



СИСТЕМЫ КОММУТАЦИИ.

Часть 2. Пакетная коммутация

Предмет изучения:

- Технологии канального уровня (Ethernet);
- Технологии сетевого уровня (IP);
- Протоколы маршрутизации (RIP, OSPF, EIGRP);
- Вспомогательные протоколы и службы стека TCP/IP (ARP, DHCP, DNS, NAT);
- Базовые средства сетевой защиты.

Литература: Манин А.А., Сосновский И.А. Системы коммутации. Принципы и технологии пакетной коммутации. Учебное пособие. – 3-е изд., перераб. и доп. – Ростов-на-Дону: СКФ МТУСИ, 2019. – 245 с.

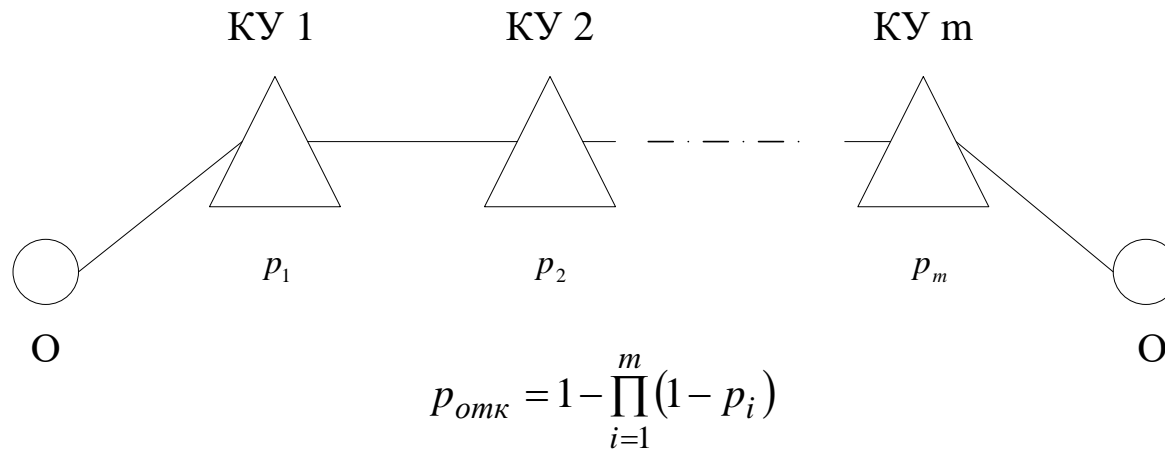


Вводная часть

1. Сравнительный анализ способов коммутации

Коммутация каналов.

Под коммутацией каналов понимается образование сквозного тракта передачи информации через определенное количество коммутационных узлов. Соответственно, фазе передачи информации предшествует фаза установления соединения.





Коммутация пакетов.

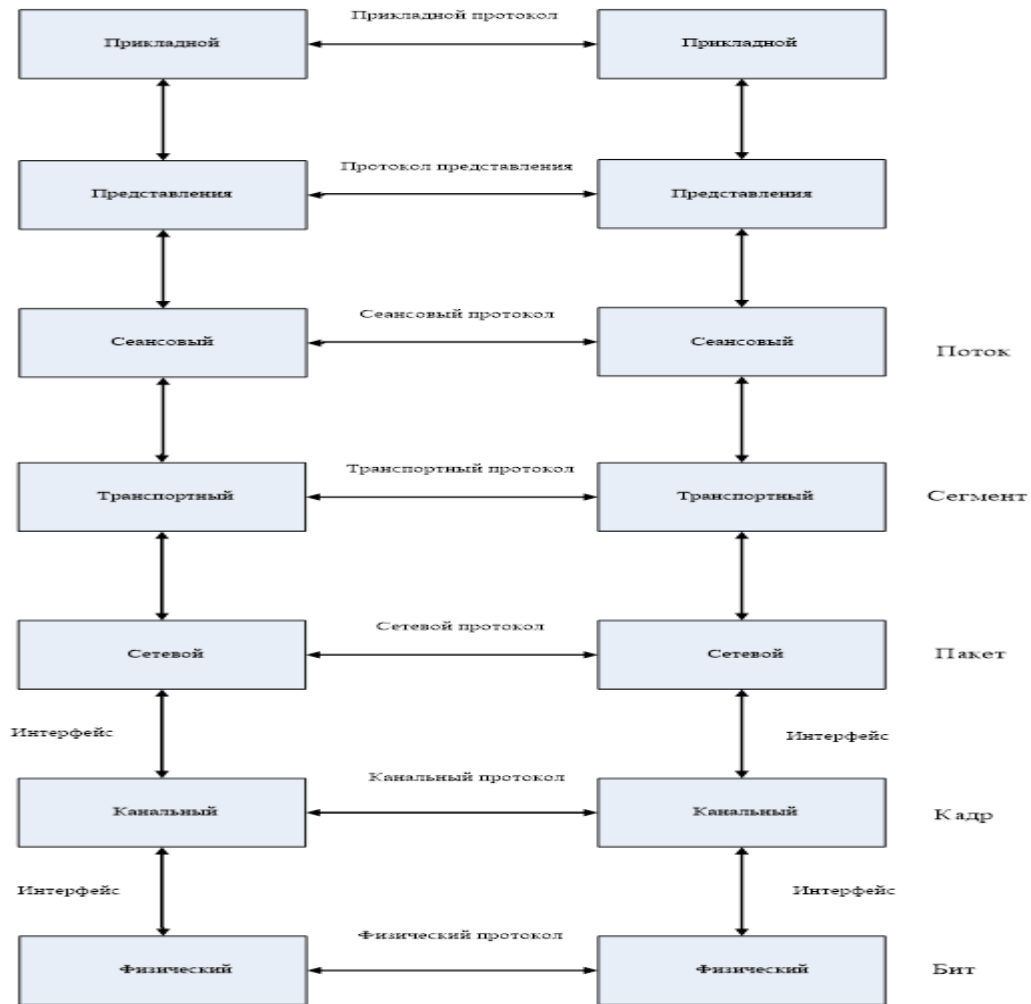
При таком способе коммутации данные передаются фрагментами фиксированного или переменного размера, называемыми пакетами. Для пакета всегда задается его максимальный размер – MTU (Maximum Transmission Unit), определяемый конкретным телекоммуникационным протоколом. В состав каждого пакета входит адресный заголовок, на основе анализа которого коммутационный узел определяет путь дальнейшей передачи.

Задержки передачи данных в сети с коммутацией пакетов можно разделить на два вида:

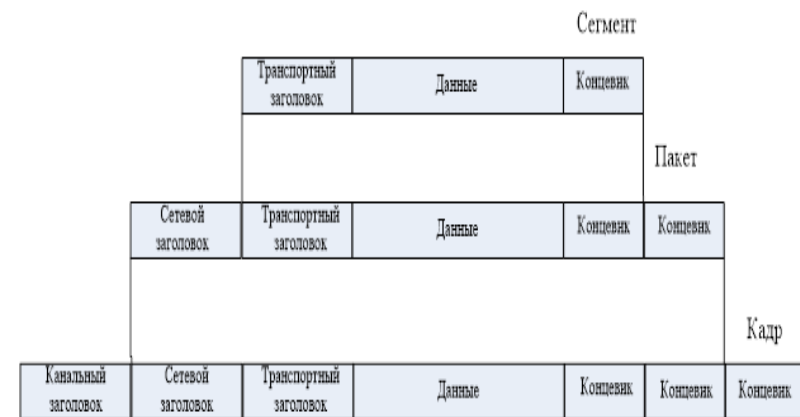
1. Алгоритмические задержки;
2. Случайные задержки.



2. Структура стека протоколов TCP/IP



Модель взаимодействия OSI



Процесс инкапсуляции



Прикладной	SMTP, POP, HTTP, FTP, TFTP, DNS, Telnet, SSH
Основной (транспортный)	UDP, TCP
Межсетевого взаимодействия	IPv4, IPv6 RIP, OSPF, EIGRP, BGP
Сетевые интерфейсы	Ethernet (IEEE 802.3)

Стек протоколов TCP/IP



Лекция 1

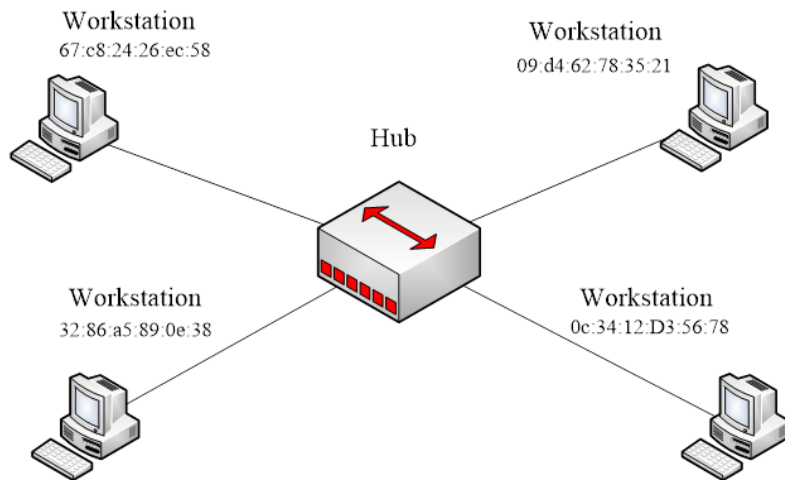
Основы технологии Ethernet

Вопросы:

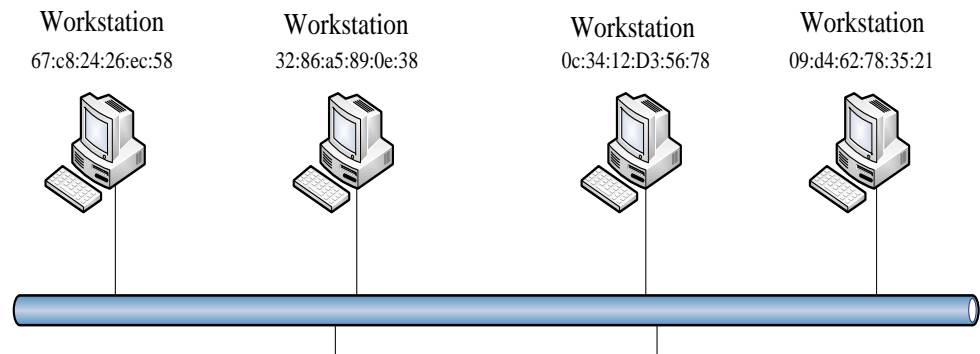
1. Метод доступа в некоммутируемой сети Ethernet.
2. Формат кадров Ethernet.
3. Физические спецификации Ethernet (самостоятельно).



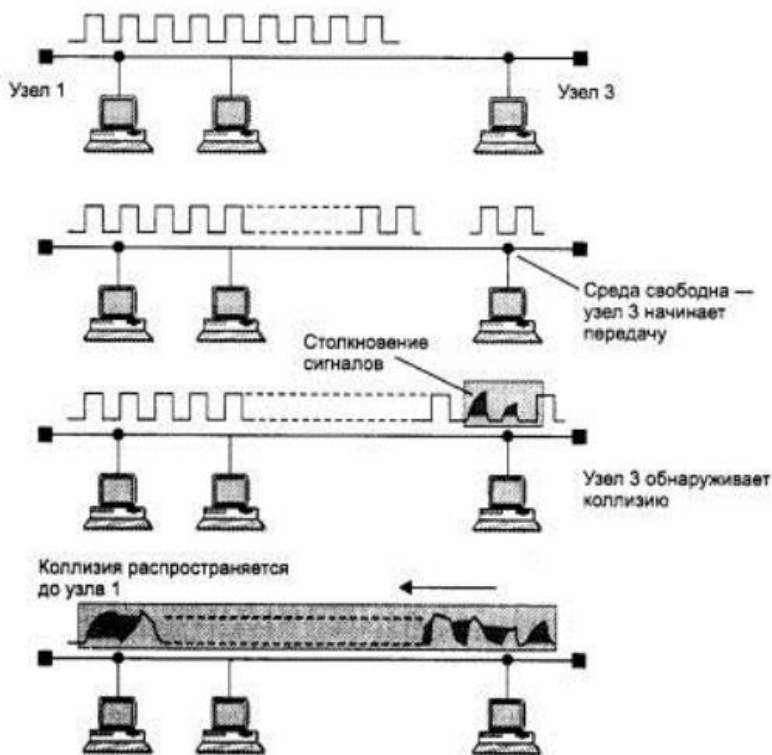
1. Метод доступа в некоммутируемой сети Ethernet.



Звездобразная топология



Шинная топология



Возникновение коллизии

Метод доступа - набор правил, регламентирующих передачу данных рабочими станциями по общей разделяемой среде.

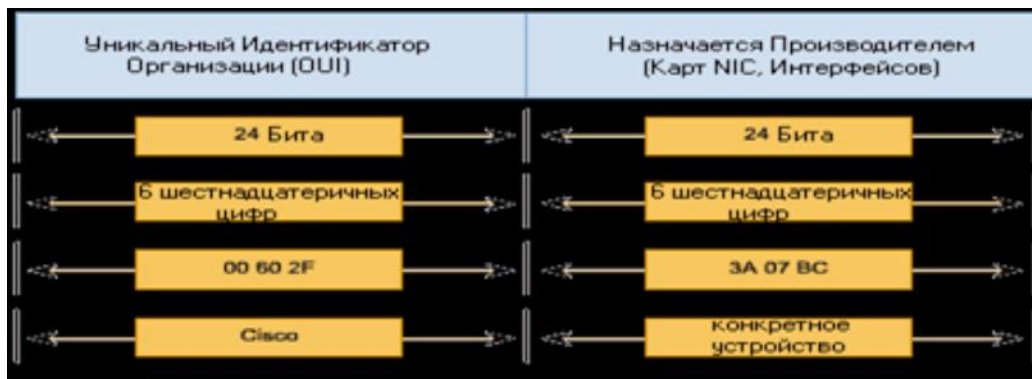
CSMA/CD – Carrier Sence Multiply Access with Collision Detection (метод коллективного доступа с контролем несущей и обнаружением коллизий)



2. Формат кадров Ethernet

Преамбула	SFD	DA	SA	L	Data	FCS
7 байт	10101011	6 байт	6 байт	2 байта	46-1497 байт	4 байта

- преамбула – последовательность, состоящая из семи одинаковых байт вида 10101010, совместно с начальным ограничителем кадра SFD используется для синхронизации принимающего порта;
- DA (Destination Address) – адрес назначения (рабочая станция, которой предназначен кадр);
- SA (Source Address) – адрес источника (рабочая станция, передающая кадр);
- L (Length) – определяет длину поля, в котором непосредственно передаются данные;
- Data – поле для передаваемых данных;
- FCS (Frame Check Sequence) – контрольная сумма, позволяющая выявить ошибки в принятом кадре.





Лекция 2

Коммутируемые сети Ethernet

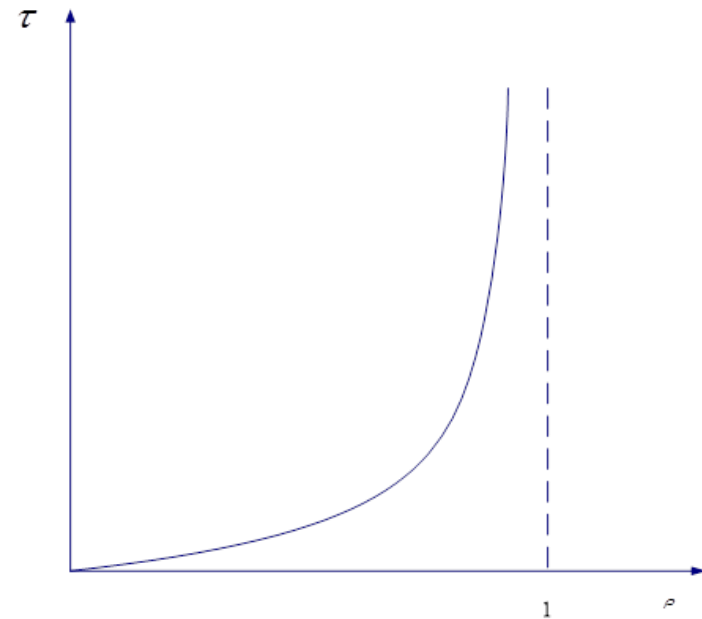
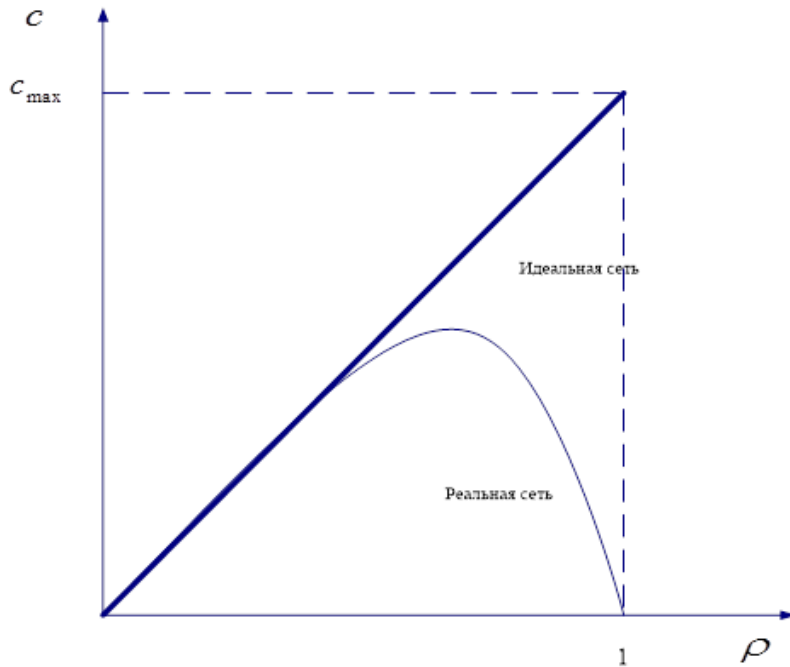
Вопросы:

1. Ограничения сетей, построенных на общей разделяемой среде.
2. Алгоритм работы прозрачного моста.
3. Коммутаторы Ethernet.



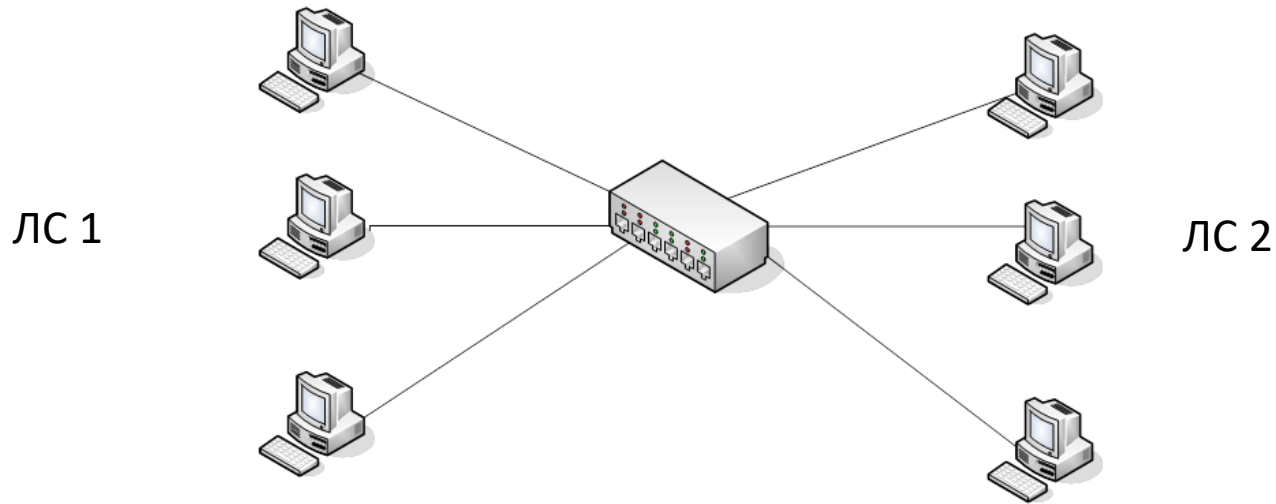
1. Ограничения сетей, построенных на общей разделяемой среде передачи

$$\rho = \frac{c}{c_{\max}} \quad - \text{коэффициент загрузки сети.}$$





2. Алгоритм работы прозрачного моста



$C = C_1 + C_{1-2} + C_2$ - суммарный трафик до сегментации.

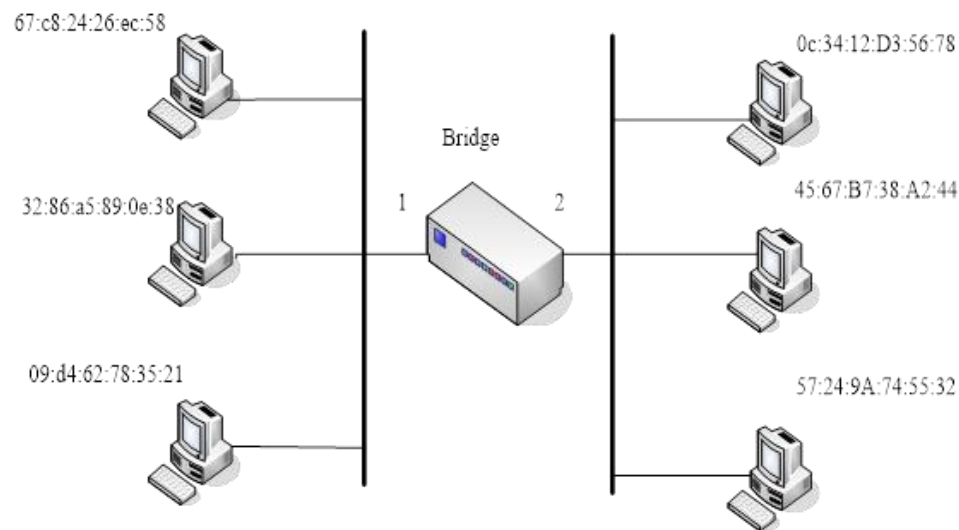
После сегментации:

$C = C_1 + C_{1-2}$ - трафик первого сегмента ЛС 1.

$C = C_2 + C_{1-2}$ - трафик второго сегмента ЛС 2.



Пример сети с мостом (Bridge)



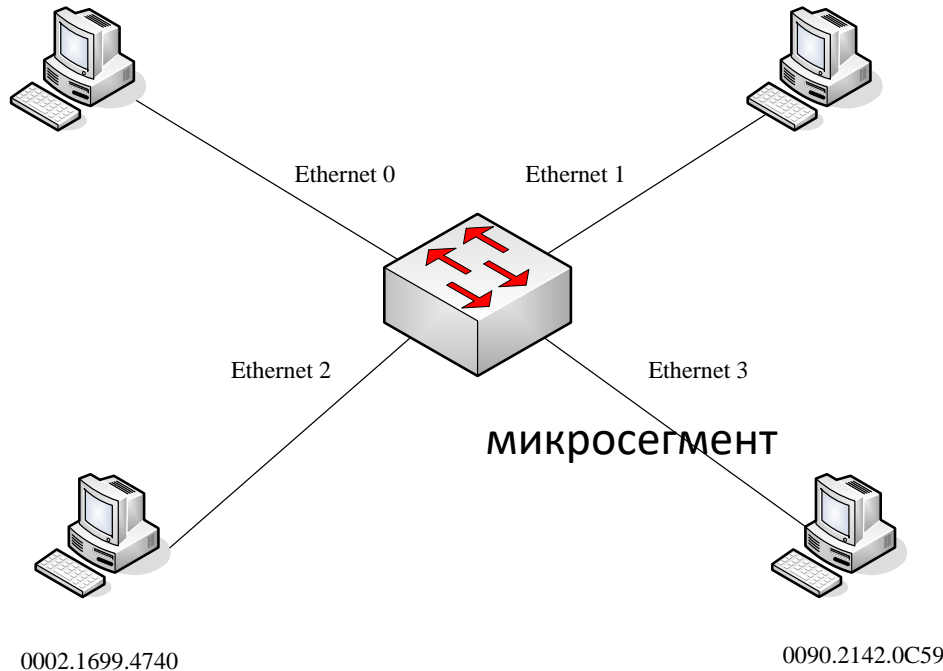
Адрес	№ сегмента (порта)
67:c8:24:26:ec:58	1
32:86:a5:89:0e:38	1
09:d4:62:78:35:21	1
0c:34:12:D3:56:78	2
45:67:B7:38:A2:44	2
57:24:9A:74:55:32	2



3. Коммутаторы Ethernet

0060.2FBA.5B24

00E0.B02B.7D01



Порт	Адрес рабочей станции
Ethernet 0	0060.2FBA.5B24
Ethernet 1	00E0.B02B.7D01
Ethernet 2	0002.1699.4740
Ethernet 3	0090.2142.0C59



Просмотр адресной таблицы на коммутаторе Cisco



```
Switch>enable
Switch#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0002.1699.4740    DYNAMIC   Fa0/3
1       0060.2fba.5b24    DYNAMIC   Fa0/1
1       0090.2142.0c59    DYNAMIC   Fa0/4
1       00e0.b02b.7d01    DYNAMIC   Fa0/2
Switch#
```



Лекция 3.

Особенности Ethernet-коммутаторов

Вопросы:

1. Техническая реализация коммутаторов (самостоятельно).
2. Характеристики коммутаторов Ethernet (самостоятельно).
3. Дополнительные функции коммутаторов.
 - 3.1 Организация виртуальных локальных сетей (VLAN).
 - 3.2 Блокировка резервных портов.
4. Моделирование работы коммутаторов

Лекция 4.

Объединение сетей средствами сетевого уровня



3.1 Дополнительная функция – организация виртуальных локальных сетей (Virtual Local Area Network – VLAN).

Причины разработки технологии VLAN:

1. Слабая изоляция сетей на коммутаторах от широковещательного шторма (Broadcast storm).
2. Облегчение локализации проблем при разделении сети.
3. Необходимость разграничения прав доступа к сетевым ресурсам.
4. Необходимость организации IP-телефонии совместно с передачей данных в единой сети.
5. Применение коммутаторов третьего уровня (Multilayer Switch).

Технология VLAN описана в открытом стандарте IEEE 802.1Q, кроме того, существует фирменный стандарт Cisco Systems, называемый ISL.



Просмотр VLAN на одном коммутаторе Cisco

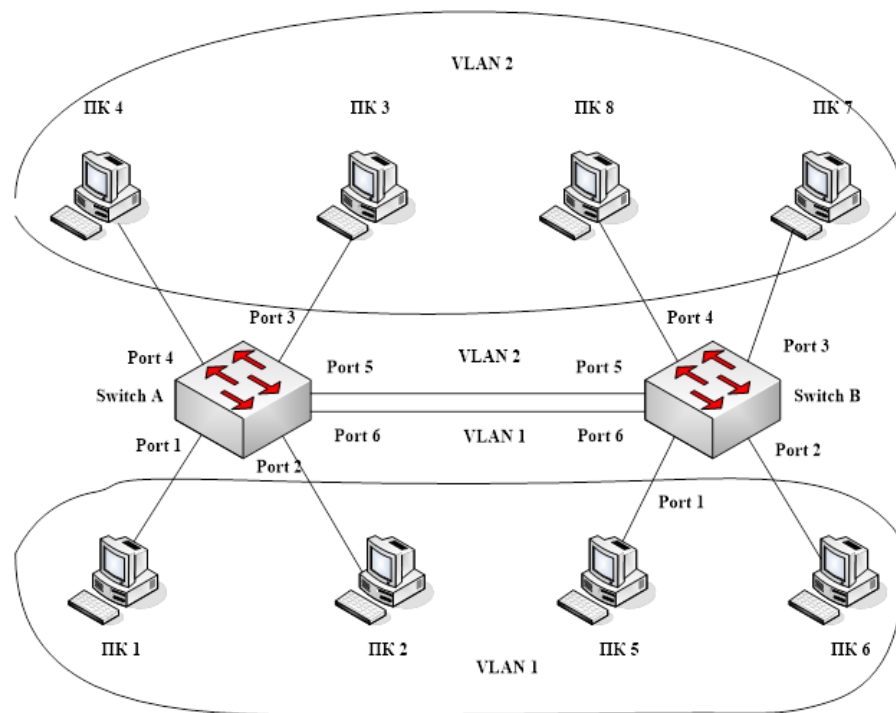
```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
2 subnet_2	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
3 subnet_3	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
4 subnet_4	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch#
```



Создание VLAN на нескольких коммутаторах



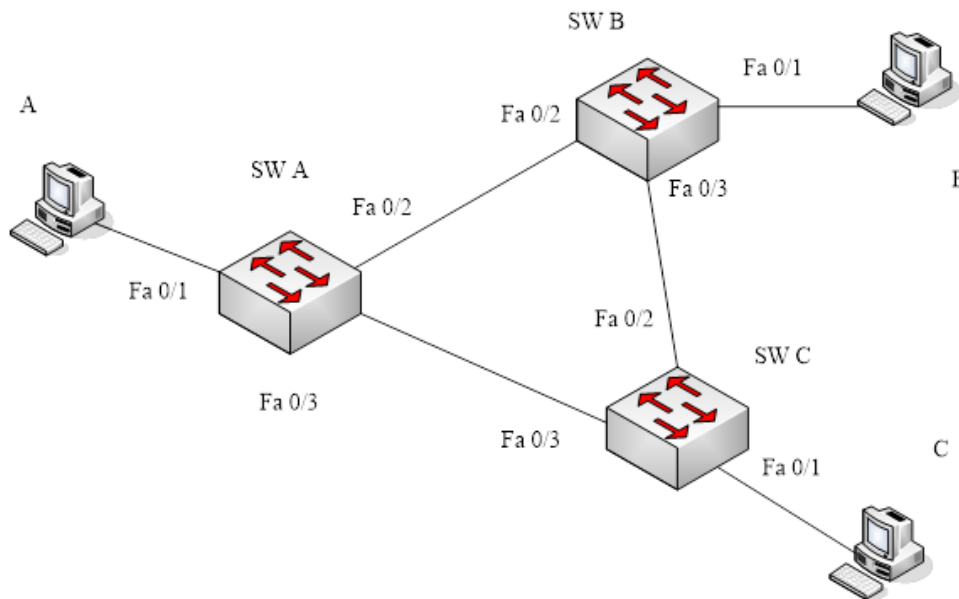
6	6	4	2	42 - 1496	4
Destination address	Source address	Ter 802.1Q	Длина/ Тип	Данные	Контр. сумма

2	3 бита	1 бит	12 бит
TPID	PCP	CFI	VLAN ID



3.2 Дополнительная функция – блокировка портов с целью исключения «петель»

Пример сети с «петлей»



Коммутатор А

Порт	Адрес рабочей станции
Fa 0/1	A

Коммутатор В

Порт	Адрес рабочей станции
Fa 0/2	A

Коммутатор С

Порт	Адрес рабочей станции
Fa 0/3	A

Коммутатор С

Порт	Адрес рабочей станции
Fa 0/2	A



Лекция 4.

Объединение сетей средствами сетевого уровня

Вопросы:

1. Ограничения сетей на мостах и коммутаторах.
2. Маршрутизация пакетов в составной сети.
3. Принципы маршрутизации.
4. Классы IP-адресов.
5. Использование масок в IP-адресации.
6. Динамическая маршрутизация.
7. Конфигурирование статической маршрутизации
8. Конфигурирование динамической маршрутизации.



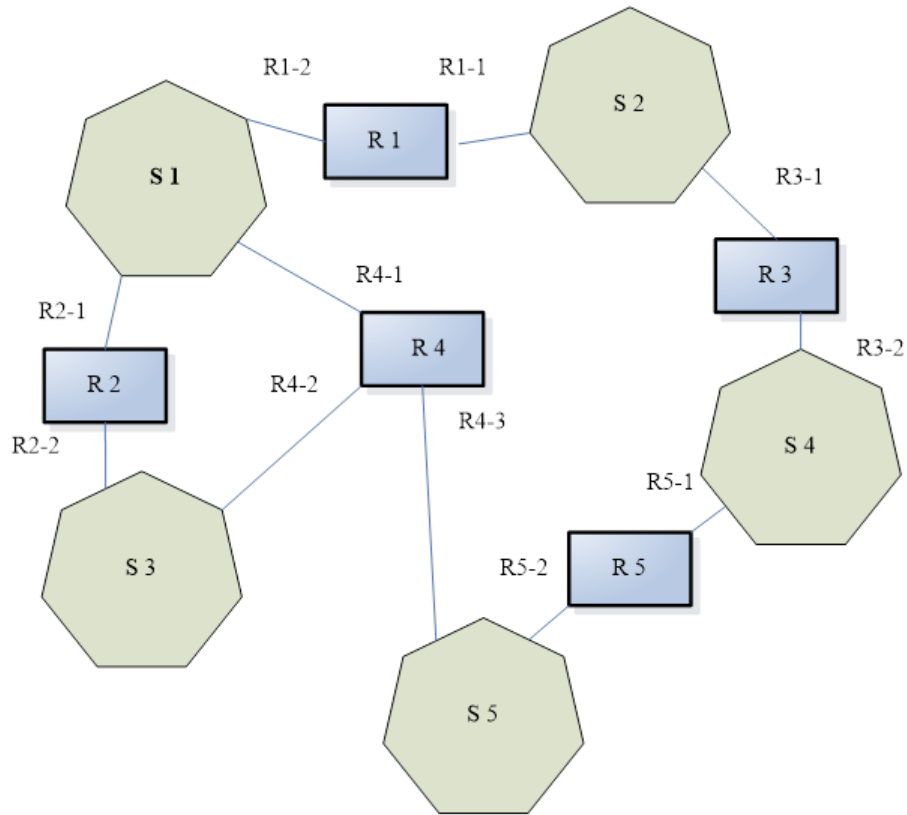
1. Ограничения сетей на мостах и коммутаторах

1. В топологии сети на коммутаторах должны отсутствовать «петли».
2. В сетях на коммутаторах неудобная система адресации – MAC-адреса являются плоскими, и задаются не администратором сети, а производителем оборудования.
3. Логические сегменты сети слабо изолированы друг от друга – широковещательные кадры передаются на все порты коммутатора, что может привести к широковещательному шторму.
4. Возможностью трансляции протоколов канального уровня обладают далеко не все типы мостов и коммутаторов, к тому же эти возможности ограничены.

Наличие серьезных ограничений у протоколов канального уровня показывает, что построение на основе средств этого уровня больших неоднородных сетей является весьма проблематичным. Естественное решение в этих случаях – это привлечение средств более высокого, сетевого уровня.



2. Маршрутизация пакетов в составных сетях



Структура сетевого
адреса

Адрес сети	Адрес узла
---------------	---------------



3. Принципы маршрутизации

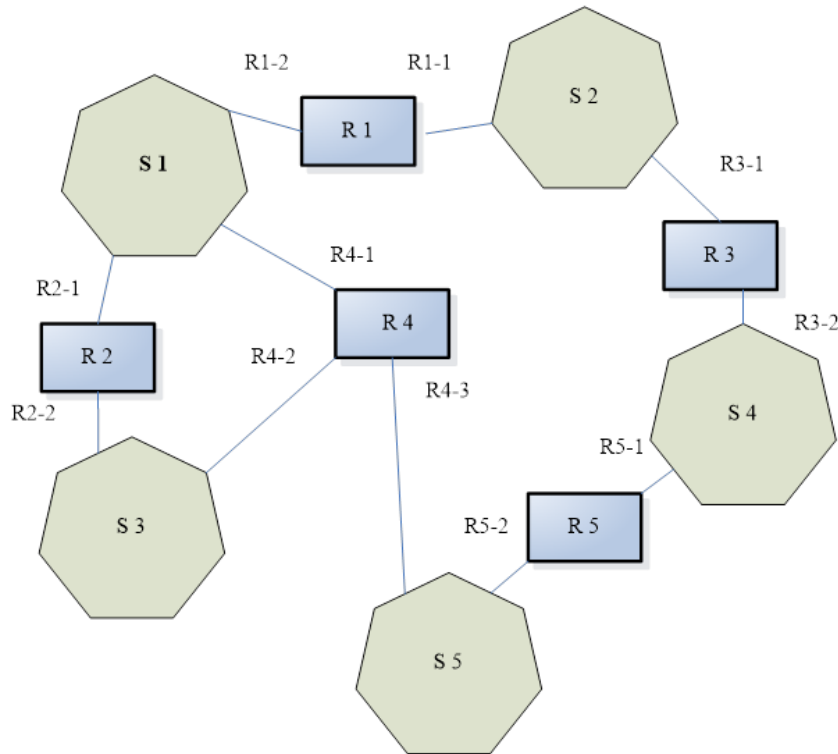


Таблица маршрутизации маршрутизатора R2

Адрес сети	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
S1	-	R2-1	0
S2	R1-2	R2-1	1
S3	-	R2-2	0
S4	R1-2	R2-1	2
S5	R4-1	R2-1	1
S5	R4-2	R2-2	1

Таблица маршрутизации узла А, принадлежащего сети S2

Адрес сети	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
S4	R3-1	A-1	1
Default	R1-1	A-1	-



4. Классы IP-адресов

Структура IP-адреса четвертой версии

11000000.10101000.01100100.00010100 – двоичная форма

192.168.100.20 – двоично-десятичная форма

0	x	x	x	x	x	x	x	2-й байт	3-й байт	4-й байт
№ сети – 1 байт								№ узла – 3 байта		

Класс А

1	0	x	x	x	x	x	x	2-й байт	3-й байт	4-й байт
№ сети – 2 байта								№ узла – 2 байта		

Класс В

1	1	0	x	x	x	x	x	2-й байт	3-й байт	4-й байт
№ сети – 3 байта									№ узла – 1 байт	

Класс С

Характеристика классов IP-адресов

Класс	Первый байт	Наименьший адрес сети	Наибольший адрес сети	Число узлов
А	0xxxxxxx	1.0.0.0	126.0.0.0	
В	10xxxxxx	128.0.0.0	191.255.0.0	
С	110xxxxx	192.0.0.0	223.255.255.0	
Д	1110xxxx	224.0.0.0	239.255.255.255	Multicast



Недостатки деления IP-адресов на классы:

1. Все возможные сети могут быть классифицированы только на три вида — крупные (с адресами класса А), средние (с адресами класса В) и малые (с адресами класса С);
2. Имеющийся дефицит адресов четвертой версии.
3. Невозможность дополнительного деления сети на подсети.



5. Использование масок в IP-адресации

Технология маски переменной длины (VLSM – Variable-Length Subnet Mask)

192.168.100.20 – адрес 255.255.255.0 – маска

11000000.10101000.01100100.00010100 - адрес

11111111.11111111.11111111.00000000 - маска

11000000.10101000.01100100.00010100

11111111.11111111.11111111.00000000

11000000.10101000.01100100.00000000

192.168.100.0 – номер сети

192.168.100.20/24

11000000.10101000.01100100.00010100

00000000.00000000.00000000.11111111

00000000.00000000.00000000.00010100

0.0.0.20 – номер узла



Деление на подсети с использованием маски переменной длины

192.168.100.0/24 – адрес сети

11111111.11111111.11111111.10000000 – 255.255.255.128 – маска.

11000000.10101000.01100100.00000000 – 192.168.100.0/25 подсеть 1;

11000000.10101000.01100100.10000000 – 192.168.100.128/25 подсеть 2.

11111111.11111111.11111111.11000000 – 255.255.255.192 – маска.

11000000.10101000.01100100.00000000 – 192.168.100.0/26 подсеть 1;

11000000.10101000.01100100.01000000 – 192.168.100.64/26 подсеть 2;

11000000.10101000.01100100.10000000 – 192.168.100.128/26 подсеть 3;

11000000.10101000.01100100.11000000 – 192.168.100.192 подсеть 4.



6. Динамическая маршрутизация. Протокол RIP

Этап 1: Создание минимальных таблиц

Минимальная таблица маршрутизатора R1

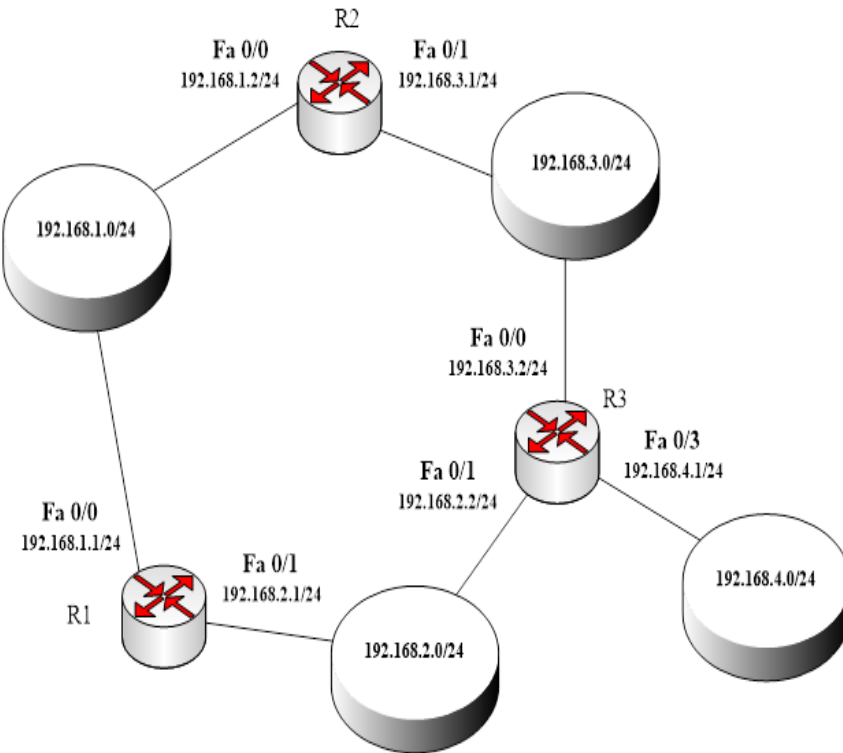
Адрес сети назначения	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
192.168.1.0	-	192.168.1.1	1
192.168.2.0	-	192.168.2.1	1

Минимальная таблица маршрутизатора R2

Адрес сети назначения	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
192.168.1.0	-	192.168.1.2	1
192.168.3.0	-	192.168.3.1	1

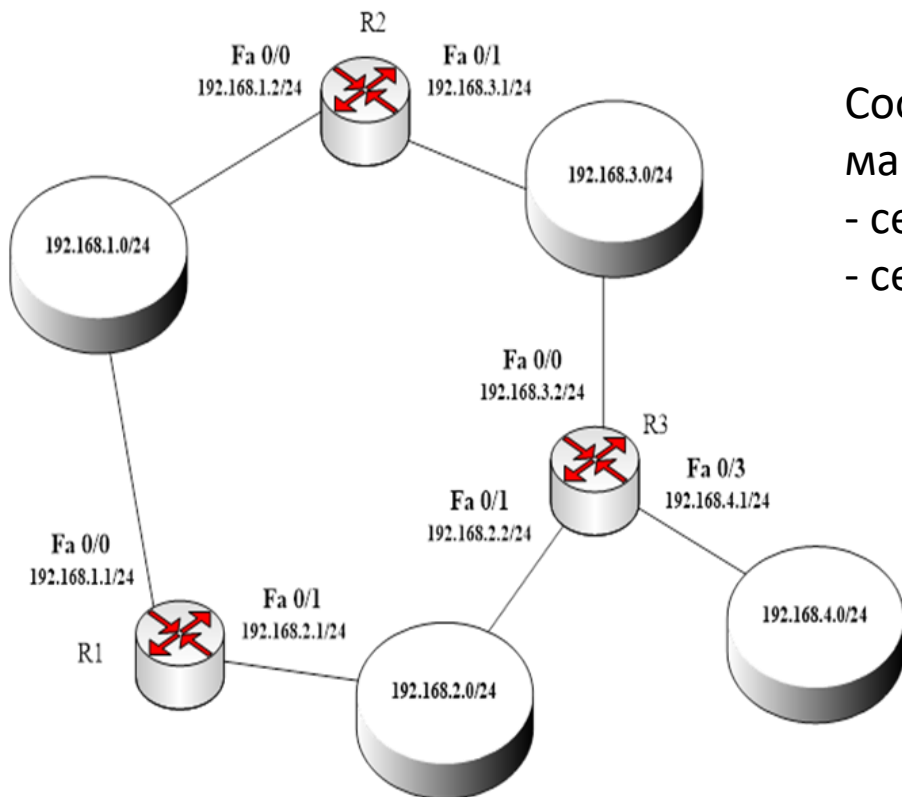
Минимальная таблица маршрутизатора R3

Адрес сети назначения	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
192.168.3.0	-	192.168.3.2	1
192.168.2.0	-	192.168.2.2	1
192.168.4.0	-	192.168.4.1	1





Этап 2: Рассылка минимальных таблиц «соседям»

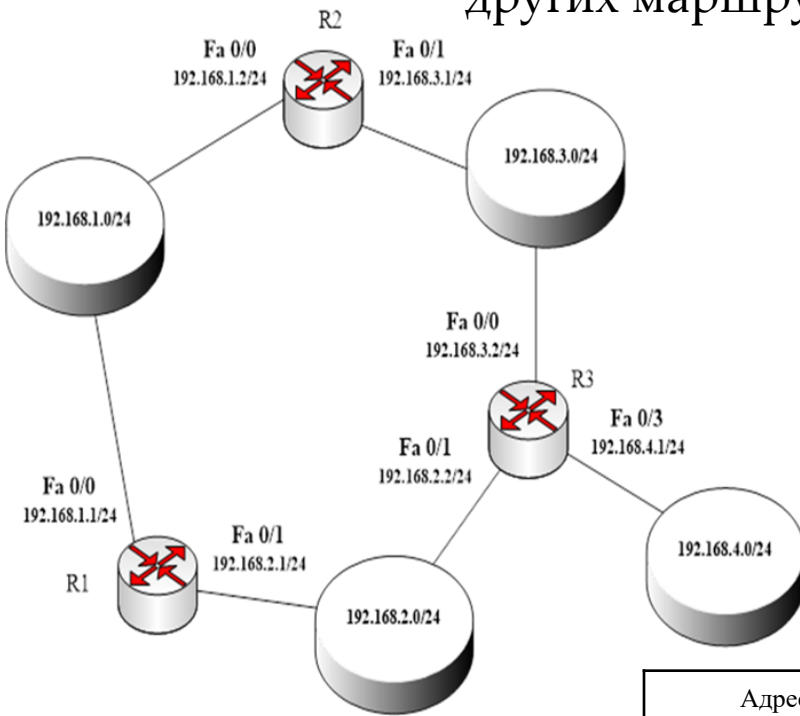


Сообщения от маршрутизатора R1 для маршрутизаторов R2 и R3:

- сеть 192.168.1.0, метрика 1;
- сеть 192.168.2.0, метрика 1.



Этап 3: Обработка информации, принятой от других маршрутизаторов



После получения информации маршрутизатор обрабатывает ее – увеличивает значение принятой метрики на единицу и запоминает порт, на который пришло данное сообщение, а также адрес маршрутизатора (точнее, его порта), передавшего сообщение. Эта информация заносится в таблицу маршрутизации.

Адрес сети назначения	Адрес порта следующего маршрутизатора	Адрес выходного порта	Метрика
192.168.1.0	-	192.168.1.1	1
192.168.2.0	-	192.168.2.1	1
192.168.1.0	192.168.1.2	192.168.1.1	2
192.168.3.0	192.168.1.2	192.168.1.1	2
192.168.3.0	192.168.2.2	192.168.2.1	2
192.168.2.0	192.168.2.2	192.168.2.1	2
192.168.4.0	192.168.2.2	192.168.2.1	2



Особенности RIP

- Рассылка таблиц производится каждые 30 с.;
- Максимальное значение метрики – 16;
- Значительное время сходимости;
- «Засорение» сети служебным трафиком;
- RIPv.1 поддерживает маршрутизацию на основе классов, а RIPv.2 – на основе масок переменной длины.



Лекция 5.

Технологии транспортного уровня

Вопросы (самостоятельно):

1. Структура сегментов протоколов UDP и TCP.
2. Установление и завершение соединений в протоколе TCP.
3. Обеспечение надежности доставки в протоколе TCP.
4. Управление потоком в протоколе TCP.



Лекция 6.

Вспомогательные протоколы и службы стека TCP/IP

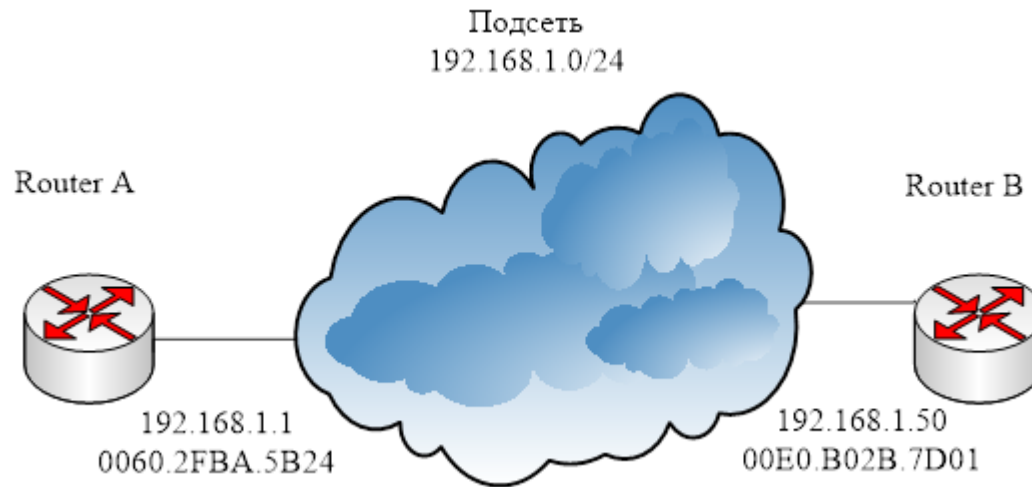
Вопросы:

1. Протокол ARP и служба DNS.
2. Протокол DHCP.
3. Технология NAT.
4. Построение корпоративной сети с DHCP, DNS, NAT.



1. Протокол ARP и служба DNS

Address Resolution Protocol (ARP) – протокол разрешения адреса



```
Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Александр Манин>arp -a

Интерфейс: 192.168.1.6 --- 0x3
  Адрес IP          Физический адрес      Тип
  192.168.1.1       b8-a3-86-45-f3-4e     динамический
C:\Documents and Settings\Александр Манин>_
```



Domain Name System (DNS) – служба доменных имен.

Типы адресов в стеке TCP/IP:

1. Числовые (IP-адреса);
2. Локальные (MAC-адреса для Ethernet);
3. Символьные доменные имена (yandex.ru).

Организационные имена зон:

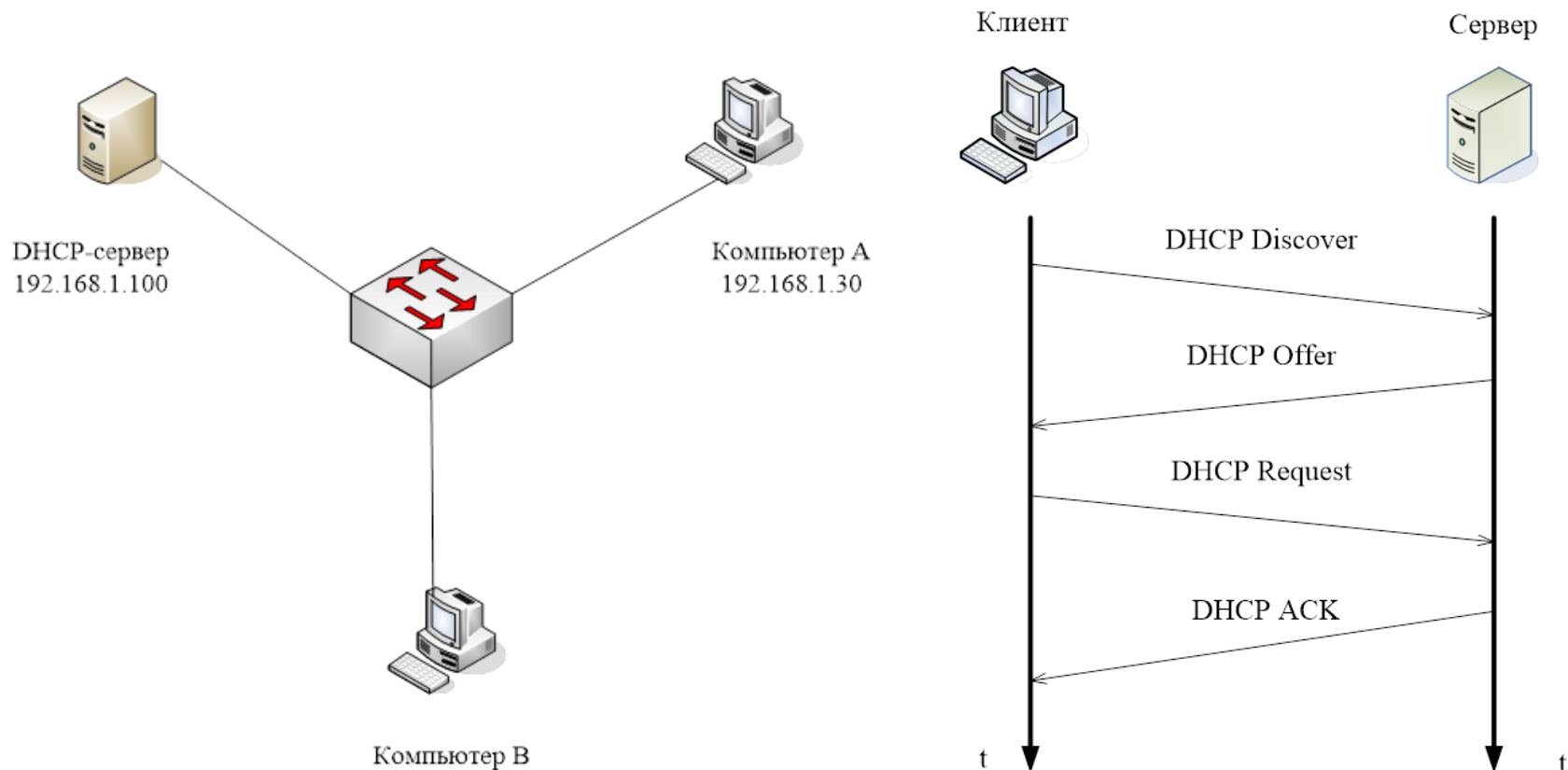
com — commercial (коммерческие)
edu — educational (образовательные)
gov — government (правительственные)
mil — military (военные)
net — network (организации,
обеспечивающие работу сети)
org — organization (некоммерческие
организации)

ro — Romania (Румыния)
ru — Russia (Россия)
si — Slovenia (Словения)
sk — Slovak Republic (Словакия)



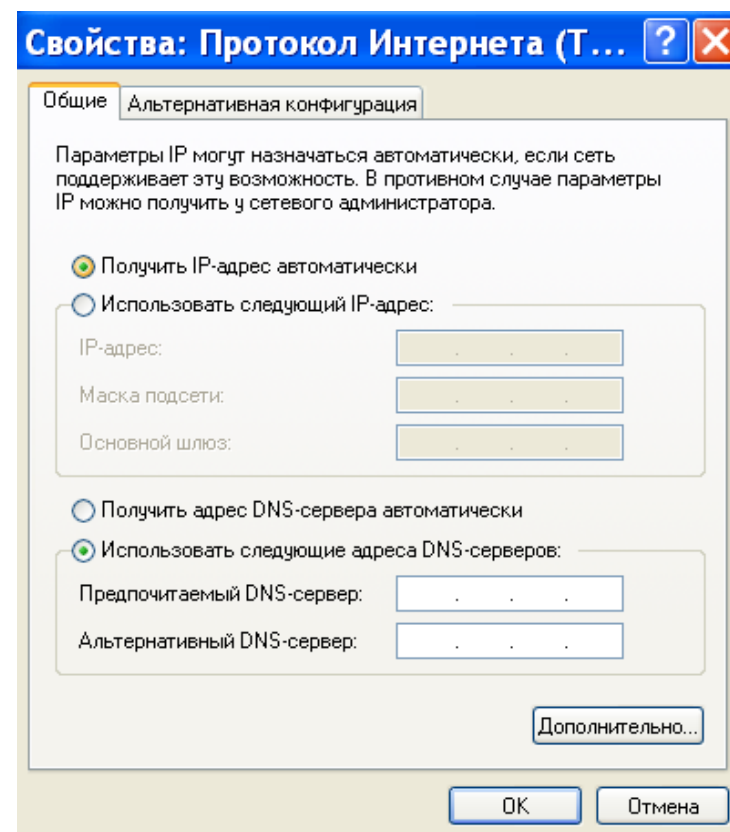
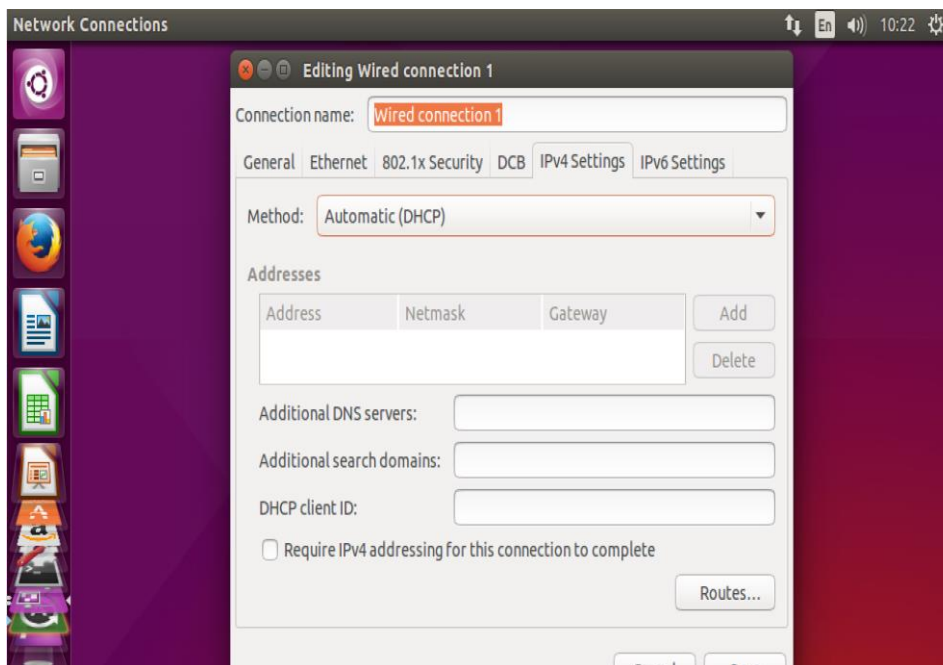
2. Протокол DHCP

Dynamic Host Configuration Protocol (DHCP) – протокол динамического конфигурирования хостов.





Автоматическое получение сетевых настроек узлами под управлением ОС Windows и Linux





3. Технология NAT

Network Address Translation (NAT) – трансляция сетевых адресов.

Причины разработки NAT:

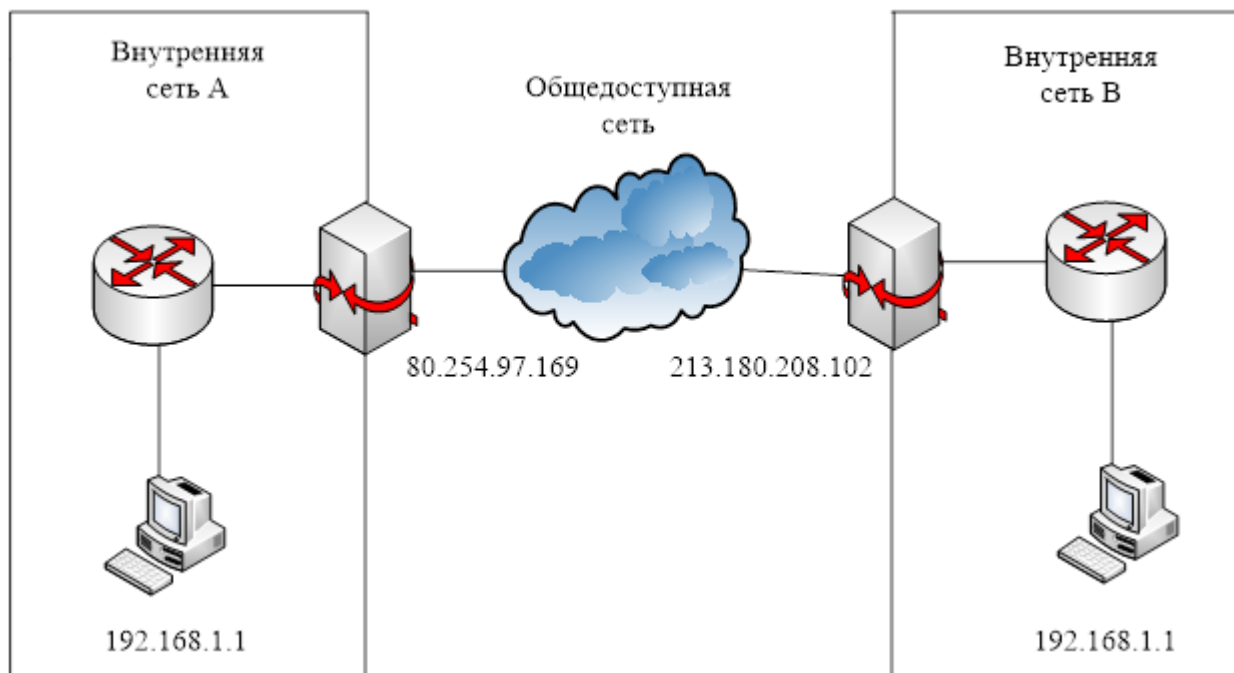
1. Дефицит IP-адресов четвертой версии.
2. Необходимость повышения безопасности корпоративных сетей.

Частные IP-адреса:

- 10.0.0.0 – блок адресов класса А;
- 172.16.0.0 – 173.31.0.0 – блок адресов класса В;
- 192.168.0.0 – 192.168.255.0 – блок адресов класса С.



Статический NAT



Соответствие частных и общедоступных адресов сети А

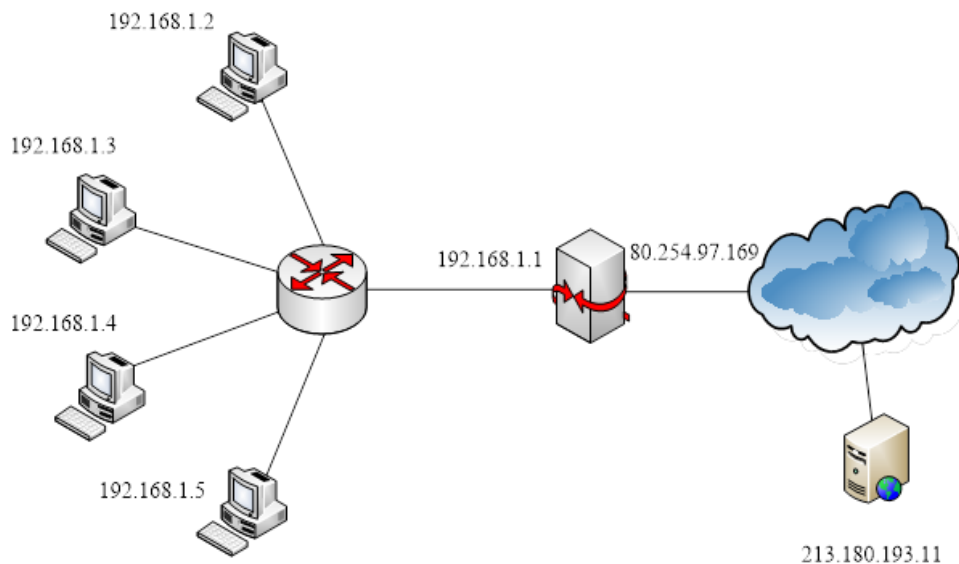
Частный адрес	Общедоступный адрес
192.168.1.1	80.254.97.169

Соответствие частных и общедоступных адресов сети В

Частный адрес	Общедоступный адрес
192.168.1.1	213.180.208.102



Динамический NAT



Соответствие адресов и номеров портов

Частный адрес	Порт	Общедоступный адрес	Назначенный порт
192.168.1.2	8080	80.254.97.169	61001
192.168.1.3	8080	80.254.97.169	61002
192.168.1.4	8080	80.254.97.169	61003
192.168.1.5	8080	80.254.97.169	61004



Лекция 7

Защита сетевых устройств от несанкционированного доступа

ВОПРОСЫ:

1. Защита консольного доступа.
2. Защита удаленного доступа.
3. Использование AAA-сервера для защиты удаленного доступа.
4. Конфигурирование защищенного доступа к сетевому оборудованию.



1. Защита консольного доступа

Доступ к устройству через консоль



- Между последовательным портом (COM) и консольным интерфейсом маршрутизатора/коммутатора установлено физическое соединение.



Защита перехода в привилегированный режим

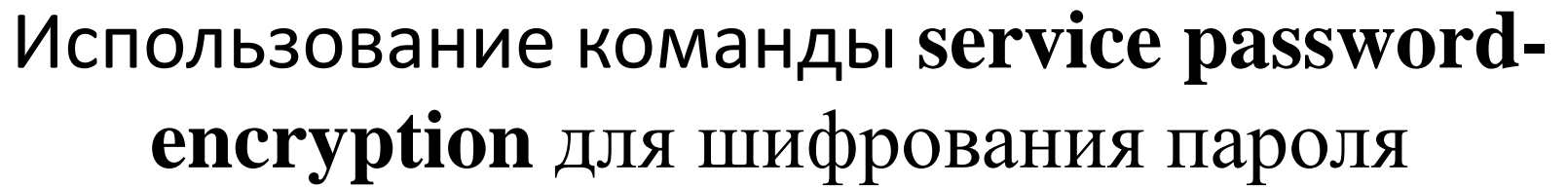
Установка паролей:

R1(config)#enable password <пароль>

R1(config)#enable secret <пароль>

```
Router#show running-config
Building configuration...

Current configuration : 498 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password manin
!
!
```



Просмотр зашифрованного пароля

Пример расшифровки пароля



Использование пароля **enable secret** (алгоритм MD5)

IOS Command Line Interface

```
Current configuration : 523 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$vsQBGz21EfTKsgVkFgb1W.
!
!
!
!
!
!
!
!
--More-- |
```



Использование пароля **enable secret** (алгоритмы SHA)

Синтаксис команды Enable Algorithm Type

Router(config)#

```
enable algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

Ключевое слово алгоритма

Описание

md5	Тип 5; выбирает алгоритм дайджеста сообщения 5 (MD5) в качестве алгоритма хеширования.
scrypt	Тип 9; выбирает scrypt в качестве алгоритма хеширования.
sha256	Тип 8; выбирает функцию формирования ключей на основе пароля 2 (PBKDF2) с защищенным алгоритмом хеширования, 256 бит (SHA-256) в качестве алгоритма хеширования.



Защита пользовательского режима

Для защиты пользовательского режима используется аутентификация по **учетным записям пользователей.**

Для хранения учетных записей используется два подхода:

1. Хранение в локальной базе непосредственно на устройстве.
2. Хранение на специализированном сервере (AAA-сервере).

По умолчанию в устройстве Cisco настроены три уровня:

1. Уровень 0. Пользователь с этим уровнем может выполнять минимальный набор команд. На практике используется крайне редко.
2. Уровень 1. Соответствует пользовательскому режиму, то есть пользователь с этим уровнем может выполнять все команды, доступные в пользовательском режиме.
3. Уровень 15. Соответствует привилегированному режиму, то есть пользователь с этим уровнем может выполнять все команды, доступные в привилегированном режиме.



Создание учетных записей пользователей в локальной базе

Команда создания учетной записи пользователя:

Router1(config)#username <логин> privilege <уровень> password/secret <пароль>

Указание разрешенных команд для пользователей уровней 2 – 14:

Router1(config)#privilege exec level <уровень> <команда>

Создание пароля на доступ к командам уровня:

Router1(config)# enable secret level <уровень> <пароль>



Пример создания локальной базы пользователей

Условия:

В организации имеется три администратора (admin1, admin2 и admin3). Admin1 является главным, ему доступны все команды (уровень 15). Admin2 имеет доступ к командам **show running-config** и **ping**, admin3 – к командам **show ip route**, **ping** и **traceroute**.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#username admin1 privilege 15 secret admin1
Router1(config)#username admin2 privilege 2 secret admin2
Router1(config)#privilege exec level 2 show running-config
Router1(config)#privilege exec level 2 ping
Router1(config)#username admin3 privilege 3 secret admin3
Router1(config)#privilege exec level 3 show ip route
Router1(config)#privilege exec level 3 ping
Router1(config)#privilege exec level 3 traceroute
Router1(config)#^Z
Router1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router1(config)#line console 0
Router1(config-line)#login local
Router1(config-line)#
```



Реализация аутентификации по локальной базе

```
Username:
Username: admin2
Password:

Router1#show ip route
^
% Invalid input detected at '^' marker.

Router1#show running-config
Building configuration...

Current configuration : 970 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router1
!
!
!
!
!
!
!
username admin1 privilege 15 secret 5 $1$mERr$7n6je7c9FKvO.o.40Rj1Q0
username admin2 privilege 2 secret 5 $1$mERr$4CFVt/60iQmc.ia/CrCAa/
username admin3 privilege 3 secret 5 $1$mERr$JpU75fgWPP7c43kksZEKc1
!
--More--
```



Использование функции AAA (Authentication, Authorization and Accounting)

Включение функции AAA:

Router1(config)#aaa new-model

Настройка аутентификации:

Router1(config)#aaa authentication login <method-list> local



2. Защита удаленного доступа

Применение Telnet





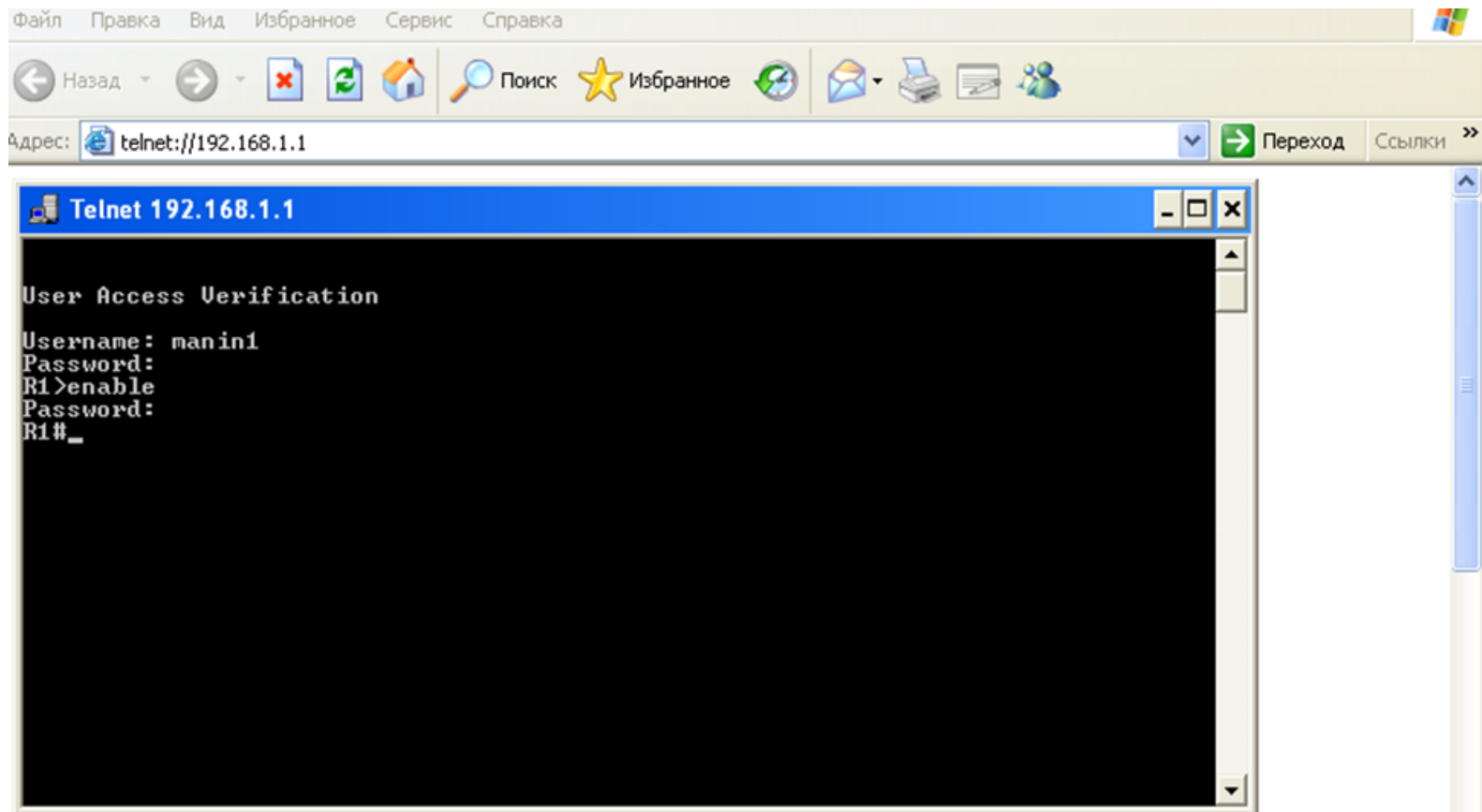
Пример конфигурирования защищенного доступа по протоколу Telnet

```
R1
Mar  1 00:03:53.315: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Mar  1 00:03:54.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
1(config-if)#enable secret floor1
1(config)#userssme manin1 privi
1(config)#userssme manin1 privile
1(config)#userssme manin1 privilege
1(config)#userssme manin1 privilege 1 secret 1234
1(config)#^
Invalid input detected at '^' marker.

1(config)#username manin1 privilege 1 secret 1234
1(config)#line vty 0 4
1(config-line)#login local
1(config-line)#exit
1(config)#ip dhcp pool 1
1(dhcp-config)#net
1(dhcp-config)#netw
1(dhcp-config)#network 192.168.1.0
1(dhcp-config)#def
1(dhcp-config)#default-router 192.168.1.1
1(dhcp-config)#^Z
1#
Mar  1 00:07:04.111: %SYS-5-CONFIG_I: Configured from console by console
1#
```



Удаленный доступ по протоколу Telnet





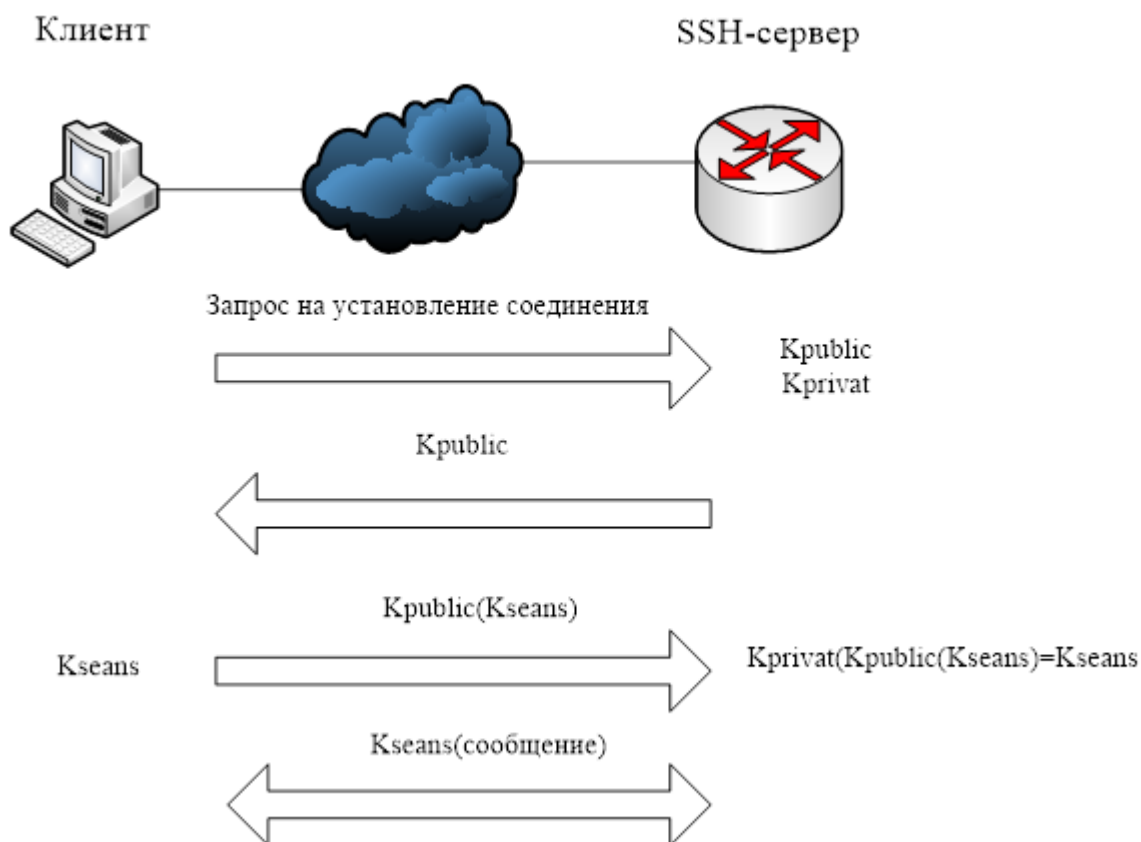
Анализ трафика, передаваемого по протоколу Telnet

Wireshark · Follow TCP Stream

```
.....!.."..'.....#.....P.....  
  
User Access Verification  
  
Username: .....xterm-256color.... ..!..!....."..'.....#mmaanniinn11  
.  
Password: 1234  
.  
R1>eennaabblllee  
.  
Password: floor1  
.  
R1#
```

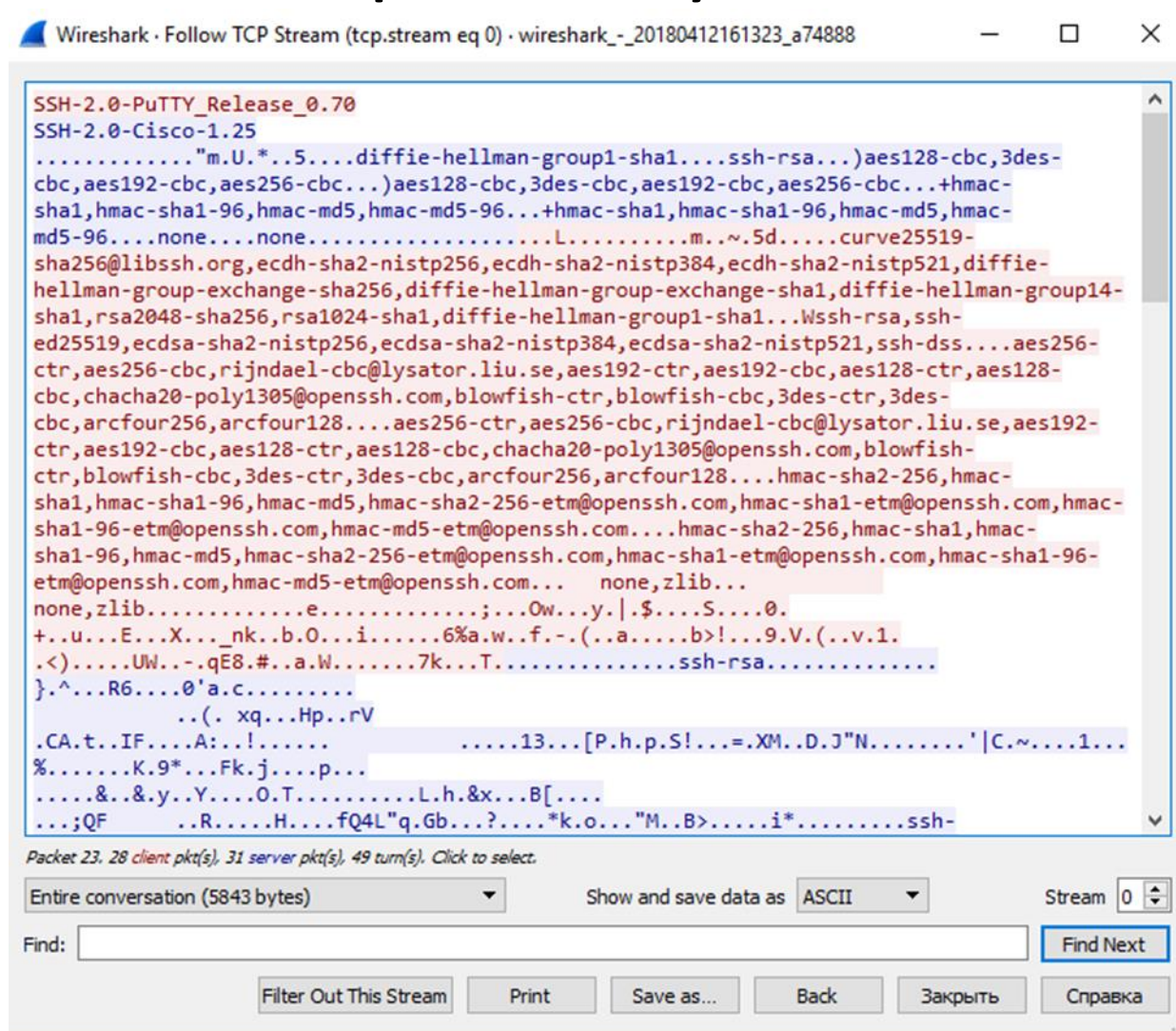


Установление соединения в протоколе SSH





Анализ трафика, передаваемого по протоколу SSH





Независимо от используемого протокола удаленного доступа сам доступ организуется с использованием виртуального интерфейса **vty**.

Без использования AAA:

```
Router1(config)#line vty 0 4
```

```
Router1(config-line)#login local
```

С использованием AAA:

```
Router1(config)#aaa new-model
```

```
Router1(config)#aaa authentication login default local
```



Конфигурирование маршрутизатора как SSH-сервера

ip domain <имя> - указание имени домена, к которому относится маршрутизатор.

crypto key generate rsa - генерирует RSA-ключ, после чего Cisco IOS просит ввести длину используемого ключа.

transport input ssh - указание маршрутизатору, что для удаленного входа должен использоваться только протокол SSH

```
R1
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain name domain.local
R1(config)#hostname R1_ssh
R1_ssh(config)#crypto key generate rsa
The name for the keys will be: R1_ssh.domain.local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1_ssh(config)#
*Mar  1 01:13:38.311: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1_ssh(config)#line vty 0 4
R1_ssh(config-line)#transport input ssh
```



Дополнительные возможности защиты при использовании SSH

R1(config-line)#exec-timeout 5 0 – величина тайм-аута сессии (5 мин. 0 сек.);

R1(config)#ip ssh time-out 15 – ограничение времени ввода логина и пароля;

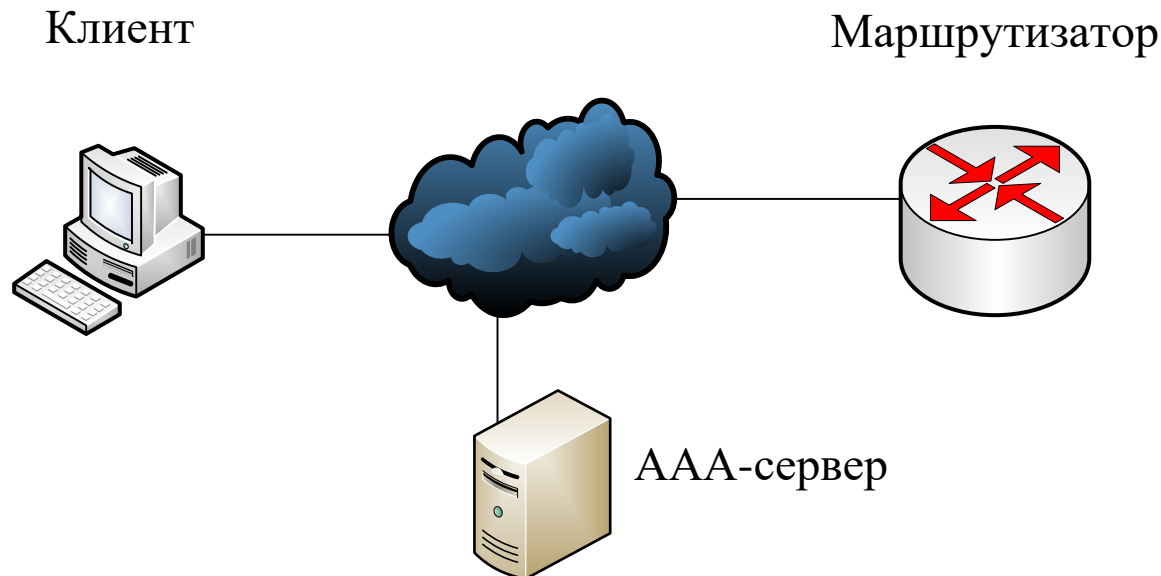
R1(config-line)#transport input ssh – разрешение удаленного входа только по протоколу SSH (Telnet работать не будет);

R1(config)#login delay 5 – задание интервала между повторными вводами пароля;

R1(config)#login block-for 60 attempts 3 within 30 – блокировка входа на 60 секунд, если в течение 30 секунд было 3 неудачных попытки входа.



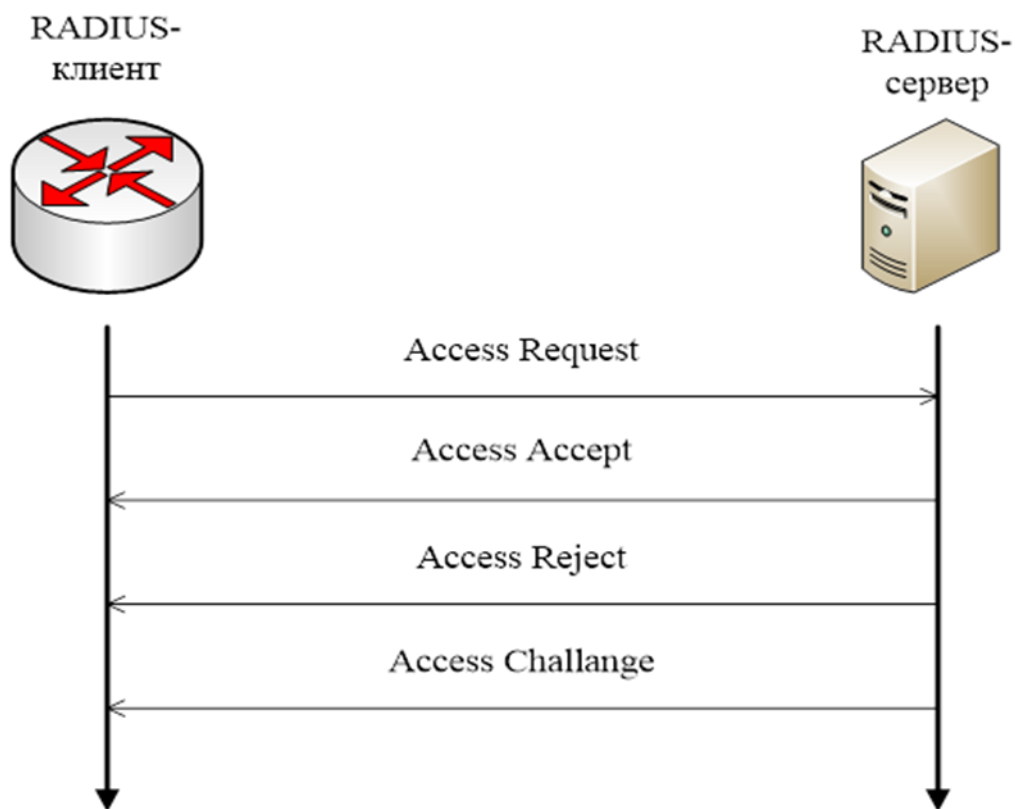
3. Использование AAA-сервера для защиты удаленного доступа



1. Пользователь пытается подключиться к сетевому устройству, вводя свои учетные данные (логин, пароль).
2. Маршрутизатор обращается к AAA-серверу и передает ему учетные данные пользователя.
3. AAA-сервер отыскивает в своей базе соответствующую учетную запись (Authentication) и определяет уровень привилегий (Authorization).
4. AAA-сервер пересылает маршрутизатору соответствующую информацию (успешность аутентификации, уровень привилегий).
5. AAA-сервер фиксирует данное событие (Accounting)
6. Маршрутизатор открывает доступ пользователя к оборудованию с учетом уровня привилегий.



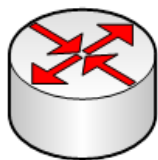
Протокол RADIUS (Remote Authentication in Dial-In User Service) передает данные в составе UDP-сегментов (порты 1812 и 1813) и работает по сценарию клиент-сервер.



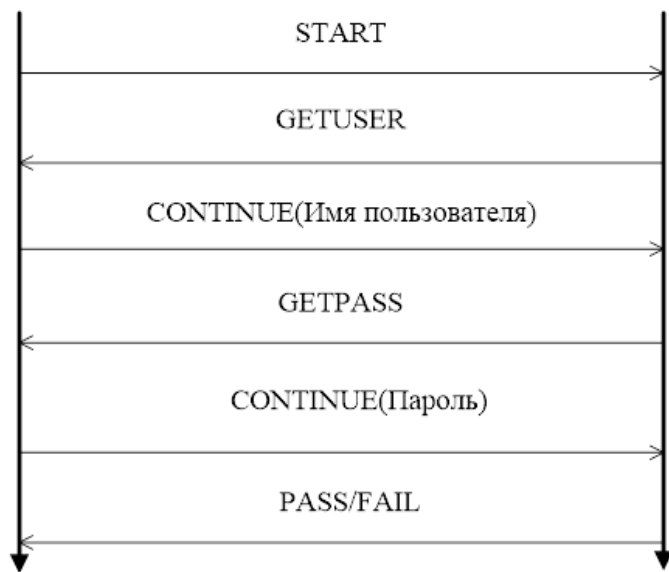
При передаче шифруется **только** пароль. Процессы аутентификации и авторизации логически не отделены друг от друга.



TACACS+
клиент



TACACS+
сервер

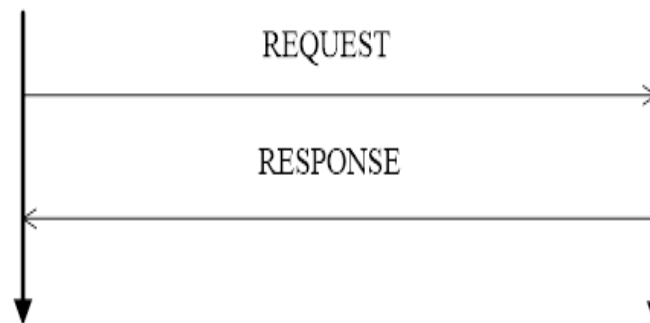


Аутентификация в
протоколе TACACS+

TACACS+
клиент



TACACS+
сервер



Авторизация в
протоколе TACACS+



4. Конфигурирование защищенного доступа к сетевому оборудованию

Аутентификация

R1(config)#username <имя> privilege 15 secret <пароль> - создание локальной учетной записи на случай недоступности AAA-сервера

R1(config)#enable secret <пароль> - создание пароля для входа в привилегированный режим

R1(config)#aaa new-model – включение режима AAA

R1(config)#tacacs-server host <адрес> - указание IP-адреса AAA-сервера

R1(config)#tacacs-server key <ключ> - указание ключа шифрования

R1(config)#aaa authentication login default group tacacs+ local – указание метода аутентификации



Пример конфигурирования маршрутизатора

```
R1
*Mar 1 00:00:04.427: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar 1 00:00:04.899: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 00:00:04.971: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
*Mar 1 00:00:05.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Mar 1 00:00:05.971: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip addr 10.6.2.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:01:59.455: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:02:00.455: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#ip dhcp pool 1
R1(dhcp-config)#net
R1(dhcp-config)#netw
R1(dhcp-config)#network 10.6.20.0 255.255.255.0
R1(dhcp-config)#def
R1(dhcp-config)#default-router 10.6.20.1
R1(dhcp-config)#ex
R1(config)#username manin2 pri
R1(config)#username manin2 privilege 15 secret 1234
R1(config)#enable secret cisco
R1(config)#aaa new-model
R1(config)#tacacs-server host 10.6.20.10
R1(config)#tacacs-server key tacgui
R1(config)#aaa authen
R1(config)#aaa authentication login default group tacacs+ local
R1(config)#^Z
R1#
*Mar 1 00:21:50.367: %SYS-5-CONFIG_I: Configured from console by console
R1#wr mem
Building configuration...
[OK]
R1#
```



```
Telnet 10.6.20.1

Unauthorized access is prohibited?
Username: manin1
Password:
Today is a perfect day! Have a nice day!

R1>enable
Password:
R1#_
```

Подключение с использованием AAA-сервера

```
Telnet 10.6.20.1

User Access Verification

Username: manin1
Password:

% Authentication failed

Username: manin2
Password:

R1>enable
Password:
R1#
```

Подключение по локальной базе (AAA-сервер недоступен)



Лекция 8

Межсетевое экранирование

Вопросы:

1. Определение и классификация межсетевых экранов.
2. Межсетевое экранирование с пакетной фильтрацией.
3. Межсетевое экранирование с сохранением состояний.
4. Zone-Based Policy Firewall (ZBFW)



1. Определение и классификация межсетевых экранов

Определение, данное в «Руководящем документе. Межсетевые экраны»
Гостехкомиссии при Президенте РФ

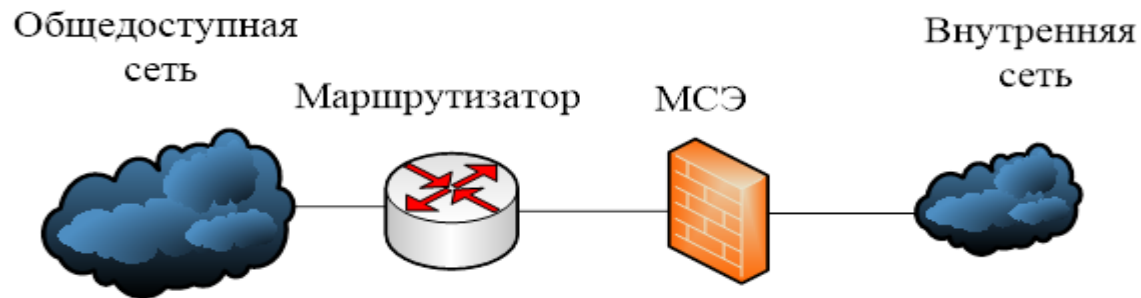
Межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т. е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе.

Функции, выполняемые межсетевым экраном:

1. Ограничение доступа во внутреннюю сеть из общедоступной сети.
2. Контроль и регулирование доступа пользователей внутренней сети к ресурсам общедоступной сети.
3. Ограничение доступа пользователей внутренней сети к критическим ресурсам.



Схемы подключения межсетевых экранов





Схемы подключения межсетевых экранов



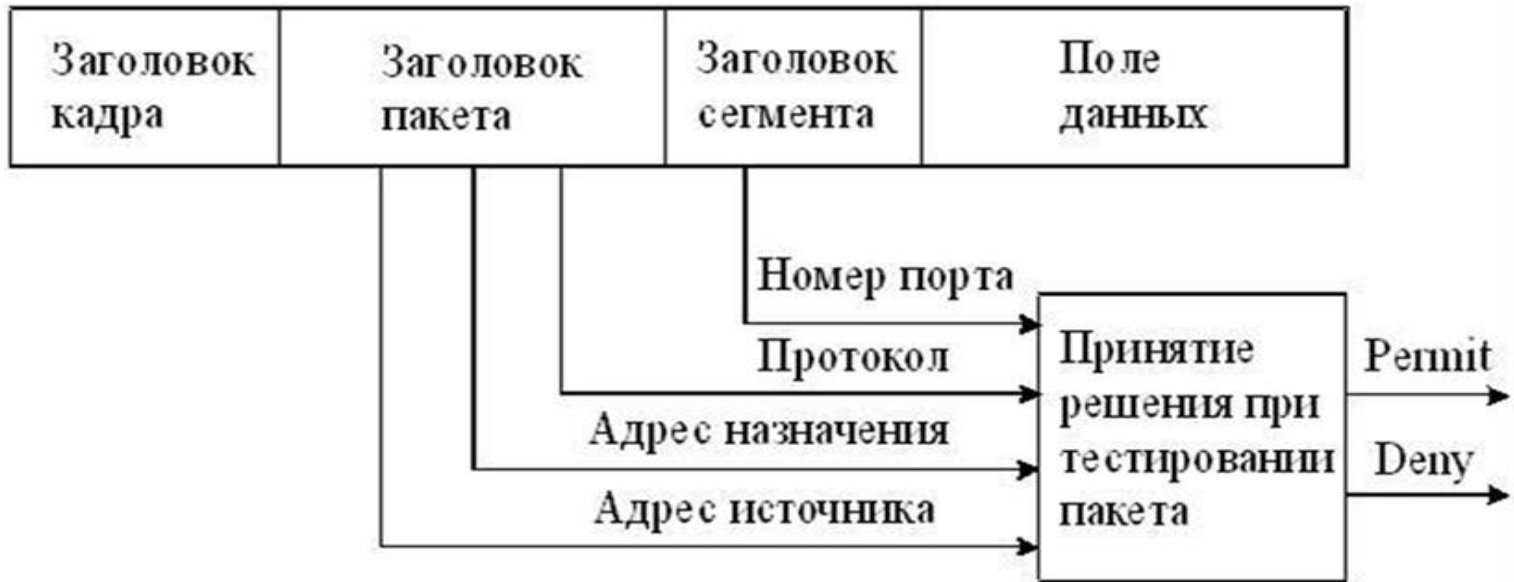
Схема с двумя МСЭ



Подключение МСЭ с интерфейсом для DMZ



2. Межсетевое экранирование с пакетной фильтрацией





Классификация списков доступа

Стандартные - анализируется сетевой адрес источника.

Расширенные – анализируются IP-адрес источника, IP-адрес назначения, поле протокола в заголовке пакета сетевого уровня и номер порта в заголовке транспортного уровня.

Диапазон номеров	Тип списка доступа
1-99	IP standard access-list
100-199	IP extended access-list
1300-1999	IP standard access-list (extended range)
2000-2699	IP extended access-list (extended range)
600-699	Appletalk access-list
800-899	IPX standard access-list
900-999	IPX extended access-list



Конфигурирование списков доступа

Этапы конфигурирования:

1. Создание ACL в режиме глобального конфигурирования.
2. Привязка ACL к интерфейсу в режиме конфигурирования интерфейса.

Router(config)#access-list {№} {permit / deny} {адрес источника} – создание стандартного ACL

Router(config-if){протокол} access-group {номер} {in / out} – привязка ACL к интерфейсу

Router(config)#access-list {№} {permit / deny} {трансп.протокол} {адр.ист} {адр.пол.} eq {№ порта или название прикладного протокола} – создание расширенного ACL

Правила назначения прикладных протоколов

Обозначение	Действие
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

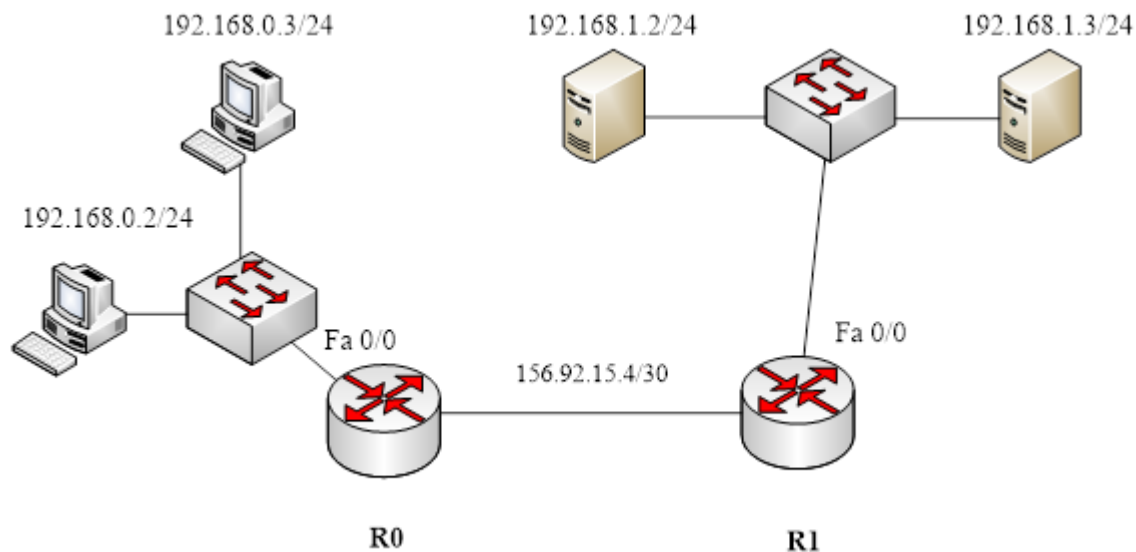


Распространенные прикладные протоколы и соответствующие им стандартные номера портов

Номер порта	Транспортный протокол	Прикладной протокол	Ключевое слово в команде access-list
20	TCP	FTP	data ftp_data
21	TCP	Управление сервером FTP	ftp
22	TCP	SSH	
23	TCP	Telnet	telnet
25	TCP	SMTP	Smtп
53	UDP, TCP	DNS	Domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	Tftp
80, 8080	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	Snmp



Пример (стандартный список)



Задача: к серверу, находящемуся в подсети 192.168.1.0/24 по адресу 192.168.1.2/24, доступ из подсети 192.168.0.0/24 разрешен только компьютеру 192.168.0.2/24.

На маршрутизаторе R1:

```
Router1(config)#access-list 10 permit 192.168.0.2
```

```
Router1(config)#interface fa 0/0
```

```
Router1(config-if)#ip access-group 10 out
```

Задача: к серверу, находящемуся в подсети 192.168.1.0/24 по адресу 192.168.1.2/24, доступ из подсети 192.168.0.0/24 разрешен всем компьютерам.

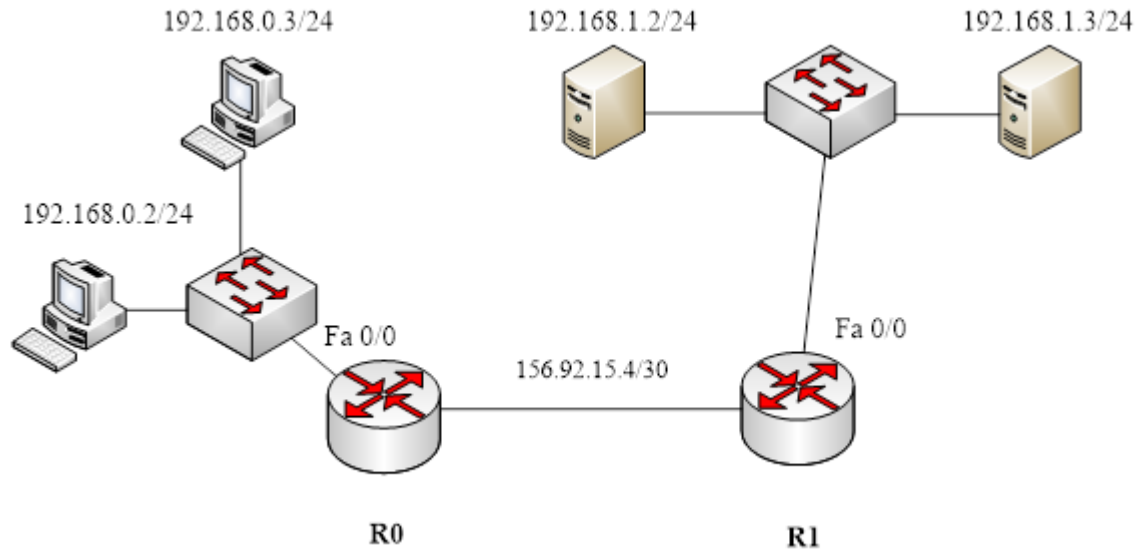
```
Router1(config)#access-list 10 permit 192.168.0.0 0.0.0.255
```

```
Router1(config)#interface fa 0/0
```

```
Router1(config-if)#ip access-group 10 out
```



Пример (стандартный список)



Задача: к тому же серверу необходимо обеспечить доступ всем компьютерам, кроме одного, имеющего адрес 192.168.0.15.

Router1(config)#access-list 11 deny host 192.168.0.15

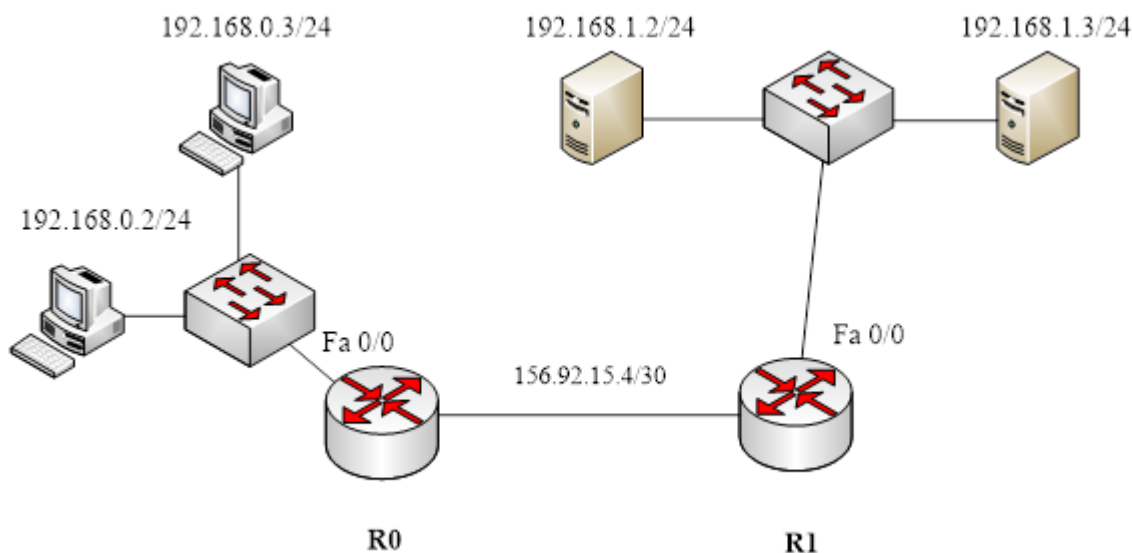
Router1(config)#access-list 11 permit any

Router1(config)#interface fa 0/0

Router1(config-if)#ip access-group 11 out



Пример (расширенный список)



Задача:

- компьютеру 192.168.0.2/24 необходимо предоставить доступ к web-серверу с адресом 192.168.1.2 по протоколу WWW;
- всем компьютерам подсети 192.168.0.0/24 необходимо предоставить доступ к FTP-серверу с адресом 192.168.1.3 по протоколу FTP.

```
Router1(config)#access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq www
Router1(config)#access-list 110 permit tcp 192.168.0.0 0.0.0.255 host 192.168.1.3 eq ftp
Router1(config)#interface fa 0/0
Router1(config-if)#ip access-group 110 out
```



Именованные списки доступа

Удобство использования именованных списков доступа заключается в том, что названию списка можно придать определенный смысл (INTERNET, ADMIN, FTP, и т.д.). Так как именованный список не имеет номера, который однозначно определяет его вид, при создании такого списка необходимо явно указать, какой именно список создается – стандартный или расширенный.

```
ip access-list <standard/extended> <имя>
```

```
<правило 1>
```

```
<правило 2>
```

```
<правило n>
```



3. Межсетевое экранирование с сохранением состояний

При запросе на установление соединения (например, ТСР-сессии) маршрутизатор запоминает эту сессию и при поступлении извне пакета сверяет его со всеми текущими сессиями. Если принятый извне пакет относится к какой-либо текущей сессии, он продвигается во внутреннюю сеть, в противном случае – отбрасывается.

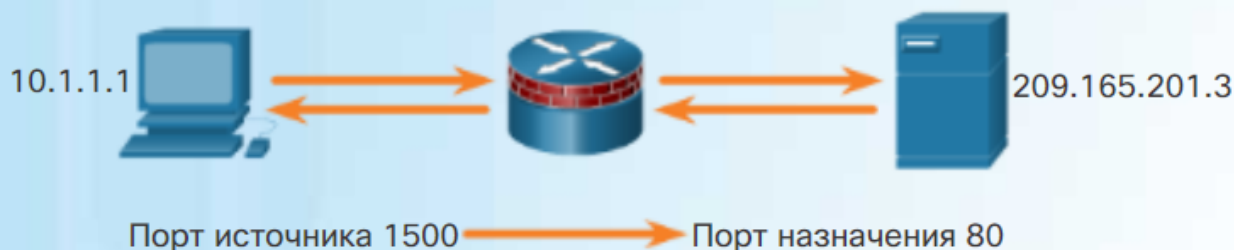
```
R1(config)#ip inspect name <имя правила> <название протокола>
```

```
R1(config)#int fa0/0
```

```
R1(config-if)#ip inspect <имя правила> <in/out>
```



Принцип работы межсетевого экрана с сохранением состояний



Внутри ACL (исходящий трафик)

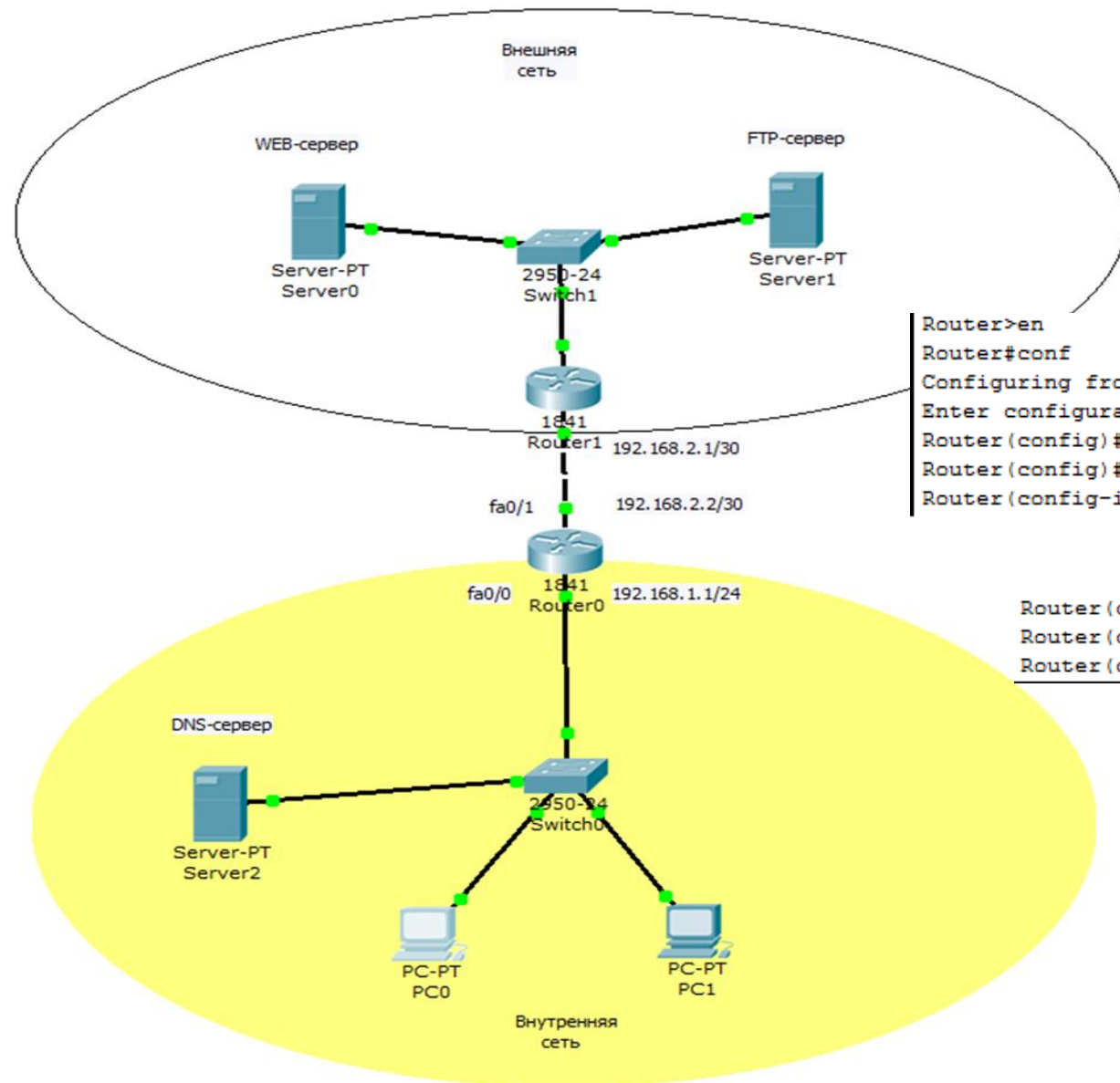
```
permit 10.1.1.0.0.0.0.255 any
```

Вне ACL (входящий трафик)

```
Dynamic: permit tcp host 209.165.201.3 eq  
80 host 10.1.1.1 eq 1500
```



Пример

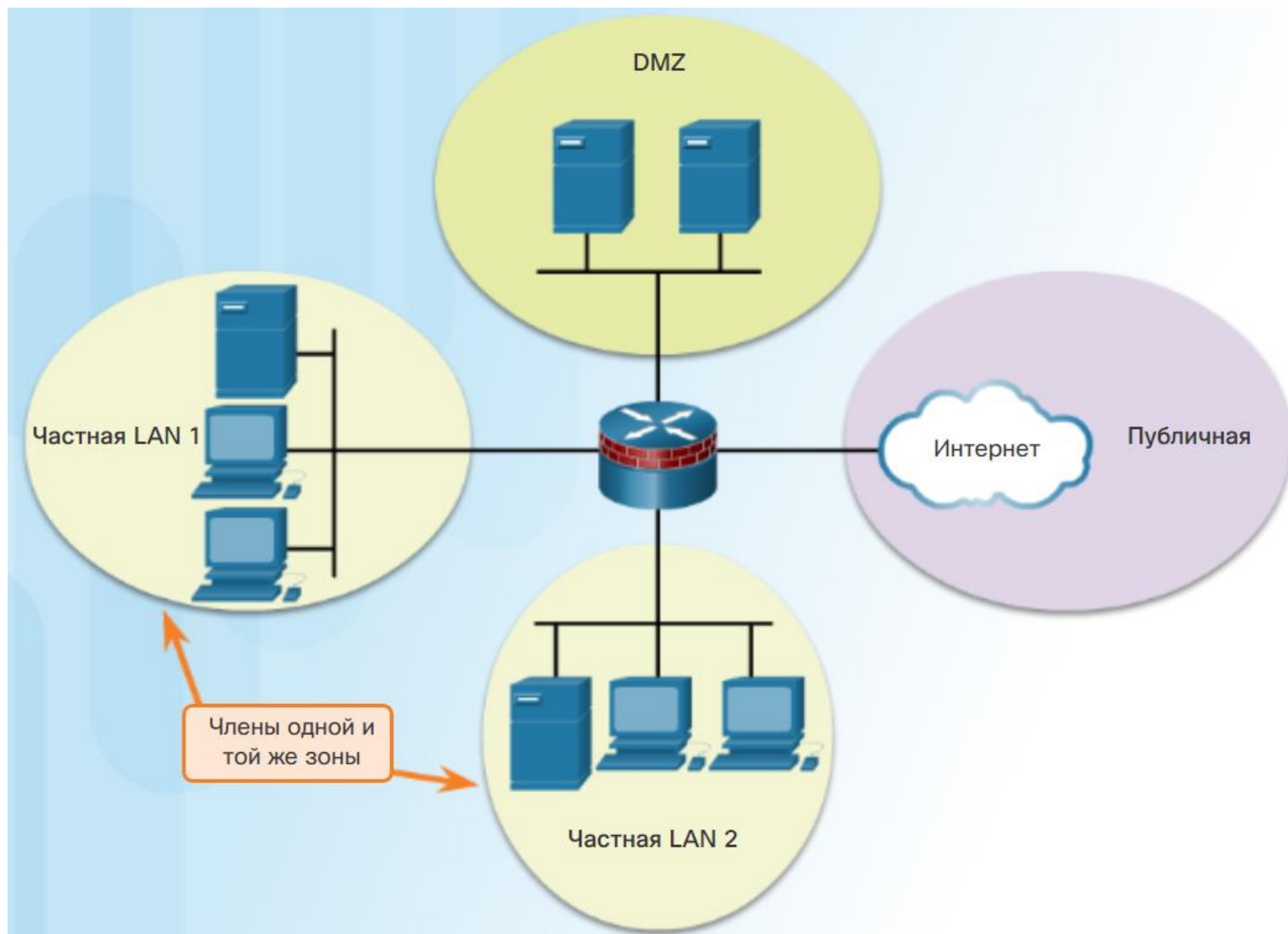


```
Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip inspect name HTTP http
Router(config)#int fa0/0
Router(config-if)#ip inspect HTTP in
```

```
Router(config)#ip access-list ex FRW
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#
```



4. Zone-Based Policy Firewall (ZBFW)





Конфигурирование ZBFW

Этапы конфигурирования:

1. Определение зон (zone).
2. Определение пар зон (zone pair).
3. Выделение интересующего трафика (class map).
4. Определение политики (действий) в отношении выбранного трафика (policy map).
5. Применение политики к парам зон (service policy).
6. Привязка интерфейсов маршрутизатора к зонам.

В большинстве случаев сеть делится, как минимум, на три зоны:

- внутренняя зона, где расположены пользователи (inside);
- внешняя зона (Интернет – outside);
- демилитаризованная зона, где расположены серверы, к которым должен быть обеспечен доступ извне (dmz).



Команды конфигурирования

zone security <имя зоны> - создание зоны безопасности.

zone-pair security <имя пары> source <имя зоны> destination <имя зоны> - создание пары зон.

class-map type inspect match-all/match-any <имя class-map> - создание class map.

Сортировка трафика:

- **access-group** - список доступа, который может фильтровать трафик на основании IP адреса и порта источника и получателя;
- **protocol** - это протоколы уровня 4 (TCP, UDP, ICMP), а также прикладные сервисы, такие как HTTP, SMTP, DNS, и т.д.;
- **class-map** - подчиненный класс, который предоставляет дополнительные критерии соответствия;
- **not** - определяет, что любой трафик, который не соответствует указанному сервису или протоколу, или листу доступа, будет выбран в данном class-map.



Команды конфигурирования

policy-map type inspect <имя policy-map> - создание политики.

class type inspect <имя class-map> - привязка policy map к class map.

Настраиваемые действия:

Drop – Трафик, обрабатываемый этим действием, отбрасывается и никакого уведомления на удаленный хост не высылается.

Pass – Пропускает трафик, не включая инспекцию протокола.

Inspect - Включает динамическую инспекцию для трафика, который проходит от зоны источника к зоне приемника, и автоматически разрешает обратный трафик.

service-policy type inspect <имя policy-map > - применение политики к парам зон.

interface <имя интерфейса> - переход в режим конфигурирования интерфейса.

zone-member security <имя зоны> - привязка интерфейса к зоне.