

Вводная презентация для подготовки кандидатов к собеседованию по техническим вопросам.

Старший специалист по подбору персонала
Калужского филиала ОАО «Вымпелком»
Екатерина Климова

Модель OSI

Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни, прикладные процессы и физические средства соединения.

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединие точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

1. Физический уровень.

На данном уровне происходит передача сигналов в среде передачи данных.

Физический кабель, оптический кабель и радио-связь.

Единица измерения, используемая на этом слое — **Биты**.

На данном уровне работает такое устройство, как НАВ (Хаб) – концентратор.

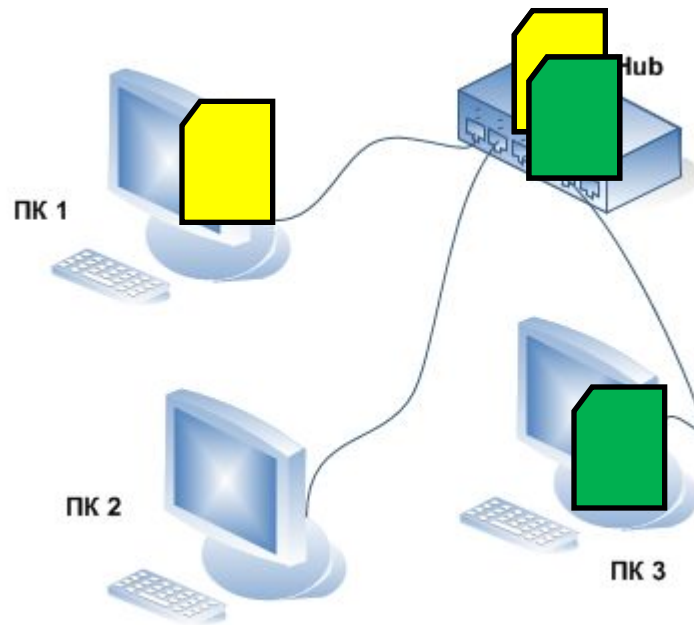
ХАБ

- сетевой концентратор, который позволяет объединить компьютеры в простую сеть. В хабе имеется определенное количество разъемов (портов), к которым подключаются все ПК сети.



Принцип работы Хаба.

ЗАДАНИЕ: Нужно передать информацию с ПК1 на ПК3



ВЫВОД: Информацию получают **все ПК в сети!**

2. Канальный уровень.

На данном уровне происходит передача внутри одного сегмента сети. Так же на этом уровне возможно обнаружение и, возможно, исправление ошибок, возникших на физическом уровне.

На данном уровне передаются **Кадры**.

На данном уровне работают Switch (Коммутатор) и Мосты.

Здесь используется понятие MAC-адреса.

MAC-адрес.

MAC – адрес – это физический адрес сетевого устройства. Его присваивает устройству производитель при изготовлении. По MAC_адресу мы можем понять, кто изготовил данное устройство. MAC–адрес состоит из шести больших латинских букв (A, B, C, D, E, F) и цифр (от 0 до 9)

Запись может быть:

1. Большими буквами через тире (6 октетов):

Пример **1C-4F-FD-E1-88-0A**

2. Маленькими буквами через двоеточие (6 октетов):

Пример **1c:4f:fd:e1:88:0a**

3. Маленькими буквами через точки (3 октета):

Пример **1c4f.fde1.880a**

Задание:

Какие из перечисленных записей будут являться MAC-адресами?

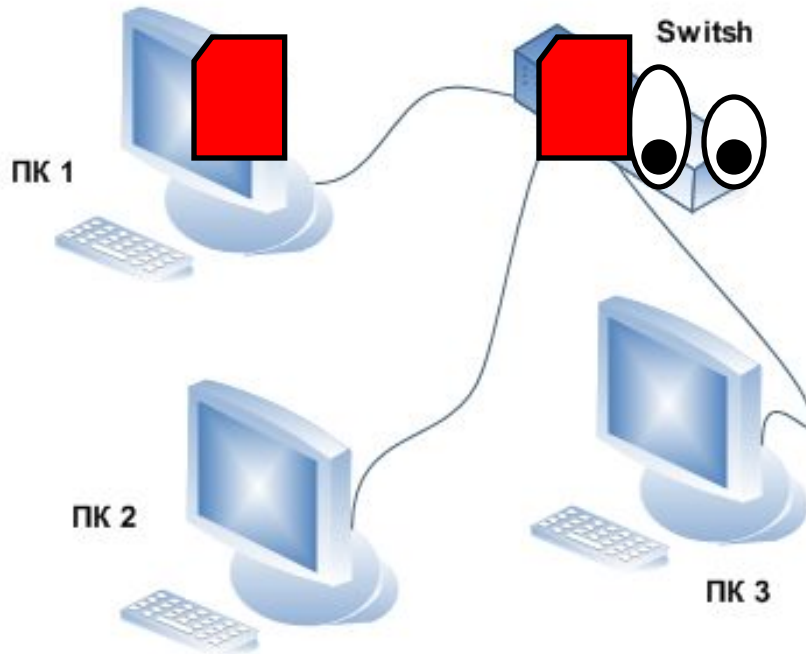
1. AB – CH – 13 – 16 - A6 – 99 - 18 **НЕТ**
2. ab : 95 : f6 : 19 : 55 : 5r **НЕТ**
3. FB – 74 – FA – 16 – 95 - 34 **ДА**
4. m6h7.7436.fdb5.t795 **НЕТ**
5. 76 – 45 – 18 – 7F – BB - FF **ДА**
6. adbf.1587.f5b1 **ДА**
7. fb : 5b : aa : 94 : f3 : 77 **ДА**
8. FA – HH – 14 – 99 – 56 – 17 **НЕТ**

СВИТЧ.

- сетевой коммутатор. Как и хаб, свитч предназначен для объединения множества компьютеров в одну локальную сеть.



Принцип работы Свитча.



ПК1 – MAC1 – подключен в порт 1
ПК2 – MAC2 – подключен в порт 2
ПК3 – MAC3 – подключен в порт 3

MAC - адрес	№ порта
MAC1	1
MAC2	2
MAC3	3

ЗАДАНИЕ: Передаем информацию от ПК1 к ПК3.

ВЫВОД: Информацию получает **только тот ПК, которому она предназначалась!**

3. Сетевой уровень.

На данном уровне происходит определение пути передачи данных. Здесь происходит трансляция из имен логических (ip-адрес) в имена физические (MAC-адрес), определение кратчайших маршрутов.

На данном уровне работает такое сетевое оборудование как Роутер (маршрутизатор).

IP-адрес.

-это уникальный сетевой адрес узла в компьютерной сети. . В сети Интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети.

В 4-й версии IP-адрес представляет собой 32-битовое число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел значением от 0 до 255, разделённых точками, например, 192.168.0.60. ~~192.168.678.2 – являться ip-адресом не будет!~~

Маска подсети и адрес подсети.

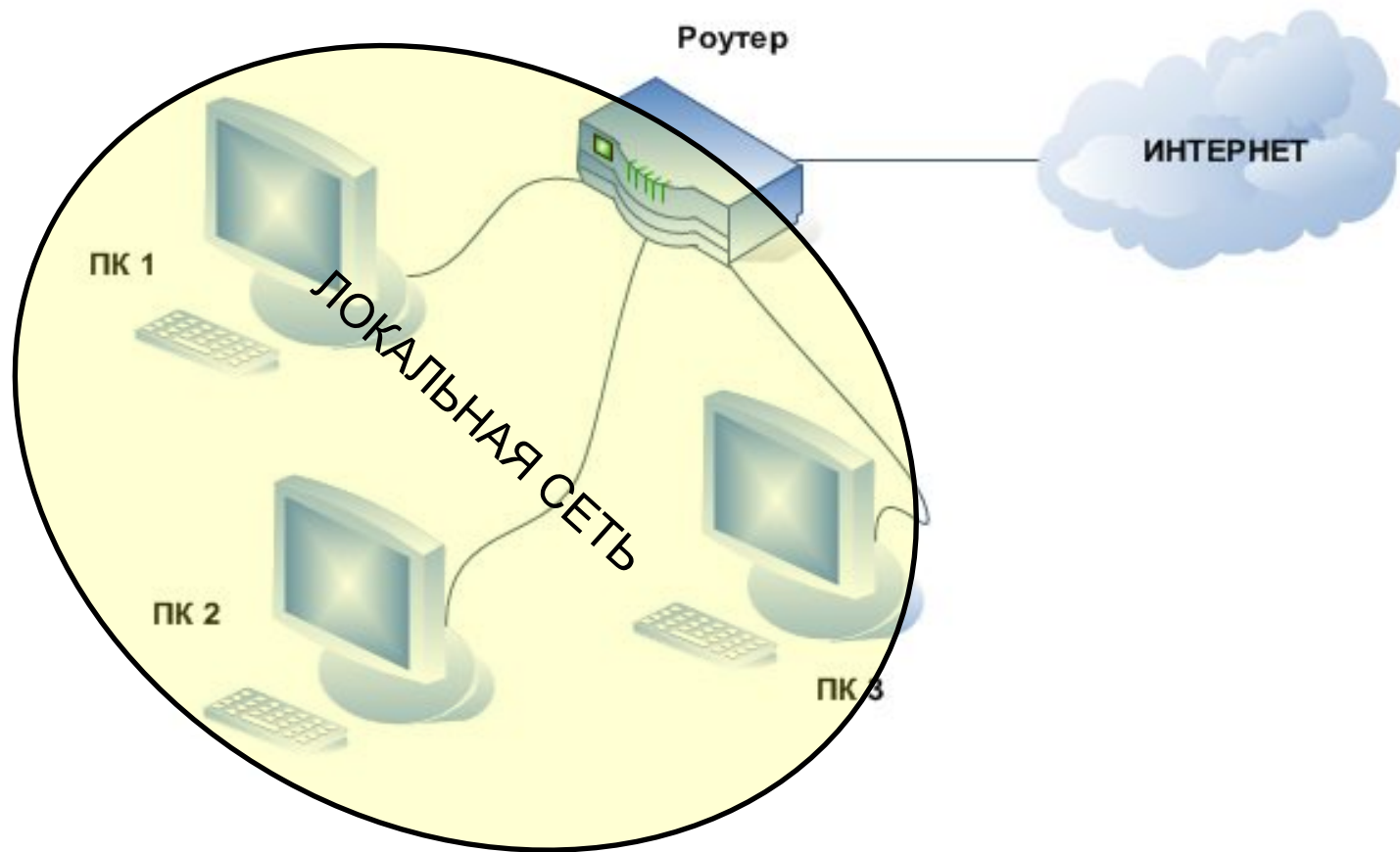
Маской подсети или **маской сети** называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети.

РОУТЕР

- маршрутизатор, который умеет передавать данные между различными сетями, например сетью вашего интернет провайдера и вашей домашней локальной сетью.



Принцип работы Роутера.



ПЛЮСЫ Роутера.

1. Нет необходимости дополнительно настраивать компьютеры и программы для подключения к сети Интернет.
2. Роутер потребляет меньше электроэнергии по сравнению с обычным ПК и его труднее взломать при грамотной настройке.
3. В случае с Wi-Fi роутером вы сможете работать в интернете с любого места вашей квартиры и наконец-таки избавитесь от кучи проводов.

VPN-соединение.

ЛОКАЛЬНАЯ СЕТЬ

ip – адрес
Маска подсети
DNS
Основной шлюз

ИНТЕРНЕТА НЕТ!



Для подключения к интернету необходимо настроить *vpn-соединение*, которое будет работать поверх *локального соединения*.

Вручную

(инструкция есть на сайте beeline.ru)

Мастером настройки


(скачать на сайте beeline.ru)

VPN-соединение.

ИНТЕРНЕТ ЕСТЬ!



Подключение: RussianProxy VPN



Пользователь: Login

Пароль:

Сохранять имя пользователя и пароль:

только для меня

для любого пользователя

Подключение Отмена Свойства Справка

Основные протоколы.

Состояние - Подключение по локальной сети

Подключение по локальной сети

Общие

Подключение

IPv4-подключение: Интернет

IPv6-подключение: Без доступа к Интернету

Состояние среды: Подключено

Длительность: 00:00:10

Скорость: 100.0 Мбит/с

Сведения...

Активность

Отправлено — Принято

Байт: 14 354 | 28 390

Свойства Отключить Диагностика

Закр

Сведения о сетевом подключении

Дополнительные сведения о сети:

Свойство	Значение
Определенный для подк...	mshome.net
Описание	Realtek RTL8139/810x Family Fast Ethernet
Физический адрес	00-1A-92-9B-A4-67
DHCP включен	Нет
Адрес IPv4	192.168.137.189
Маска подсети IPv4	255.255.255.0
Аренда получена	17 августа 2011 г. 11:43:50
Аренда истекает	24 августа 2011 г. 11:43:49
Шлюз по умолчанию IPv4	192.168.137.1
DNS-сервер IPv4	192.168.137.1
WINS-сервер IPv4	
Служба NetBIOS через T...	Нет
Локальный IPv6-адрес ка...	fe80::d952:7d41:aca8:6074%10
Шлюз по умолчанию IPv6	
DNS-сервер IPv6	

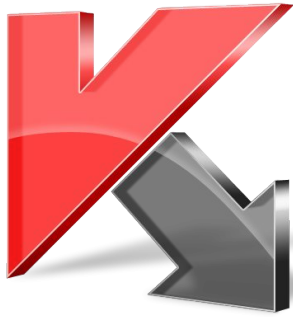
Закреть

TCP - один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP. Отличие данного протокола от UDP в том, что перед передачей данных предварительно устанавливается соединение между хостами. Благодаря этому данный протокол является надежным.

UDP – протокол передачи данных. С помощью данного протокола передаются данные без предварительной установки связи между хостами (устройствами). Данный вид протокола не является надежным, т.к. данные могут не доходить до конечной точки, либо путаться.

ARP — протокол в компьютерных сетях, предназначенный для определения **MAC-адреса** по известному **IP-адресу**.

SMTP — это протокол, предназначенный для передачи электронной почты в сетях TCP/IP. Работает в почтовых приложениях, например Outlook для передачи почтовых сообщений. На прием работает протокол POP3.

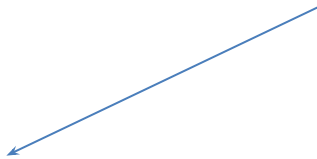


Антивирус и брандмауэр
(firewall).

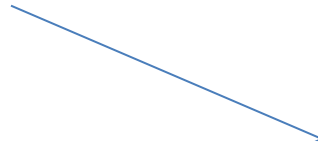


Антивирус

- специализированная программа **для обнаружения компьютерных вирусов**, а также нежелательных программ вообще и восстановления заражённых такими программами файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.



Антивирус сравнивает каждый имеющийся в компьютере файл со своей базой данных, содержащей информацию об известных ей вредоносных программах. Для того чтобы работа такого антивируса была действительно эффективной, требуется, чтобы информация в этой базе постоянно обновлялась, причем чем чаще, тем лучше.



Отслеживание действий, характерных для вирусов. Антивирусные программы анализируют то, как ведут себя те или иные файлы, и принимают решение об их нейтрализации. Чаще всего такой антивирусный мониторинг ведется на протяжении всего времени работы компьютера.

Брендмауэр(firewall)

- это программа, позволяющая надежно защитить компьютер, подключенный к локальной либо глобальной компьютерной сети, от атак сетевых злоумышленников.

Как правило, брендмауэр постоянно находится в оперативной памяти компьютера, функционируя в фоновом режиме. Работает он по следующему принципу: осуществляет фильтрацию всего **входящего трафика**, проверяя все подозрительные пакеты и отправляя их обратно. Пакеты, содержание которых опасений не вызывает (например, предназначенные веб-браузеру), без проблем пропускаются программой в компьютер. Кроме разделения пакетов на "разрешенные" и "подозрительные", с отсеиванием последних, программа умеет определять ip-адрес компьютера, с которого пришел "подозрительный" пакет.

Что касается **исходящего трафика**, то здесь firewall просто отслеживает все попытки запущенных на компьютере пользователя программ получить доступ к локальной сети либо сети Интернет. Это необходимо для блокировки работы различных программ злоумышленника, предназначенных для перехвата паролей и пересылки их своему создателю.

Типы передачи данных.

- **Unicast** (юникаст) – процесс отправки пакета от одного хоста к другому хосту.
- **Multicast** (мультикаст) – процесс отправки пакета от одного хоста к некоторой ограниченной группе хостов.
- **Broadcast** (бродкаст) – процесс отправки пакета от одного хоста ко всем хостам в сети.