Компьютерные сети лекции.

Компьютерные сети. Термины, определения.

Компьютерная сеть – это система инфраструктурных элементов позволяющих согласованно использовать распределённые вычислительные ресурсы.

Задачи компьютерной сети:

1. Обеспечение доступности вычислительных ресурсов
2. Обеспечение безопасности инфраструктур
3. Обеспечение целостности инфраструктур

Структура компьютерной сети.

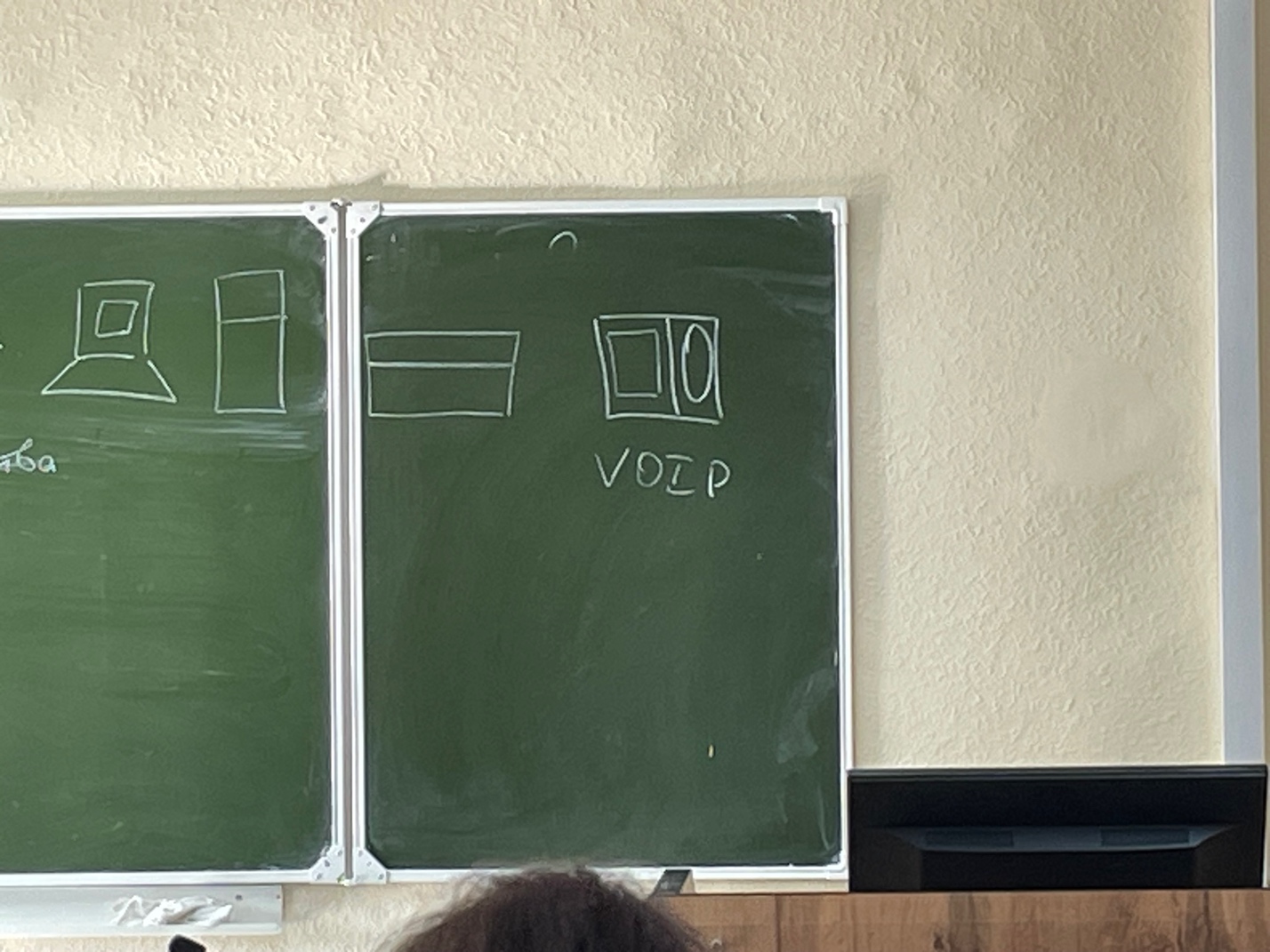
Сети состоят из следующих элементов:

1. Оконечные устройства
2. Промежуточные устройства
3. Каналы
4. Поток

К оконечным устройствам относятся: Компьютеры, сервера, сетевые принтеры, телефоны, камеры, датчики. Они характеризуются тем, что генерируют поток. Эти устройства являются отправителями и получателями потока.

На схемах оконечные устройства обозначаются как в Cisco Packet Tracer.

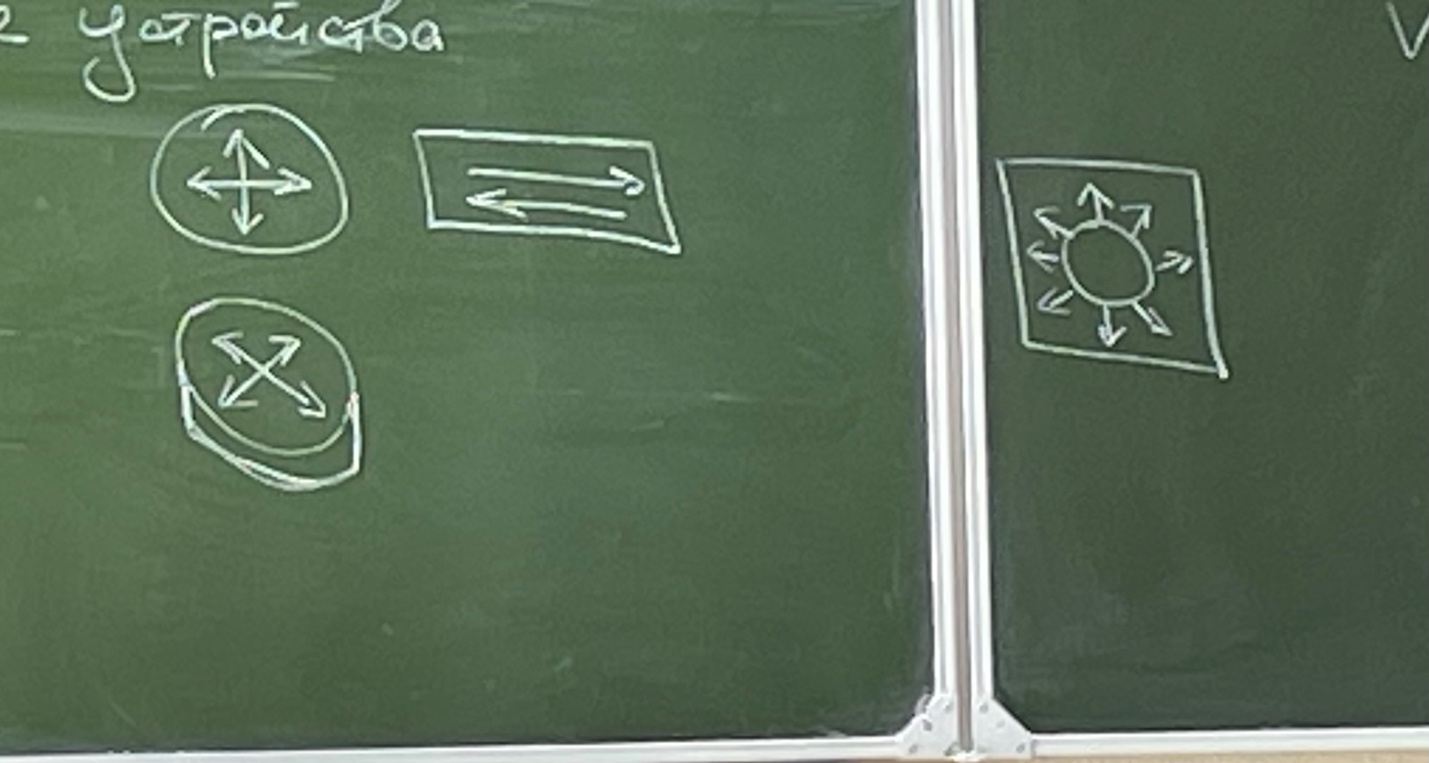
Компьютер, сервер, сетевой принтер, телефон VOIP:



Промежуточные устройства.

Основная характеристика промежуточных устройств в том, что они предназначены для передачи или пересылки потока.

Виды промежуточных устройств: маршрутизатор(роутер), коммутатор(свитч), сетевой экран(firewall):



Каналы передачи потока.

Под каналом понимают среду передачи потока, каналы бывают кабельные и эфирные.

К кабельным каналам относят:

1. Витую пару
2. Оптоволокно
3. Серийное и консольное подключение

К эфирным каналам относят:

1. Wi-Fi
2. Bluetooth
3. Инфракрасный канал

Разница между каналами – в физических принципах, логически все каналы работают одинаково.

Физический уровень работы каналов принято называть уровнем 2, а логический уровень работы канала принято называть уровнем 3. Сетевые схемы составляются на двух уровнях работы канала L2 и L3.

В дальнейшем мы будем объединять схемы L2 и L3.

Сетевые устройства тоже распределяются по уровням:

* Конечные устройства и роутеры – уровень 3
* Свитчи – уровень 2
* Firewall – и 2 и 3

В дальнейшем под каналом мы будем понимать витую пару.

Витая пара существует 2х видов:

1. - - - - кроссовый кабель
2. \_\_\_\_ прямой кабель

Устройства одного уровня соединяются кроссовым кабелем, устройства разных уровней – прямым.

Под потоком мы будем понимать любой трафик который способен быть переданым в нашей сети.

Устройства в сети связываются с каналом через интерфейс. Интерфейс это совокупность службы, протокола, порта и разъёма.

В нашем случае подавляющее большинство интерфейсов работает по протоколу Ethernet и каждый интерфейс обозначается буквой и цифрами.

***24.09 Общие сведения об адресации***

Каждый компьютер в сети пронумерован, каждый номер называется адресом.

Адреса:

1. Физические (MAC) – уровень 2 протокол ARP
2. Логические (ip): - уровень 3 протокол TCP/UDP

* v4 32bit
* v6 128bit

Адреса решают следующие задачи:

1. Обеспечение уникальности сетевых узлов
2. Обеспечение доставки сигналов по сети с помощью маршрутизации

Физические адреса в первую очередь обрабатываются протоколом ARP, который является основным для свитчей.

MAC-адреса присваиваются интерфейсам на заводе изготовителе и являются уникальными в мировом масштабе.

MAC-адрес – это 64-битная последовательность и 16-ричной системе счисления, мы считаем его неуправляемым.

Логические адреса – изменяемые, настраиваемые, удаляемые.

Любой из упомянутых адресов, представляет собой натуральное число.

11000000.10101000.00000000.00000001 – IP-адрес (32 бита) = 192.168.0.1

I II III IV

Для удобства человека адрес делят на 4 логических части (октеты, каждая по 8 бит).

Двоичный адрес переводится в десятичный по октетам.

128 64 32 16 8 4 2 1

1 1 0 0 0 0 0 0 128+64=192

Каждому интерфейсу в сети на самом деле соответствует несколько адресов:

1. Собственный IP-адрес
2. Маска подсети (Subnet Mask)

Маска – IP-адрес в котором все единицы стоят слева, а нули справа и они никогда не перемешиваются. Маска представляется либо десятично-точечно, либо записывают количество единиц. Количество единиц называют длиной маски. Именно маска является расчётным инструментом в маршрутизации. Комбинация MAC, IP и mask реализуют нахождение доставки пакетов в любую точку мира.

***1.10***

Класс

1 октет

Длина стандарт маски

Стандартная маска десяти-точечной нотации

A

1-126

/8

255.0.0.0

B

128-191

/16

255.255.0.0

C

192-223

/24

255.255.255.0

D, E

224-255

-

-

Частные:

От 10.0.0.0 до 10.255.255.255

От 172.16.0.0 до 172.16.255.255

От 192.168.00 до 192.168.255.255

127.x.y.z

Все остальные IP-адреса общие

Частные используют внутри корпоративных сетей

Общие адреса используются в внешних сетях провайдера

Если наша сеть не имеет выхода в реальную сеть провайдера, то между общими и частными адресами нет разницы.

Если в схеме адресации используются стандартные маски, то IP-адрес делится на 2 логические части.

11.10.10.10 – 00001011. 00001010. 00001010. 00001010

| ID-сети ID-узла

Класс A -> /8 -> 11111111.00000000. 00000000. 00000000

Узлы способны передавать друг другу пакеты без маршрутизации только в пределах одного и того-же номера сети.

Этот же принцип работает если используется маска меньше стандартной.

11.10.10.10 – 00001011. 00001010. 00001010. 00001010

| ID-сети ID-узла

Класс A -> /6 -> 11111111.00000000. 00000000. 00000000

Если используется маска больше стандартной, IP-адрес делится на 3 части.

11.10.10.10 – 00001011. 00001010. 00001010. 00001010

| ID-сети ID-подсети ID-узла

Класс A -> /10 -> 11111111.00000000. 00000000. 00000000

Узлы в рассмотренных ранее топологиях способны обмениваться сигналами только в пределах своей подсети.

Во всех случаях адрес узла не может состоять из одних нулей или одних единиц.

В этой связи на практике возникают следующие задачи:

1. Ёмкость подсети
2. Количество подсетей - K=2y, где y – количество битов в идентификаторе подсети
3. Доступность узлов

Ёмкость подсети – количество клиентов, которые будут видеть друг друга без маршрутизации. E=2x-2, где x – количество битов в идентификаторе узла.

В реальных случаях нужно стремиться к как можно большей длине маски.

Доступность узлов.

Главная задача имеет несколько способов решения:

1. Универсальный – выписать все интересующие адреса в двоичном виде и сравнить в них столько левых битов, сколько в маске единиц.

10.10.137.10/18 255.255.192.0

10.10.46.10/18 255.0.0.0

137 = 1 0 0 0 1 0 0 1

46 = 0 0 1 0 1 1 1 0

1. Сетевой диапазон

0-63

64-127

128-191

192- …

Определить самый правый октет в маске который изменился по сравнению со стандартной, из 256 вычесть значение этого октета, получить диапазон, начиная с нуля выписать все промежутки. Узлы будут видеть друг друга в том случае, если находятся в одном диапазоне.

1. Конъюнкция – хорош, когда под рукой инженерный калькулятор.

***8.10 Таблицы маршрутизации.***

Рассмотрим две топологии:

1. PC1(F0) – (F1) switch (F2) – (F0)PC2
2. PC1 – router1 – router2 – PC2

Рассмотрим, как в обоих случаях происходит доставка пакетов от PC1 до PC2.

Разумеется, предполагаем, что сеть сошлась.

Таблица ARP

|  |  |  |
| --- | --- | --- |
| Num | интерфейс | Соотв. MAC |
| 1 | F1 | MAC1 |
| 2 | F2 | MAC2 |

|  |  |  |  |
| --- | --- | --- | --- |
| Ip1 | Mac1 | Ip2 | Mac3 |
| Адрес отправителя | | Адрес получателя | |

При коммутации в заголовке пакета меняются только mac адреса.

В дополнение к этому на клиентах и на роутерах дополнительно возникает таблица маршрутизации. На клиентах таблицу маршрутизации можно проверить командой route print, а на роутерах show ip route. В зависимости от версии ОС вид таблицы маршрутизации может быть разный, но смысл всегда один.

Таблица маршрутизации состоит из строк, и каждая строка называется маршрутом. Каждый маршрут имеет следующие характеристики:

***29.10 Динамическая маршрутизация***

Доставка пакетов осуществляется в соответствии с таблицами. Если роутер подключён к той или иной сети, то информация их неё попадает автоматически. Если администратор записывает маршрут вручную, то происходит статическая маршрутизация.

Существуют следующие протоколы динамической маршрутизации:

1. rip – частные сети
2. ospf – частные и общие
3. bgp – общие
4. is-is – общие

Протокол rip – никак не различает соседей, работает в рамках одного общего процесса, хорош если в сегменте не больше 30 роутеров.

R1 (config)#

router rip

version2

network <сеть и маска> - n-штук

Если данный набор команд выполнить на всех роутерах, то сеть rip начнёт сходиться.

C: 4.4.4.0/50

A: 192.168.10.64/27 🡨🡪 R1 🡨🡪 R2 🡨🡪 B: 172.16.20.64/28

\ /

R3

R1 (config)#

router rip

version2

network 192.168.10.64 255.255.255.224

network 4.4.4.0 255.255.255.252

R2 (config)#

router rip

version2

network 172.16.20.64 255.255.255.240

network 4.4.4.0 255.255.255.252

Маршруты, полученные по протоколу rip помечаются буквой r.

Уточнения:

1. При использовании динамической маршрутизации необязательно анонсировать все сети.
2. С помощью протокола rip можно делиться статическими маршрутами
3. При использовании динамической маршрутизации возникает административная дистанция, чем она больше, тем менее предпочтителен маршрут
4. При использовании rip никак нельзя выбрать соседей, с которыми ты хочешь делиться информацией о сетях

Протокол ospf – в отличие от протокола rip позволяет достаточно гибко выбирать соседей, существует в рамках нескольких процессов и не имеет ограничений на количество роутеров в сегменте. Ospf действует в рамках разных процессов и разных областей. В отличие от rip обмен можно ограничить ещё и интерфейсами.

R1 (router-config)#

router ospf 10

passive-interface default - отключение всех интерфейсов

network 192.168.10.64 0.0.0.31 area <номер области> - включение нужных интерфейсов

network 4.4.4.0 0.0.0.3 area <номер области>

R2 (router-config)#

router ospf1

version2

network 172.16.20.64 0.0.0.15

network 4.4.4.0 0.0.0.3

Команда ospf используется в инверсной маске сетей, которая получается от текущей маски с вычетом 27. Контролировать работу rip модно только с помощью команды show ip route

19.11. DHCP

Позволяет настроить интерфейсы сети автоматически. В основе DHCP лежит понятие пула. Пул – набор адресов которые могут получать клиенты для работы в сети.

Агрегация каналов, преобразование сетевых адресов, маршруты по умолчанию.