принтеры, сканеры, а также обмениваться данными и использовать вычислительную мощность друг друга. Для связи между устройствами нужны интерфейсы, которые делятся на физические и логические. Физические определяются контактами разъема и электрическими связями, логические — форматом информационных сообщений и правилами их обмена. Интерфейсы компьютеров сети реализуются через сетевой адаптер и драйвер устройства, а интерфейсы компьютера и периферийного устройства — через интерфейсную карту компьютера и контроллер устройства.

4. Высокая скорость передачи данных. Современные вычислительные сети должны обеспечивать высокую скорость передачи данных, чтобы поддерживать быстрое выполнение операций.

Высокая степень надежности. Важно, чтобы современные сети были надежными и имели возможность обнаруживать и исправлять ошибки передачи данных.

Безопасность. Современные сети должны быть защищены от несанкционированного доступа, хакерских атак и вирусов.

Масштабируемость. Вычислительные сети должны быть масштабируемыми, чтобы обеспечивать устойчивую работу вне зависимости от количества узлов и пользователей.

Гибкость. Современные сети должны быть гибкими и иметь возможность легко адаптироваться к различным потребностям бизнеса.

Высокая производительность. Современные вычислительные сети должны обладать высокой производительностью, чтобы эффективно обрабатывать большие объемы данных.

Простота управления. Следует обеспечить легкое управление вычислительными сетями, чтобы администраторам было легко настраивать и управлять ими.

5. Структура OSI (Open Systems Interconnection) состоит из 7 уровней, которые отвечают за различные аспекты передачи данных в компьютерных сетях:

Физический уровень (Physical layer) — электрические, оптические и другие физические параметры передачи данных.

Канальный уровень (Data link layer) — организация доступа к среде передачи данных, контроль ошибок на физическом уровне.

Сетевой уровень (Network layer) — передача данных между сетями, обеспечение маршрутизации и управление трафиком.

Транспортный уровень (Transport layer) — обеспечение надежной и управляемой передачи данных между приложениями, контроль целостности и управление потоком данных.

Сеансовый уровень (Session layer) — установление, поддержание и завершение сеанса соединения между приложениями.

Уровень представления данных (Presentation layer) — конвертация, кодирование и декодирование данных в форматы, пригодные для интерпретации приложениями.

Прикладной уровень (Application layer) — поддержка приложений, включая управление файлами, электронной почты, веб-серверы и прочее.

Каждый уровень имеет свою функцию и уникальный набор протоколов для обеспечения передачи данных. Все уровни совместно работают для обеспечения надежной и эффективной передачи данных в компьютерных сетях.

6. Сетевой уровень модели OSI является третьим по счету уровнем эталонной модели сетевого взаимодействия. На третьем уровне модели OSI происходит формирование маршрутов и путей передачи данных между устройствами, находящимися в сети. Естественно, маршрут определяется оптимально и при этом учитывается дальность маршрута и нагрузка на узлы сети.

Также на третьем уровне эталонной модели происходит преобразование логических сетевых адресов в физические и наоборот, этот процесс получил название – трансляция. Роутеры, установленные в ваших квартирах – это хороший пример устройств сетевого уровня модели OSI. Самым популярным протоколом третьего уровня модели OSI является протокол IP, на данный момент поддерживается две версии протокола IP: IPv4 и IPv6.

7. Краткая характеристика уровней модели OSI:

Физический уровень (Physical layer) определяет способ физического соединения компьютеров в сети. Функциями средств, относящихся к данному уровню, являются побитовое преобразование цифровых данных в сигналы, передаваемые по физической среде (например, по кабелю), а также собственно передача сигналов.

Канальный уровень(Data Link layer) отвечает за организацию передачи данных между абонентами через физический уровень, поэтому на данном уровне предусмотрены средства адресации, позволяющие однозначно идентифицировать отправителя и получателя во всем множестве абонентов, подключенных к обще линии связи. В функции данного уровня также входит упорядочивание передачи с целью параллельного использования одной линии связи несколькими парами абонентов. Кроме того, средства канального уровня обеспечивают проверку ошибок, которые могут возникать при передаче данных физическим уровнем.

Сетевой уровень(Network layer) обеспечивает доставку данных между компьютерами сети, представляющей собой объединение различных физических сетей. Данный уровень предполагает наличие средств логической адресации, позволяющих однозначно идентифицировать компьютер в объединенной сети. Одной из главных функций, выполняемых средствами данного уровня, является целенаправленная передача данных конкретному получателю.

Транспортный уровень(Transport layer) реализует передачу данных между двумя программами, функционирующими на разных компьютерах, обеспечивая при этом отсутствие потерь и дублирования информации, которые могут возникать в результате ошибок передачи нижних уровней. В случае, если данные, передаваемые через транспортный уровень, подвергаются фрагментации, то средства данного уровня гарантируют сборку фрагментов в правильном порядке.

Сессионный (или сеансовый) уровень (Session layer) позволяет двум программам поддерживать продолжительное взаимодействие по сети, называемое сессией (session) или сеансом. Этот уровень управляет установлением сеанса, обменом информацией и завершением сеанса. Он также отвечает за идентификацию, позволяя тем самым только определенным абонентам принимать участие в сеансе, и обеспечивает работу служб безопасности с целью упорядочивания доступа к информации сессии.

Уровень представления(Presentation layer) осуществляет промежуточное преобразование данных исходящего сообщения в общий формат, который предусмотрен средствами нижних уровней, а также обратное преобразование входящих данных из общего формата в формат, понятный получающей программе.

Прикладной уровень (Application layer) предоставляет высокоуровневые функции сетевого взаимодействия, такие, как передача файлов, отправка сообщений по электронной почте и т.п.

Транспортный уровень (transport layer) обеспечивает приложениям или верхним уровням стека — прикладному, представления и сеансовому — передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов транспортного сервиса от низшего класса 0 до высшего класса 4. Эти виды сервиса отличаются качеством предоставляемых услуг; срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное — способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети — компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/ IP.

Транспортный уровень реализует туннельную связь между двумя конечными узлами, то есть он отвечает за надежную передачу данных между удаленными узлами поверх ненадёжной сети, в котором в любой момент времени может случиться всё что угодно, также транспортный уровень позволяет компьютеру разделять трафик различных приложений, а еще он выполняет фрагментацию, то есть разбивает данные, получаемые с верхнего уровня на мелкие фрагменты.

8. Канальный уровень (Data Link Layer, DLL) помогает понять, как отправлять данные с одного узла на другой через физический уровень (уровень 1). Например, первый уровень работает с битами и символами, а второй уровень обрабатывает кадры (контейнеры для сетевых пакетов).

Поскольку канальный уровень построен поверх физического уровня, он должен гарантировать, что данные, отправленные с одного узла, действительно достигают другого узла без ошибок. Поскольку второй уровень обрабатывает все: от передачи до контроля ошибок, ему нужны дополнительные усилия в виде двух подуровней: LLC (управление логическим каналом) и MAC (управление доступом к среде). Давайте подробнее рассмотрим каждый из них.

На канальном уровне происходит управление доступом к среде передачи данных и обработка ошибок, связанных с передачей данных по сети. Для этого канальный уровень использует различные методы контроля доступа, такие как CSMA/CD, который позволяет управлять коллизиями (столкновениями) при передаче данных.

Также на канальном уровне происходит служебная обработка, которая включает контрольные суммы и другую информацию, необходимую для обнаружения и исправления ошибок при передаче данных. Канальный уровень работает с физическим уровнем (на котором происходит фактическая передача данных), а также с более высокими уровнями модели OSI, такими как сетевой уровень и уровень приложений.

Таким образом, канальный уровень в компьютерных сетях является важной частью модели OSI и отвечает за обеспечение надежной и безопасной передачи данных по сети.

9. Представительский уровень участвует в трансформации данных в универсальный распознаваемый формат без изменения содержания. Так как в разных устройствах утилизируются различные форматы, информация, обработанная на представительском уровне, даёт возможность системам понимать друг друга, преодолевая синтаксические и кодовые различия. Кроме того, на шестом этапе появляется возможность шифровки и дешифровки данных, что обеспечивает секретность.

Принцип работы представительского уровня заключается в преобразовании данных из формата, понятного для приложения пользователя, в формат, принятый для передачи по сети, и наоборот. Это может включать в себя кодирование и декодирование данных, сжатие и расшифровку информации и преобразование форматов данных таких как ASCII, UTF-8, JPEG, MPEG и других.

Таким образом, представительский уровень играет важную роль в обеспечении совместимости различных устройств и программных средств, делая обмен данными между ними возможным и эффективным. Он также задумывался как промежуточный уровень, разделяющий физический и логический уровни модели OSI.

10. 1.«Шина» (Bus). В этой топологии все компьютеры соединяются друг с другом одним кабелем. Посланные в такую сеть данные передаются всем компьютерам, но обрабатывает их только тот компьютер, аппаратный МАС-адрес сетевого адаптера которого записан в кадре как адрес получателя. Эта топология исключительно проста в реализации и дешева (требует меньше всего кабеля), однако имеет ряд существенных недостатков: 1. Такие сети трудно расширять (увеличивать число компьютеров в сети и количество сегментов — отдельных отрезков кабеля, их соединяющих). 2. Поскольку шина используется совместно, в каждый момент времени передачу может вести только один из компьютеров. 3. «Шина» является пассивной топологией — компьютеры только «слушают» кабель и не могут восстанавливать затухающие при передаче по сети сигналы. Чтобы удлинить сеть, нужно использовать повторители (репитеры), усиливающие сигнал перед его передачей в следующий сегмент. 4. Надежность сети с топологией «шина» невысока. Если кабель соединяющий компьютеры рвется в одном месте, то вся система перестает работать.

2. «Кольцо» (Ring). В данной топологии каждый из компьютеров соединяется с двумя другими так, чтобы от одного он получал информацию, а второму — передавал ее (Рис. 5.9). Последний компьютер подключается к первому, и кольцо замыкается. Преимущества сетей с топологией «кольцо»: 1. Каждый из компьютеров выступает в роли повторителя, усиливая сигнал, что позволяет строить сети большой протяженности; 2. Из-за отсутствия столкновений топология обладает высокой устойчивостью к перегрузкам, обеспечивая эффективную работу с большими потоками передаваемой по сети информации

Недостатки:1. Сигнал в «кольце» должен пройти последовательно (и только в одном направлении) через все компьютеры, каждый из которых проверяет, не ему ли адресована информация, поэтому время передачи может быть достаточно большим; 2. Подключение к сети нового компьютера часто требует ее остановки, что нарушает работу всех других компьютеров; 3. Выход из строя хотя бы одного из компьютеров или устройств нарушает работу всей сети; 4. Обрыв или короткое замыкание в любом из кабелей кольца делает работу всей сети невозможной;

3. Активная топология «звезда» (Active Star). В такой конфигурации все потоки данных шли исключительно через центральный компьютер; он же полностью отвечал за управление информационным обменом между всеми участниками сети. Конфликты при такой организации взаимодействия в сети были невозможны, однако нагрузка на центральный компьютер была столь велика, что ничем другим, кроме обслуживания сети, этот компьютер, как правило, не занимался. Выход его из строя приводил к отказу всей сети, тогда как отказ периферийного компьютера или обрыв связи с ним на работе остальной сети не сказывался.

4. Полносвязная топология - топология сети при которой каждый компьютер связан с каждым компьютером сети. Эта топология требует большого количества проводов, но отказ каждого отдельного компьютера не влияет на работоспособность остальной сети.

5. Гибридная топология – топология в которой применяются две и более топологий.

11. Доступ к среде передачи – это совокупность правил, по которым осуществляется управление разрешением на передачу информации для сетевых устройств. Есть несколько типов доступа к среде передачи: 1. Множественный доступ с контролем несущей/обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) – метод доступа к среде передачи, при котором все компьютеры в сети прослушивают кабель перед передачей данных и при обнаружении коллизии инициализируют повторную передачу пакета (через случайный промежуток времени).

2. Множественный доступ с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) - метод доступа к среде передачи, при котором используется либо доступ с квантованием времени, при котором каждый компьютер может передавать информацию только в строго определенные для него моменты времени, либо отправление запроса в сеть на получение доступа к среде.

3. Передача маркера (Token passing) - метод доступа к среде передачи, при котором право передавать данные может сетевое устройство, владеющее маркером.

12. Архитектура сети - это структура, в рамках которой организуется связь между различными компонентами сети, включая устройства, протоколы и службы. Архитектура сети определяет размещение и конфигурацию сетевых компонентов, а также принципы обмена данными в сети.

Существует несколько видов архитектур сетей, включая:

Централизованная архитектура - все устройства правятся центральным сервером, который обрабатывает и управляет всей информацией. Обычно используется для небольших и средних сетей.

Распределенная архитектура - каждое устройство ведет набор данных и работает с другими устройствами для обмена информацией. Обычно используется в больших сетях, где централизованное управление может оказаться неэффективным.

Архитектура клиент-сервер - распределенная архитектура, где клиенты запрашивают данные у сервера, который обрабатывает запросы и отправляет назад результаты.

Peer-to-Peer (P2P) - распределенная архитектура, где компьютеры связываются друг с другом напрямую, без участия центрального сервера. Используется в среде обмена большими файлами и получений информации.

Архитектура сети также может быть сконструирована по типу соединений, топологии сети или протоколов связи.

В архитектуре сети устройства связи играют ключевую роль, так как они позволяют обмениваться данными между сетевыми устройствами. Некоторые из основных устройств связи, используемых в сетях, включают:

1. Коммутаторы (switches) - устройства, которые обеспечивают коммутацию пакетов данных внутри локальной сети (LAN). Они позволяют устройствам подключаться и обмениваться данными напрямую друг с другом.

2. Маршрутизаторы (routers) - устройства, которые определяют наилучший маршрут для пересылки пакетов данных из одной сети в другую. Они также могут обеспечивать трансляцию IP-адресов между различными сетевыми интерфейсами.

3. Модемы (modems) - устройства, которые позволяют подключать компьютеры к Интернету посредством телефонной линии, кабельного телевидения или другого типа канала связи.

4. Шлюзы (gateways) - устройства, которые обеспечивают преобразование данных между двумя различными сетевыми протоколами или форматами данных.

5. Концентраторы (hubs) - устройства, которые позволяют объединить несколько устройств в одну локальную сеть.

6. Активные оптические сетевые устройства (Active Optical Networking Devices) - устройства, которые обеспечивают передачу данных по оптоволоконному кабелю.

7. Беспроводные точки доступа (Wireless Access Points) - устройства, которые обеспечивают беспроводное подключение к сети.

Каждый из этих видов устройств связи вносит свой вклад в общую архитектуру сети и позволяет обеспечить высокую скорость передачи данных и надежную связь между устройствами.

13. Стек протоколов – Это иерархически организованная совокупность протоколов, достаточная для реализации взаимодействия узлов в компьютерной сети. Существующие стеки протоколов: TCP/IP, IPX/SPX, SNA и другие.

Адресация – процесс, при котором микропроцессор обращается к определенному сегменту памяти или внешнему устройству, используя определенные адреса. Каждый пакет, проходящий по сети содержит адрес получателя, и идет согласно определенным правилам маршрутизации.

Маршрутизация - это процесс направления пакета по лабиринту сетей, находящихся между источником и адресатом. Важнейшую задачу выбора наилучшего пути следования пакета данных решают маршрутизаторы на основе таблиц маршрутизации. В таблицы маршрутизации входит информация о номерах и масках подсетей назначения, адресах шлюзов и собственных портов маршрутизатора, а также о метриках. Для адресов, отсутствующих в таблице, применяется специальный адрес − адрес шлюза по умолчанию.

Самым распространенным «семейством» протоколов, на котором построен интернет является ТСР/IP − это ряд протоколов под общим названием TCP/IP (по названиям двух основных протоколов: TCP и IP).

Каждый компьютер в сетях ТСР/IP имеет адреса трех уровней: физический (МАС-адрес), сетевой (IP−адрес) и символьный (DNS− имя).

14. Среда передачи данных - это физическая среда, по которой происходит передача данных между двумя устройствами. Существуют различные среды передачи данных, такие как проводная, оптическая, радиоволновая.

Пропускная способность - это мера скорости передачи данных через среду передачи. Она выражается в битах в секунду (bps) или килобитах в секунду (kbps), мегабитах в секунду (Mbps) или гигабитах в секунду (Gbps). Чем выше пропускная способность, тем быстрее можно передавать данные.

Производительность - это мера эффективности среды передачи данных. Она выражается в количестве передаваемых данных в единицу времени и зависит от пропускной способности и других характеристик среды передачи, таких как задержки и ошибки передачи данных. Высокая производительность гарантирует быструю и надежную передачу данных.

15. Скрученная пара проводов называется витой парой (twisted pair). Витая пара существует в экранированном варианте (Shielded Twistedpair, STP), когда пара медных проводов обертывается в изоляционный экран, и неэкранированном (Unshielded Twistedpair, UTP), когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю. Коаксиальный кабель (coaxial) имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения – для локальных сетей, для глобальных сетей, для кабельного телевидения и т. п.

16. Структурированная кабельная система (Structured Cabling System, SCS) — это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

При построении структурированной кабельной системы подразумевается, что каждое рабочее место на предприятии должно быть оснащено розетками для подключения телефона и компьютера, даже если в данный момент этого не требуется, поскольку последующие изменения в сети производятся за счет перекоммутации уже проложенных кабелей.

17. Типичная иерархия структурированной кабельной системы включает: 1. горизонтальные подсистемы (в пределах этажа); 2. Вертикальные подсистемы (внутри здания); 3. Подсистему кампуса (в пределах одной территории с несколькими зданиями).

Горизонтальная подсистема соединяет кроссовый шкаф этажа с розетками пользователей. Подсистемы этого типа соответствуют этажам здания. Вертикальная подсистема соединяет кроссовые шкафы каждого этажа с центральной аппаратной здания. Следующим шагом иерархии является подсистема кампуса, которая соединяет несколько зданий с главной аппаратной всего кампуса. Эта часть кабельной системы называется магистралью (backbone).

18. Использование структурированной кабельной системы дает много преимуществ: 1. Универсальность. Структурированная кабельная система может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. 2. Увеличение срока службы. Срок морального старения хорошо структурированной кабельной системы может составлять 10-15 лет. 3. Уменьшение стоимости добавления новых пользователей и изменения их мест размещения. Известно, что стоимость кабельной системы значительна и определяется в основном стоимостью работ по ее монтажу. Поэтому более выгодно провести однократную работу по прокладке кабеля, возможно, с большим запасом по длине, чем несколько раз выполнять прокладку, наращивания длину кабеля. 4. Возможность легкого расширения сети. Структурированная кабельная система является модульной, поэтому ее легко расширять. Она является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты. 5. Обеспечение более эффективного обслуживания. 6. Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой, поскольку отказ одного из устройств или соединительных элементов приводит к трудно локализуемому отказу всей сети. Концентраторы диагностируют и локализуют неисправный участок. 7. Надежность.

19.(Неточная информация) Для подключения к сети интернет необходимо иметь соответствующее оборудование, такое как модемы, роутеры и прочее, также необходимо провести настройку настройку сетевых протоколов и служб, таких как DHCP, DNS и других.

Также необходимо подумать о безопасности сети. Нужно настроить межсетевой экран (firewall) для защиты сети от внешних угроз, таких как вирусы, хакеры и другие злоумышленники.

Также нужно провести настройку сетевых служб, таких как электронная почта, файловые серверы, базы данных и другие. Это должно обеспечить надежность и доступность этих служб для пользователей.

20. Конфигурирование коммутаторов - это процесс настройки коммутатора для оптимальной работы в сети. Это включает в себя задание IP-адреса, настройку VLAN, настройку портов и т.д.

Вот несколько шагов, которые нужно выполнить при конфигурировании коммутатора:

1. Назначение IP-адреса: Для управления коммутатором через сеть, нужно назначить ему IP-адрес.

2. Настройка VLAN: Каждый порт коммутатора может быть настроен на определенную VLAN. Это позволяет разделять трафик на разные группы, что повышает безопасность и эффективность сети.

3. Настройка портов: Каждый порт коммутатора может быть настроен на определенный режим работы, например, access или trunk. Access-порты используются для подключения устройств к VLAN, а trunk-порты используются для передачи трафика между коммутаторами.

4. Настройка протоколов.

21. Передача данных - это обмен данными между двумя узлами по какой-либо форме канала (средства передачи), такого как кабель. Теперь обмен этими данными осуществляется тремя способами: 1. Однонаправленный: связь всегда однонаправленная, т. е. одно устройство будет передавать, а другое - принимать. Например, клавиатура, традиционные мониторы и т.д. 2. Полудуплексный: Связь осуществляется в обоих направлениях, но не одновременно, т.е. если одно устройство отправляет, другое будет получать, и наоборот. Например, портативные рации. 3. Полный дуплекс: Связь осуществляется в обоих направлениях одновременно, т.е. устройство может отправлять и получать данные одновременно. Например, телефонная линия.

Сетевые протоколы - это наборы установленных правил, которые определяют, как форматировать, передавать и получать данные, чтобы сетевые устройства компьютера — от серверов и маршрутизаторов до конечных точек – могли взаимодействовать независимо от различий в их базовой инфраструктуре, дизайне или стандартах.

Нам нужны сетевые протоколы для: 1. Кодирование сообщений 2. Форматирование и инкапсуляция сообщений 3. Синхронизация сообщений 4. Размер сообщения 5. Варианты доставки сообщений

Типы компьютерных сетей :1. Клиент-сервер - это распределенная структура приложения, которая распределяет задачи или рабочие нагрузки между поставщиками ресурса или услуги, называемыми серверами, и лицами, запрашивающими услуги, называемыми клиентами. Часто клиенты и серверы взаимодействуют по компьютерной сети на отдельном оборудовании, но и клиент, и сервер могут находиться в одной системе. 2. Одноранговая сеть (P2P).

Одной из наиболее распространенных является модель OSI (Open Systems Interconnection), которая состоит из семи уровней:

1. Физический уровень - определяет физические характеристики среды передачи данных, такие как кабель, разъемы, сигналы и т.д.

2. Канальный уровень - обеспечивает надежную передачу данных между устройствами в сети, используя методы контроля ошибок и управления потоком данных.

3. Сетевой уровень - отвечает за определение маршрута передачи данных между устройствами в разных сетях.

4. Транспортный уровень - обеспечивает надежную передачу данных между приложениями, используя протоколы, такие как TCP и UDP.

5. Сеансовый уровень - устанавливает и управляет соединением между приложениями на разных устройствах.

6. Уровень представления - обеспечивает преобразование данных из формата, используемого приложениями, в формат, который может быть передан по сети.

7. Прикладной уровень - предоставляет интерфейс для приложений, позволяя им обмениваться данными между собой.

22. Концептуально, архитектура протоколов TCP/IP состоит из четырех уровней, каждый из которых выполняет определенные функции в процессе передачи данных. Вот краткое описание каждого уровня:

1. Сетевой интерфейс (Network Interface Layer) - этот уровень отвечает за передачу данных по физической сети, такой как Ethernet или Wi-Fi. Он управляет адресацией устройств, физическими характеристиками передачи данных и обнаружением ошибок.

2. Интернет-слоя (Internet Layer) - этот уровень отвечает за маршрутизацию пакетов данных через сеть. Он использует протокол IP (Internet Protocol), который определяет адресацию устройств и способ передачи данных между ними.

3. Транспортный слой (Transport Layer) - этот уровень отвечает за управление передачей данных между приложениями на разных устройствах. Он использует протоколы TCP (Transmission Control Protocol) и UDP (User Datagram Protocol), которые обеспечивают надежную или не надежную передачу данных соответственно.

4. Прикладной слой (Application Layer) - этот уровень отвечает за передачу данных между конечными приложениями на разных устройствах. Он использует различные протоколы, такие как HTTP (Hypertext Transfer Protocol) для передачи веб-страниц, FTP (File Transfer Protocol) для передачи файлов, SMTP (Simple Mail Transfer Protocol) для передачи электронной почты и т.д.

Каждый уровень архитектуры TCP/IP выполняет свою функцию в процессе передачи данных, обеспечивая надежность, эффективность и безопасность передачи данных в компьютерных сетях.

Уровень доступа – это базовая часть сети.

К уровню доступа непосредственно физически присоединяются сами пользователи.

Именно отсюда люди подключаются к другим узлам и используют общий доступ к файлам и принтерам. Уровень доступа состоит из узлов и первого уровня сетевых устройств, к которым они подключаются.

23. Протокол TCP/IP - это набор стандартов, используемых для передачи данных в компьютерных сетях. Он состоит из двух основных протоколов: протокола интернет-протокола (IP) и протокола управления передачей (TCP).

IP-адрес - это уникальный идентификатор, который присваивается каждому устройству в сети, чтобы оно могло обмениваться данными с другими устройствами. IP-адрес состоит из четырех чисел, разделенных точками, например, 192.168.0.1.

Маска подсети - это дополнительный параметр, который используется для разделения сети на подсети. Она определяет, какая часть IP-адреса относится к сети, а какая к устройству. Маска подсети также представляется в виде четырех чисел, разделенных точками, например, 255.255.255.0.

Основной шлюз - это устройство, которое используется для связи между разными сетями. Когда устройство отправляет данные в другую сеть, оно отправляет их через основной шлюз.

Деление на подсети с помощью маски подсети - для разделения сети на подсети, маска подсети используется для определения, какая часть IP-адреса относится к сети, а какая к устройству. Например, если маска подсети равна 255.255.255.0, то первые три числа IP-адреса относятся к сети, а последнее число - к устройству. Это означает, что в этой сети может быть до 254 устройств.

IP-маршрутизация - это процесс отправки данных через сеть от одного устройства к другому. Когда устройство отправляет данные в другую сеть, оно отправляет их через основной шлюз. Основной шлюз получает данные и отправляет их дальше по сети, пока они не достигнут нужного устройства. Этот процесс называется IP-маршрутизацией.

24. Адресация в стеке протоколов TCP/IP осуществляется на разных уровнях протоколов, начиная от физического уровня и заканчивая прикладным уровнем.

На физическом уровне адресация осуществляется с помощью MAC-адресов, которые уникальны для каждого сетевого интерфейса устройства.

На сетевом уровне адресация происходит с помощью IP-адресов, которые являются уникальными для каждого устройства в сети. IP-адреса состоят из 4 чисел, разделенных точками, каждое из которых может принимать значения от 0 до 255.

На транспортном уровне адресация осуществляется с помощью портов. Каждое приложение, использующее протокол TCP или UDP, имеет свой уникальный номер порта, который используется для идентификации приложения на устройстве.

На прикладном уровне адресация осуществляется с помощью URI-адресов, которые используются для идентификации ресурсов в сети. URI-адреса могут содержать информацию о протоколе, IP-адресе и номере порта.

В целом, адресация в стеке протоколов TCP/IP является многоуровневой и служит для идентификации устройств и приложений в сети, а также для передачи данных между ними.

25. Стек протоколов TCP/IP включает в себя несколько типов адресов, которые используются для идентификации устройств и приложений в сети:

1. Физический адрес (MAC-адрес) - это уникальный идентификатор сетевого интерфейса устройства в локальной сети. MAC-адрес состоит из 6 байтов и обычно записывается в виде шестнадцатеричного числа, разделенного двоеточием. Физический адрес используется на низшем уровне стека протоколов TCP/IP для передачи данных между устройствами в локальной сети.

2. IP-адрес - это уникальный идентификатор устройства в сети. IP-адрес состоит из 4 байтов и записывается в виде четырех чисел, разделенных точками. IP-адрес используется на уровне сетевого протокола для маршрутизации пакетов данных между устройствами в сети.

3. Порт - это идентификатор приложения, которое обменивается данными между устройствами в сети. Порт представляет собой 16-битное число и может принимать значения от 0 до 65535. Порты используются на уровне транспортного протокола для идентификации приложений, которые обмениваются данными.

4. URL-адрес - это адрес веб-страницы или другого ресурса в интернете. URL-адрес состоит из нескольких частей, включая протокол (например, HTTP или HTTPS), доменное имя и путь к ресурсу. URL-адрес используется на уровне прикладного протокола для доступа к ресурсам в интернете.

Все эти типы адресов в стеке протоколов TCP/IP используются для идентификации устройств и приложений в сети и обеспечения передачи данных между ними.

26. Виртуальная локальная сеть (Virtual Local Area Network, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети обладают всеми свойствами физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т.к. любой порт коммутатора можно настроить на принадлежность виртуальной локальной сетью (Virtual LAN, VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов определенной VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть, т.е. пакеты, для данной VLAN будут коммутироваться коммутатором только в пределах этой VLAN. Для того, чтобы трафик одной VLAN попадал в другую, применяются сетевые устройства 3-го уровня OSI, а именно маршрутизаторы.

27. Маршрутизаторы - это устройства, которые используются для соединения нескольких сетей и передачи данных между ними. Они работают на сетевом уровне модели OSI и выполняют функции маршрутизации, которые позволяют передавать данные от отправителя к получателю в сети.

Маршрутизаторы используют таблицы маршрутизации для определения оптимального пути передачи данных между сетями. Они также могут выполнять функции фильтрации и перевода адресов (NAT), что позволяет использовать один внешний IP-адрес для нескольких устройств в локальной сети.

Маршрутизаторы имеют как локальные, так и глобальные интерфейсы. Локальные интерфейсы соединяют маршрутизатор с устройствами в локальной сети, а глобальные интерфейсы соединяют маршрутизатор с другими сетями.

Одним из наиболее распространенных протоколов маршрутизации является протокол маршрутизации интернета (IP-маршрутизация). Он используется для передачи данных между сетями, используя IP-адреса.

В современных корпоративных сетях маршрутизаторы часто используются в связке с другими устройствами, такими как коммутаторы и файрволы, для обеспечения безопасности и эффективности передачи данных.

28. Важнейшей задачей сетевого уровня является маршрутизация — передача пакетов между двумя конечными узлами в составной сети.

Цель маршрутизации - доставка пакетов по назначению с максимизацией эффективности. Чаще всего эффективность выражена взвешенной суммой времен доставки сообщений при ограничении снизу на вероятность доставки. Маршрутизация сводится к определению направлений движения пакетов в маршрутизаторах. Выбор одного из возможных в маршрутизаторе направлений зависит от текущей топологии сети (она может меняться хотя бы из-за временного выхода некоторых узлов из строя), длин очередей в узлах коммутации, интенсивности входных потоков и т.п.

Алгоритмы маршрутизации включают процедуры:

- измерение и оценивание параметров сети;

- принятие решения о рассылке служебной информации;

- расчет таблиц маршрутизации (ТМ);

- реализация принятых маршрутных решений.

В зависимости от того, используется ли при выборе направления информация о состоянии только данного узла или всей сети, различают алгоритмы изолированные и глобальные. Если ТМ реагируют на изменения состояния сети, то алгоритм адаптивный(динамический), иначе фиксированный (статический), а при редких корректировках - квазистатический. В статических маршрутизаторах изменения в ТМ вносит администратор сети, а в динамических маршрутизатор сам составляет таблицу маршрутизации.

29. Маршрутизация между VLAN — это процесс маршрутизации трафика между сетями VLAN с использованием выделенного маршрутизатора или многоуровневого коммутатора. Маршрутизация между VLAN упрощает обмен данными между устройствами, изолированными границами VLAN.

Устаревший метод маршрутизации между VLAN обусловлен доступностью физического порта коммутатора для каждой настроенной VLAN. Данный метод был заменён на топологию router-on-a-stick, которая полагается на внешний маршрутизатор с подынтерфейсами, подключёнными через транковые каналы к коммутатору 2-го уровня. При использовании метода router-on-a-stick на каждом логическом подынтерфейсе необходимо настроить соответствующие IP-адреса и параметры VLAN. Необходимо настроить транк и инкапсуляцию на маршрутизаторе и на соответствующем порту коммутатора.

Другой способ реализации маршрутизации между VLAN — многоуровневая маршрутизация с использованием коммутации 3-го уровня. Коммутация 3-го уровня использует интерфейсы SVI и маршрутизируемые порты. Коммутация 3-го уровня обычно настраивается на уровне распределения и ядра. Коммутация 3-го уровня с интерфейсами SVI — это форма маршрутизации между VLAN. Маршрутизируемый порт является физическим портом, работающим аналогично интерфейсу маршрутизатора. В отличие от порта доступа маршрутизируемый порт не связан с определённой VLAN.

30. Статическая маршрутизация — вид маршрутизации, при котором маршруты вручную указываются администратором при настройке маршрутизатора. К преимуществам статической маршрутизации можно отнести: •простоту настройки (в небольших сетях); •отсутствие дополнительной нагрузки на сеть (в отличии от динамических протоколов маршрутизации). К недостаткам относится: •сложность маршрутизации; •при возникновении каких-либо изменений в сети, как правило, потребуется вмешательство администратора и настройка новых, актуальных статических маршрутов

31. Маска подсети переменной длины (VLSM) - это метод, используемый при проектировании IP-сетей для создания подсетей с различными масками подсети. VLSM позволяет сетевым администраторам более эффективно распределять IP-адреса, используя меньшие маски подсети для подсетей с меньшим количеством хостов и большие маски подсети для подсетей с большим количеством хостов.

VLSM позволяет сетевым администраторам создавать подсети с различными масками подсети для более эффективного использования IP-адресов. Используя приведенный выше пример, VLSM можно было бы использовать для назначения маски подсети 255.255.255.128 меньшей подсети с 10 хостами, которая предоставляла бы 126 доступных IP-адресов, и маски подсети 255.255.255.192 большей подсети с 50 хостами, которая предоставляла бы 62 доступных IP-адреса.

VLSM широко используется в современных сетях для создания подсетей разного размера и оптимизации использования IP-адресов.

32. Протоколы динамической маршрутизации (Dynamic Routing Protocols) – это программные алгоритмы, которые позволяют автоматически определять оптимальные маршруты передачи данных между устройствами в компьютерных сетях.

Их основное назначение – это обеспечение автоматической настройки маршрутизаторов в сети, что позволяет упростить управление сетью и повысить ее надежность.

Принцип работы протоколов динамической маршрутизации заключается в том, что каждый маршрутизатор в сети передает информацию о своих соседях и маршрутах, которые он знает, другим маршрутизаторам в сети. Эта информация передается в форме сообщений, называемых обновлениями маршрутов (route updates).

Каждый маршрутизатор использует эти обновления, чтобы создать таблицу маршрутизации, которая содержит информацию о наилучшем пути для достижения каждого узла в сети. Эта таблица обновляется автоматически, когда в сети происходят изменения в топологии (структуре) сети.

История развития протоколов динамической маршрутизации началась в 1969 году, когда был разработан первый протокол – Routing Information Protocol (RIP). Он был предназначен для использования в сетях ARPANET (Advanced Research Projects Agency Network) и был основан на принципе распространения информации о маршрутах с помощью обновлений маршрутов.

В последующие годы было разработано множество других протоколов динамической маршрутизации, таких как Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS) и др. Каждый из них имел свои преимущества и недостатки и был предназначен для использования в различных типах сетей.

Сравнивая преимущества и недостатки подходов, в действительности говорить о том, что лучше, а что хуже было бы не совсем корректно, поскольку, по сути, эти виды маршрутизации используются для разных целей.

Например, настроить постоянный удаленный доступ к ПК или серверу возможно только через статическую маршрутизацию. Аналогично и с другими системами: 1. Камеры видеонаблюдения; 2. Файловый сервер; 3. Почтовый сервер; 4. бекап-сервер; 5. архив 1С и другие

Главный плюс динамической маршрутизации — и ее же существенный недостаток —в однократном использовании присваиваемых устройствам при каждом новом подключении IP-адресов.

При статической маршрутизации адреса всегда будут сохраняться в неизменном виде. Такой принцип важен для закрытых локальных сетей, где обращение к серверам и системам хранения данных всегда происходит по одному адресу. Он важен во всемирной паутине, где каждому онлайн-ресурсу присвоен свой IP-адрес, который также должен оставаться неизменным.

Если подключения временные, с ограниченными привилегиями, и происходят в больших количествах, то идеальным решением для такой сети станет динамическая маршрутизация с ее очевидными преимуществами в автоматизации и простом масштабировании.

Если устройства обязаны всегда находиться по определенному адресу, а передача данных требует усложненных протоколов безопасности или, к примеру, подразумевает пересылку больших объёмов данных, то в этом случае стоит настраивать статическую маршрутизацию и никак иначе.

33. Адресация в IP-сетях - это процесс назначения уникального идентификатора каждому устройству в сети, чтобы они могли обмениваться данными. IP-адрес состоит из 32-битного числа, разделенного на 4 октета, каждый из которых может принимать значения от 0 до 255.

Классы IP-адресов - это способ разделения IP-адресов на группы в зависимости от их диапазона значений. Существует 5 классов IP-адресов: A, B, C, D и E. Каждый класс имеет свой диапазон значений первого октета и определяет, сколько бит в адресе зарезервировано для сетевой части и сколько для хостовой части.

Класс A: IP-адреса класса A имеют первый октет в диапазоне от 1 до 126. Первый октет зарезервирован для сетевой части, а оставшиеся три октета используются для хостовой части. Это означает, что в классе A может быть до 126 сетей, каждая из которых может содержать до 16 777 214 устройств.

Класс B: IP-адреса класса B имеют первый октет в диапазоне от 128 до 191. Первые два октета зарезервированы для сетевой части, а оставшиеся два октета используются для хостовой части. Это означает, что в классе B может быть до 16 384 сетей, каждая из которых может содержать до 65 534 устройств.

Класс C: IP-адреса класса C имеют первый октет в диапазоне от 192 до 223. Первые три октета зарезервированы для сетевой части, а последний октет используется для хостовой части. Это означает, что в классе C может быть до 2 097 152 сетей, каждая из которых может содержать до 254 устройств.

Класс D: IP-адреса класса D используются для мультикастинга, когда данные отправляются на группу устройств, а не на одно конкретное. IP-адреса класса D имеют первый октет в диапазоне от 224 до 239.

Класс E: IP-адреса класса E зарезервированы для будущего использования и имеют первый октет в диапазоне от 240 до 255.Особые IP-адреса - это адреса, которые имеют особое значение в сети и не могут быть назначены устройствам. Они используются для различных целей, например, для локальной сети, для маршрутизаторов и т.д. К ним относятся адреса сети и широковещательный адрес.

Использование масок в IP-адресации - это способ определения сетевой и хостовой частей IP-адреса. Маска представляет собой последовательность единиц и нулей, которые определяют, какие биты адреса относятся к сетевой части, а какие к хостовой. Маска записывается в виде 4 чисел, разделенных точками, каждое из которых представляет количество единиц в бинарном виде.

Порядок распределения IP-адресов - это процесс назначения IP-адресов устройствам в сети. IP-адреса могут быть назначены статически или динамически. Статические адреса назначаются вручную и остаются неизменными, пока их не изменят вручную. Динамические адреса назначаются автоматически с помощью протокола DHCP и могут изменяться при каждом подключении устройства к сети.

34. Маршрутизаторы работают на уровне сетевого протокола и могут использоваться для направления трафика между локальными сетями или между локальной сетью и интернетом. Они имеют несколько интерфейсов, которые позволяют им подключаться к различным сетям, и используют различные протоколы маршрутизации для определения наилучшего пути для доставки пакетов данных от отправителя к получателю.

Основная функция маршрутизатора заключается в том, чтобы принимать пакеты данных из одной сети и перенаправлять их в другую сеть, используя таблицы маршрутизации. Таблицы маршрутизации содержат информацию о сетях и маршрутах, которые маршрутизатор может использовать для доставки пакетов данных.

Когда маршрутизатор получает пакет данных, он проверяет его адрес назначения и сравнивает его с таблицей маршрутизации, чтобы определить наилучший путь для доставки пакета. Затем маршрутизатор перенаправляет пакет на соответствующий интерфейс и отправляет его в следующую сеть.

Маршрутизаторы также могут выполнять другие функции, такие как фильтрация трафика, перевод сетевых адресов (NAT), управление пропускной способностью и управление сетевой безопасностью. В целом, маршрутизаторы являются важным компонентом любой сети и обеспечивают эффективную и безопасную передачу данных.

35. Маршрутизирующие протоколы - это программное обеспечение, которое используется на маршрутизаторах для определения путей передачи данных в сети. Они обеспечивают автоматическое определение маршрутов и перенаправление трафика между различными сегментами сети.

Существует множество различных маршрутизирующих протоколов, но они обычно делятся на две категории: векторные и состояния каналов.

Векторные протоколы, такие как RIP (Routing Information Protocol) и IGRP (Interior Gateway Routing Protocol), используют информацию о расстоянии и направлении для определения наилучшего маршрута. Они обмениваются информацией между собой и принимают решения на основе этой информации.

Состояния каналов протоколы, такие как OSPF (Open Shortest Path First) и IS-IS (Intermediate System to Intermediate System), используют более сложную информацию о состоянии каналов, такую как пропускная способность и задержки, для определения наилучшего маршрута. Они также обмениваются информацией между собой, чтобы принимать решения.

Кроме того, существуют также протоколы маршрутизации для различных типов сетей, такие как BGP (Border Gateway Protocol) для маршрутизации между автономными системами (AS).

36. Задаем название устройства

Router(config)# hostname

2. Задаем пароль для входа в привилегированный режим.

Router(config)# enable secret password

3. Задаем пароль на подключение через консоль.

Router(config)# line console 0

Router(config-line)# password password

Router(config-line)# login

4. Задаем пароль для удаленного доступа по Telnet / SSH.

Router(config-line)# line vty 0 4

Router(config-line)# password password

Router(config-line)# login

Router(config-line)# transport input {ssh | telnet}

5. Шифруем все пароли введенные на устройстве.

Router(config-line)# exit

Router(config)# service password-encryption

6. Задаем баннер, который будет выводится при подключении к устройству. В данном баннере обычно указывается правовая информация о последствиях несанкционированного подключения

Router(config)# banner motd delimiter message delimiter

7. Сохраняем конфигурацию.

Router(config)# exit

Router# copy running-config startup-config

37. Статическая маршрутизация - это процесс настройки маршрутизатора для пересылки пакетов между различными сетями. Для настройки статической маршрутизации необходимо выполнить следующие шаги: 1. Определить сетевые интерфейсы. Необходимо определить, какие интерфейсы будут использоваться для связи с другими сетями. 2. Настроить IP-адреса на интерфейсах. Каждому интерфейсу необходимо присвоить уникальный IP-адрес. 3. Определить маршруты. Необходимо определить, какие маршруты будут использоваться для пересылки пакетов между сетями. 4. Настроить статическую маршрутизацию. Необходимо настроить маршрутизатор для использования определенных маршрутов для пересылки пакетов между сетями.

Пример настройки статической маршрутизации на маршрутизаторе Cisco:

Определение сетевых интерфейсов:

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

interface GigabitEthernet0/1

ip address 10.0.0.1 255.255.255.0

Определение маршрутов:

ip route 192.168.2.0 255.255.255.0 10.0.0.2

ip route 10.1.1.0 255.255.255.0 192.168.1.2

Настройка статической маршрутизации:

ip routing

38. Для конфигурирования динамической маршрутизации используются две основные команды: router і network. Команда router запускает процесс маршрутизации и имеет форму:

Router(config)# router protocol [keyword]

,где Protocol - любой из протоколов маршрутизации: RIP, IGRP, OSPF и т.п., keyword –дополнительные параметры.

Затем необходимы команды network:

Router ( config-router)# network network-number [keyword]

где network-number - идентифицирует непосредственно подключенную сеть, добавляемую в процесс маршрутизации, keyword –дополнительные параметры. network-number позволяет процессу маршрутизации определить интерфейсы, которые будут брать участие в отсылке и приёме пакетов актуализации маршрутной информации.

Для просмотра информации о протоколах маршрутизации используется команда show ip protocol., которая выводит значения таймеров процессов маршрутизации и сетевую информацию, имеющую отношение к маршрутизации. Эта информация может использоваться для идентификации маршрутизатора, подозреваемого в поставке плохой маршрутной информации

Содержимое таблицы IP маршрутизации выводится командой show ip route. Она содержит записи про все известные маршрутизатору сети и подсети и указывает на способ получения этой информации.

39. Протоколы вектора расстояния (distance-vector protocols) используются для определения кратчайшего пути между двумя узлами в сети. Они основаны на обмене информацией о расстоянии до соседних узлов и выборе пути с наименьшим расстоянием.

Основные особенности протоколов вектора расстояния:

1. Медленная сходимость: при изменении топологии сети или отказе узла, протоколы вектора расстояния могут потребовать много времени для обновления таблиц маршрутизации и сходимости к новому оптимальному пути.

2. Неэффективное использование пропускной способности: протоколы вектора расстояния не учитывают загруженность линий связи и могут использовать неоптимальные пути, что может привести к перегрузке некоторых узлов и снижению производительности сети.

3. Неустойчивость к петлям в сети: при наличии петель между узлами, протоколы вектора расстояния могут создавать неоптимальные маршруты и приводить к непредсказуемому поведению сети.

4. Не поддерживают различные типы сервисов: протоколы вектора расстояния не учитывают различные типы сервисов, которые могут требовать различных параметров качества обслуживания.

5. Не поддерживают большие сети: протоколы вектора расстояния могут не справляться с большими сетями, так как требуют большого количества ресурсов для обработки и передачи информации.

40. Построение компьютерной сети может быть разным в зависимости от ее целей и требований. Однако, в общих чертах, процесс построения компьютерной сети может быть описан следующим образом: 1. Определение целей и требований сети: необходимо определить, для каких целей будет использоваться сеть и какие требования к ней предъявляются (например, скорость передачи данных, количество пользователей, типы устройств и т.д.). 2. Выбор типа сети: на основе целей и требований выбирается тип сети, который будет использоваться (например, локальная сеть, глобальная сеть, Wi-Fi сеть и т.д.). 3. Выбор оборудования: после выбора типа сети необходимо выбрать оборудование, которое будет использоваться для ее построения (например, маршрутизаторы, коммутаторы, модемы, сетевые карты и т.д.). 4. Подключение оборудования: после выбора оборудования необходимо его подключить и настроить для работы в сети. 5. Настройка сети: после подключения оборудования необходимо настроить сеть, установить адреса IP, настроить права доступа и т.д. 6. Тестирование и отладка: после настройки сети необходимо ее протестировать и отладить, чтобы убедиться в ее правильной работе. 7. Обслуживание и поддержка: после построения сети необходимо обеспечить ее обслуживание и поддержку, чтобы она работала без сбоев и проблем.

Это общий процесс построения компьютерной сети. Однако, каждая сеть может иметь свои особенности и требования, поэтому процесс построения может быть более сложным и детальным.

Линии связи и каналы передачи данных - это физические средства передачи информации между устройствами. К ним относятся провода, кабели, оптоволокно, беспроводные сети и другие технологии. Эти средства используются для передачи различных типов данных, включая голосовые, видео-, текстовые и другие форматы.

Существует несколько видов сетевой архитектуры, которые используются для создания компьютерных сетей, таких как:

Клиент-серверная архитектура - это модель, в которой существует один или несколько центральных серверов, которые обрабатывают запросы от клиентов, которые используют для доступа к данным и приложениям сеть. Примерами клиент-серверных архитектур являются почтовые серверы, серверы баз данных, веб-серверы и другие.

Peer-to-Peer (P2P) архитектура - это модель, в которой устройства выступают как равноправные партнеры и могут обмениваться информацией друг с другом без центрального сервера. Эта архитектура широко используется в торрент-сетях, VoIP-системах и других приложениях.

Шина (Bus) архитектура - это модель, в которой все устройства находятся на одной шине, которая связывает их и позволяет им обмениваться данными. Эта архитектура часто используется для локальных сетей.

Звездная (Star) архитектура - это модель, в которой все устройства подключаются к центральному коммутатору, который обрабатывает все запросы и передает данные между устройствами. Эта архитектура часто используется в крупных корпоративных сетях.

Сеть с гибкой топологией - это модель, в которой не существует жесткой топологии, и устройства могут подключаться друг к другу в любом порядке. Эта архитектура используется в сетях с повышенными требованиями к гибкости и масштабируемости.

И, конечно, существуют различные комбинации и гибриды этих архитектур, которые используются в сетевых системах для оптимизации производительности и надежности передачи данных.

41. Стандарт технологии TokenRing, также известный как IEEE 802.5, был разработан для создания локальных сетей с высоким уровнем надежности и производительности.

Технология TokenRing работает по принципу передачи данных по кольцу. Каждое устройство в сети соединено с предыдущим и следующим устройством в цепочке, образуя кольцевую топологию.

Для передачи информации использовался механизм токена, который перемещался по кольцу от устройства к устройству. Каждое устройство могло передать данные только после получения токена. Это позволяло снизить конфликты на линии связи и обеспечивать равномерное распределение времени доступа к сети между устройствами.

Сети Token Ring работают с двумя битовыми скоростями - 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается. Сети Token Ring, работающие со скоростью 16 Мбит/с, имеют некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мбит/с.

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры - посланный кадр всегда возвращается в станцию - отправитель. В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например, может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

42. FDDI (Fiber Distributed Data Interface) — это стандарт, или, вернее, набор сетевых стандартов, ориентированных, прежде всего, на передачу данных по волоконно-оптическом белю со скоростью 100 Мбит/с. Подавляющая часть спецификаций стандарта FDDI была разработана проблемной группой ХЗТ9.5 (ANSI) во второй половине 80-х годов. FDDI стала вой ЛВС, использующей в качестве среды передачи оптическое волокно.

В настоящее время большинство сетевых технологий поддерживают волоконно-оптический интерфейс в качестве одного из вариантов физического уровня, но FDDI оста наиболее отработанной высокоскоростной технологией, стандарты на которую прошли проверку временем и устоялись, а оборудование различных производителей показывает хорошую степень совместимости.

При разработке технологии FDDI ставились в качестве наиболее приоритетных следующие цели: - Повышение битовой скорости передачи данных до 100 Мбит/с; - Повышение отказоустойчивости сети за счет стандартных процедур восстановления после отказов различного рода — повреждения кабеля, некорректной работы сетевого узла, возникновения высокого уровня помех на линии и т. п.; - Максимально эффективное использование потенциальной пропускной способности с как для асинхронного, так и для синхронного графиков.

Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. У протокола FDDI есть и существенные отличия от Token Ring. Эти отличия связаны с требованиями, которые необходимы для поддержки большой скорости передачи информации, больших расстояний и возможности наряду с асинхронной передачи данных вести синхронную передачу. Два основных отличия в протоколах управления маркером у FDDI и IEEE 802.5 Token Ring следующие: - в Token Ring станция, передающая кадры, удерживает маркер до тех пор, пока не получит все отправленные пакеты. В FDDI же станция выпускает маркер непосредственно окончанием передачи кадра (кадров); - FDDI не использует приоритет и поля резервирования, которые Token Ring использует для выделения системных ресурсов.

43. Gigabit Ethernet (GbE) - это стандарт сетевой связи, который позволяет передавать данные со скоростью в 1 Гбит/с.

Он был разработан в 1998 году и стал первым коммерчески доступным стандартом высокоскоростных сетей Ethernet. GbE работает на стандартном витой паре медных кабелей (CAT5e, CAT6 и выше).

Он используется в крупных офисах, центрах обработки данных, на научных станциях и других местах, где необходимо быстрое передача большого объема данных.

Стоит отметить, что GbE не является самым быстрым стандартом, на данный момент уже существуют стандарты 10GbE (10 Гбит/с), 40GbE и 100GbE, но GbE все еще широко используется и остается одним из наиболее распространенных и универсальных стандартов в сфере сетевых технологий.

44. Канальный уровень (или уровень передачи данных) является частью архитектуры вычислительной системы и отвечает за передачу данных между устройствами и компонентами системы. Некоторые из базовых технологий, используемых на канальном уровне, включают:1. Локальные сети (LAN) - сетевые технологии, позволяющие передавать данные между устройствами в ограниченной географической области, например, внутри офиса или здания. Ethernet является одной из наиболее распространенных технологий локальных сетей. 2. Глобальные сети (WAN) - технологии, которые позволяют передавать данные между устройствами на большие расстояния, как правило, через Интернет. Примерами глобальных сетей являются интернет, VPN и MPLS. 3. Беспроводные сети (WLAN) - технологии, которые позволяют передавать данные без проводной связи между устройствами. Wi-Fi является самой распространенной технологией беспроводных сетей. 4. Протоколы передачи данных - стандарты, используемые для передачи данных о канальном уровне. Некоторые из наиболее распространенных протоколов передачи данных включают TCP/IP, UDP и ICMP. 5. Средства передачи данных - физические средства, используемые для передачи данных между устройствами. Некоторые из таких средств включают в себя медные кабели (например, витая пара), оптические кабели и радиоволны.

В 1980 году в результате работы «комитета 802», организации Instituteof Electrical and Electronics Engineers, IEEE, было принято семейство стандартов IEEE 802-х, которые содержат рекомендации по проектированию нижних уровней локальных сетей. Позже результаты работы этого комитета легли в основу комплекса международных стандартов ISO 8802-1...5.

Стандарты семейства IEEE 802.х охватывают два нижних уровня модели ISO /OSI - физический и канальный, потому что именно эти уровни в наибольшей степени отражают специфику локальных сетей

Функции канального уровня подразделяются на два подуровня: 1. управление доступом к среде передачи (MediaAccess Control, MAC); 2. управление логическим соединением (LogicalLink Control, LLC).

Подуровень MAC определяет такие элементы канального уровня, как логическая топология сети, метод доступа к среде передачи информации и правила физической адресации между сетевыми объектами.Аббревиатура MAC используется также при определении физического адреса сетевого устройства: физический адрес устройства (который определяется внутри сетевого устройства или сетевой карты на этапе производства) часто называют МАС-адресом этого устройства. Существует возможность программно изменить МАС-адрес большого количества сетевых устройств, особенно сетевых карт. При этом необходимо помнить, что канальный уровень модели ISO /OSI накладывает ограничения на использование МАС-адресов: в одной физической сети не может быть двух или более устройств, использующих одинаковый МАС-адрес.

Для определения физического адреса сетевого объекта может быть использовано понятие «адрес узла». Адрес узла чаще всего совпадает с МАС-адресом или определяется логически при программном переназначении адреса.

Подуровень LLC определяет правила синхронизации передачи и сервиса соединений. Этот подуровень канального уровня тесно взаимодействует с сетевым уровнем модели ISO /OSI и отвечает за надежность физических (с использованием МАС-адресов) соединений.

45. ARP(англ. Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера. Существуют следующие типы сообщений ARP: запрос ARP (ARP request) и ответ ARP (ARP reply). Система-отправитель при помощи запроса ARP запрашивает физический адрес системы-получателя. Ответ (физический адрес узла-получателя) приходит в виде ответа ARP.

Стандарт Ethernet, определенный в документе IEEE 802.3, дает описание единственного формата кадра уровня MAC. Так как в кадр уровня MAC должен вкладываться кадр уровня LLC, описанный в документе IEEE 802.2, то по стандартам IEEE в сети Ethernet может использоваться только единственный вариант кадра канального уровня, заголовок которого является комбинацией заголовков подуровней MAC и LLC.

Кадр Ethernet DIX, или Ethernet II, появился в результате работы консорциума трех фирм Digital, Intel и Xerox в 1980 году, представившего на рассмотрение комитету 802.3 свою фирменную версию стандарта Ethernet в качестве проекта международного стандарта.

Однако комитет 802.3 принял стандарт, отличающийся в некоторых деталях от предложения DIX, причем отличия касались и формата кадра. Так возник формат кадра 802.3/LLC, 802.3/802.2, или Novell 802.2.

q Кадр Raw 802.3, или Novell 802.3, появился в результате усилий компании Novell по ускорению работы своего стека протоколов в сетях Ethernet.

Кадр Ethernet SNAP стал результатом деятельности комитета 802.2 по приведению предыдущих форматов кадров к некоторому общему стандарту и приданию кадру необходимой гибкости, что позволило бы в будущем добавлять новые поля или изменять их назначение.

Кадр 802.3/LLC. Заголовок кадра 802.3/LLC является результатом объединения полей заголовков кадров, определенных в стандартах IEEE 802.3 и 802.2.

Стандарт 802.3 определяет восемь полей заголовка.

46. Ethernet-это сетевая технология, которая позволяет компьютерам и другим устройствам в одной сети связываться друг с другом. В отличие от беспроводной связи, в сети Ethernet сигналы проходят по проводам. Это тип сети, лежащей в основе локальных сетей (LAN), городских сетей (MAN) и глобальных сетей (WAN). Каждое устройство в сети Ethernet имеет карту Ethernet, более известную как NIC (контроллер сетевого интерфейса). Эти устройства называются узлами, и они общаются друг с другом с помощью протоколов . В контексте сети протокол — это язык общения между подключенными устройствами. Узлы обмениваются данными через фреймы, блоки информации, которые узлы отправляют в виде коротких сообщений. Фреймы несут информацию, которую узел отправляет другому узлу. Если протокол — это язык, кадры — это предложения. Протокол Ethernet определяет набор правил для построения фреймов, и каждый фрейм имеет адрес назначения и адрес источника для идентификации отправителя и получателя фрейма. Нет двух узлов с одинаковым адресом. Устройства подключаются друг к другу через Ethernet-кабели, также называемые средой.

MAC-адрес (Media Access Control address) — это уникальный идентификатор, присваиваемый сетевому адаптеру компьютера или другого сетевого устройства, чтобы идентифицировать его в сети. MAC-адрес состоит из 6 байтов (48 бит) и может быть представлен в шестнадцатеричной системе счисления. Он используется, например, для маршрутизации пакетов данных в локальной сети и для управления доступом к сетевым ресурсам. Кроме того, MAC-адрес может быть использован для защиты от несанкционированного доступа к сети.

47. БПД - это беспроводная передача информации между устройствами на определенном расстоянии. Существует несколько способов синхронизации устройств для передачи данных, каждый из которых имеет свои характеристики и минимальное/максимальное расстояние передачи. Для синхронизации устройств по радиоканалу используются специальные адаптеры, которые могут быть установлены в различных устройствах и передавать информацию по каналам разных частот и диапазонов.

Wi-Fi — это стандарт беспроводного подключения LAN для коммуникации разных устройств, относящийся к набору стандартов IEEE 802.11. Wi-Fi использует радиоволны (так же, как Bluetooth и сотовые сети) для коммуникации устройств в малом масштабе, например: в домах, торговых центрах, на площадях и т. д. Wi-Fi — это самый недорогой и быстрый способ передачи данных на короткие расстояния, включая просмотр веб-страниц, онлайн-игры, видеостриминг и VoIP-вызовы.

Стандарт 802.11 определяет беспроводную передачу информации между устройствами на определенном расстоянии с помощью специальных адаптеров. Существуют два основных режима организации сети: с базовой станцией и без нее. Беспроводные сети 802.11 легко сопрягаются с проводными сетями Ethernet.

48. Протокол OSPF (Open Shortest Path First) - это протокол маршрутизации, который используется для определения наименьшего пути между узлами в сети.

Каждый узел в сети, подключенный к OSPF, отправляет сообщения о состоянии своих соединений с другими узлами в сети. Эти сообщения передаются всем узлам в сети, чтобы каждый узел мог построить карту сети и определить наилучший путь до каждого узла.

OSPF также использует понятие областей, чтобы разделить сеть на более мелкие сегменты и уменьшить нагрузку на сеть. Каждая область имеет свой собственный экземпляр OSPF, который обрабатывает только информацию об этой области.

Протокол OSPF является протоколом класса Link-State, что означает, что каждый узел в сети имеет полную карту сети и знает о состоянии каждого соединения в сети.

49. Протокол маршрутизации RIP (Routing Information Protocol) - это протокол, который используется для автоматической маршрутизации IP-пакетов в сетях с динамической маршрутизацией. Он работает на основе расстояния до цели (distance-vector), где каждый маршрутизатор передает информацию о своих соседях и их маршрутах к цели.

Протокол RIP обменивает информацией о маршрутах между соседними маршрутизаторами, чтобы каждый маршрутизатор знал о доступных маршрутах к целевым сетям. Он использует максимальное число прыжков (hop count) для определения расстояния до цели, где каждый прыжок представляет один маршрутизатор на пути к цели.

Протокол RIP также использует таймеры для обновления информации о маршрутах и удаления неактуальных записей. Каждые 30 секунд маршрутизаторы обмениваются информацией о маршрутах, а если маршрут не был обновлен в течение 180 секунд, он считается устаревшим и удаляется из таблицы маршрутизации.

50. BGP (Border Gateway Protocol) - это протокол маршрутизации, который используется для обмена информацией между автономными системами (AS) в Интернете. Он используется для определения наилучшего маршрута для передачи данных между AS.

Протокол BGP работает на основе сети маршрутизаторов, которые обмениваются информацией о доступных маршрутах. Каждый маршрутизатор BGP поддерживает таблицу маршрутизации, которая содержит информацию о доступных маршрутах и их характеристиках.

Протокол BGP также используется для управления трафиком в Интернете. Он может быть настроен таким образом, чтобы определить наилучший маршрут для передачи трафика на основе различных критериев, таких как скорость соединения, стоимость маршрута и т.д.

51.Списки контроля доступа (ACL) - это механизмы, используемые для определения, кто имеет доступ к ресурсам в компьютерных сетях. Они позволяют администраторам сети управлять доступом пользователей к файлам, папкам, приложениям и другим ресурсам. Списки контроля доступа могут быть настроены на уровне операционной системы, сетевых устройств или приложений. Они могут быть настроены для определения прав доступа на основе имени пользователя, группы пользователей, IP-адреса или других параметров. Списки контроля доступа могут быть использованы для обеспечения безопасности сети и защиты конфиденциальной информации.

52. Принцип работы списков контроля доступа заключается в том, что они определяют права доступа пользователей к определенным ресурсам в сети. Для этого администратор настраивает ACL, указывая, какие пользователи или группы пользователей могут получить доступ к определенным ресурсам, а какие - нет. При попытке доступа к ресурсу система проверяет, соответствует ли запрос правилам ACL, и разрешает или запрещает доступ в зависимости от этого.

ACL могут быть настроены на разных уровнях сети, например, на уровне операционной системы, на уровне сетевых устройств или на уровне приложений. В каждом случае правила ACL могут быть настроены для разных параметров, таких как имя пользователя, группа пользователей, IP-адрес и т.д.

53.Существует два типа ACL-списков Cisco для IPv4:

1. Списки контроля доступа на основе номеров (Standard ACL) - позволяют настраивать правила доступа только на основе исходного IP-адреса отправителя пакета. Они могут использоваться для блокировки или разрешения трафика на основе IP-адресов.

2. Списки контроля доступа на основе именованных расширений (Extended ACL) - позволяют настраивать правила доступа на основе исходного и целевого IP-адресов, номеров портов, протоколов и других параметров. Они могут использоваться для более точной фильтрации трафика в сети.

54. DHCP - протокол автоматической настройки сетевых параметров устройств, подключенных к сети. Устройство отправляет запрос на получение IP-адреса, DHCP-сервер назначает свободный адрес и отправляет другие параметры. Назначенный IP-адрес имеет ограниченный срок действия. DHCP значительно упрощает процесс настройки и управления сетью.

55. Nat (Network Address Translation) - это технология, которая позволяет связывать локальную сеть с глобальным интернетом, переводя IP-адреса устройств в локальной сети на общедоступный адрес. Nat используется для оптимизации использования доступных IP-адресов и защиты локальной сети от атак извне.

56. Существует 3 базовых концепции трансляции адресов: 1. Статическое преобразование сетевых адресов (NAT) выполняет взаимно однозначное преобразование внутренних IP-адресов во внешние. Это позволяет преобразовать IP-адрес внутренней сети во внешний IP-адрес.

Статический NAT позволяет устанавливать соединения как внутренним, так и внешним системам, например, хостам Internet. Этот тип преобразования особенно рекомендуется применять для организации общего доступа к системе, находящейся во внутренней сети. Для этого нужно создать правило NAT для преобразования фактического адреса системы во внешний адрес. Этот адрес будет доступен внешним пользователям. В этом случае никто не сможет получить информацию о внутренней сети для последующих атак извне.

Ниже перечислены особенности статического NAT:

Это взаимно однозначное преобразование.

Его можно инициировать как из внешней, так и из внутренней сети.

Целевой адрес для преобразования может быть любым адресом.

Целевой адрес для преобразования не может применяться в качестве интерфейса IP

Нельзя применять NAT для преобразования портов.

2. Динамический NAT применяется при подключении компьютеров внутренней сети к хостам внешней сети.

При таком способе преобразования адресов создается пул сетевых адресов, применяемый для установления соединений с внешней сетью. Каждому соединению присваивается уникальный внешний адрес. Максимальное число активных соединений ограничено числом внешних адресов в пуле. Другими словами, между соединениями и адресами устанавливается взаимно-однозначное соответствие. Динамический NAT позволяет подключаться к Internet с помощью IP-адреса, выделенного из пула. На следующей схеме приведен пример динамического NAT.

3. Маскарадный NAT (Network Address Translation) - это метод, который позволяет скрыть реальные IP-адреса устройств в локальной сети и заменить их на один общий IP-адрес. Этот общий IP-адрес используется для связи с другими сетями в Интернете.

Когда устройство из локальной сети отправляет запрос в Интернет, маскарадный NAT заменяет его реальный IP-адрес на общий IP-адрес, который назначен маршрутизатору. Когда ответ приходит от внешнего сервера, маршрутизатор использует информацию в пакете для определения, какому устройству в локальной сети нужно отправить ответ.

Маскарадный NAT позволяет использовать один общий IP-адрес для нескольких устройств в локальной сети, что экономит адресное пространство и упрощает настройку сети. Однако, это может привести к проблемам с подключением к некоторым сервисам, которые требуют уникальных IP-адресов для каждого устройства.

57. PAT (Port Address Translation) — технология трансляции адресов с использованием портов. Данная технология решает проблему доставки возвратных пакетов. Так как количество белых IP ограничено нам необходимо экономить эти адреса. Помня об этом, была создана технология РАТ. Она позволяет локальным хостам использовать частные IP-адреса и установить один зарегистрированный адрес на маршрутизатор доступа. В технологии преобразования адресов РАТ используется особенность работы протокола ТСР: с точки зрения сервера абсолютно все равно, осуществляются соединения с тремя разными хостами с разными адресами или соединения устанавливаются с одним хостом на один IP-адрес, но с разными портами. Следовательно, чтобы подключить к Интернету множество хостов небольшого офиса с помощью одного только зарегистрированного публичного IP адреса, служба РАТ транслирует частные адреса локальных хостов в один имеющийся зарегистрированный. Чтобы правильно пересылать пакеты обратной коммуникации локальным хостам, маршрутизатор хранит у себя таблицу IP адресов и номеров портов для протоколов TCP и UDP