

СЕТИ и ТЕЛЕКОММУНИКАЦИИ

Лекция №6 Сетевой уровень модели ISO/OSI

Модель OSI и TCP/IP – функции сетевого уровня

Протоколы сетевого уровня

Адресация на сетевом уровне

Маршрутизация. Протоколы маршрутизации

Модель OSI и TCP/IP

Уровни модели OSI	Уровни модели стека TCP/IP	Протоколы стека TCP/IP
<i>Прикладной</i>	<i>Прикладной</i>	<i>FTP, HTTP, SMTP, POP3, IMAP4, Telnet, DNS, DHCP, SNMP и др.</i>
<i>Представительский</i>		
<i>Сеансовый</i>		
<i>Транспортный</i>	<i>Транспортный</i>	<i>TCP, UDP</i>
<i>Сетевой</i>	<i>Межсетевой</i>	<i>ICMP, IGMP, ARP IP</i>
<i>Канальный</i>	<i>Доступ к среде</i>	<i>Ethernet, SLIP, ATM, FR, Wireless Wi-Fi и др.</i>
<i>Физический</i>		

Сетевой уровень позволяет устройствам взаимодействовать с другими устройствами в сети. Обеспечивает логическую адресацию в сети, пакетирование, инкапсуляцию и деинкапсуляцию сегментов, маршрутизацию пакетов.

Протокольный блок данных сетевого уровня называется пакетом.

Модель ТСР/IP

* **Пользователи** создают соединения; * **Программное обеспечение** конвертирует данные пользователей в цифровой формат; * **Драйвера** предоставляют доступ к аппаратному обеспечению и конвертирует данные из цифрового формата в сигналы; * **Аппаратное обеспечение** накладывает сигналы на среду передачи.



* **Сигналы** передаются с использованием аппаратного обеспечения (сетевого оборудования)



Пользователь

Программное
обеспечение
и драйвера
системы

Аппаратное
обеспечение

Прикладной
уровень

Транспортный
уровень

Межсетевой
уровень

Уровень доступа к
среде передачи

Физическая среда
передачи данных

Пользователь

Программное
обеспечение
и драйвера
системы

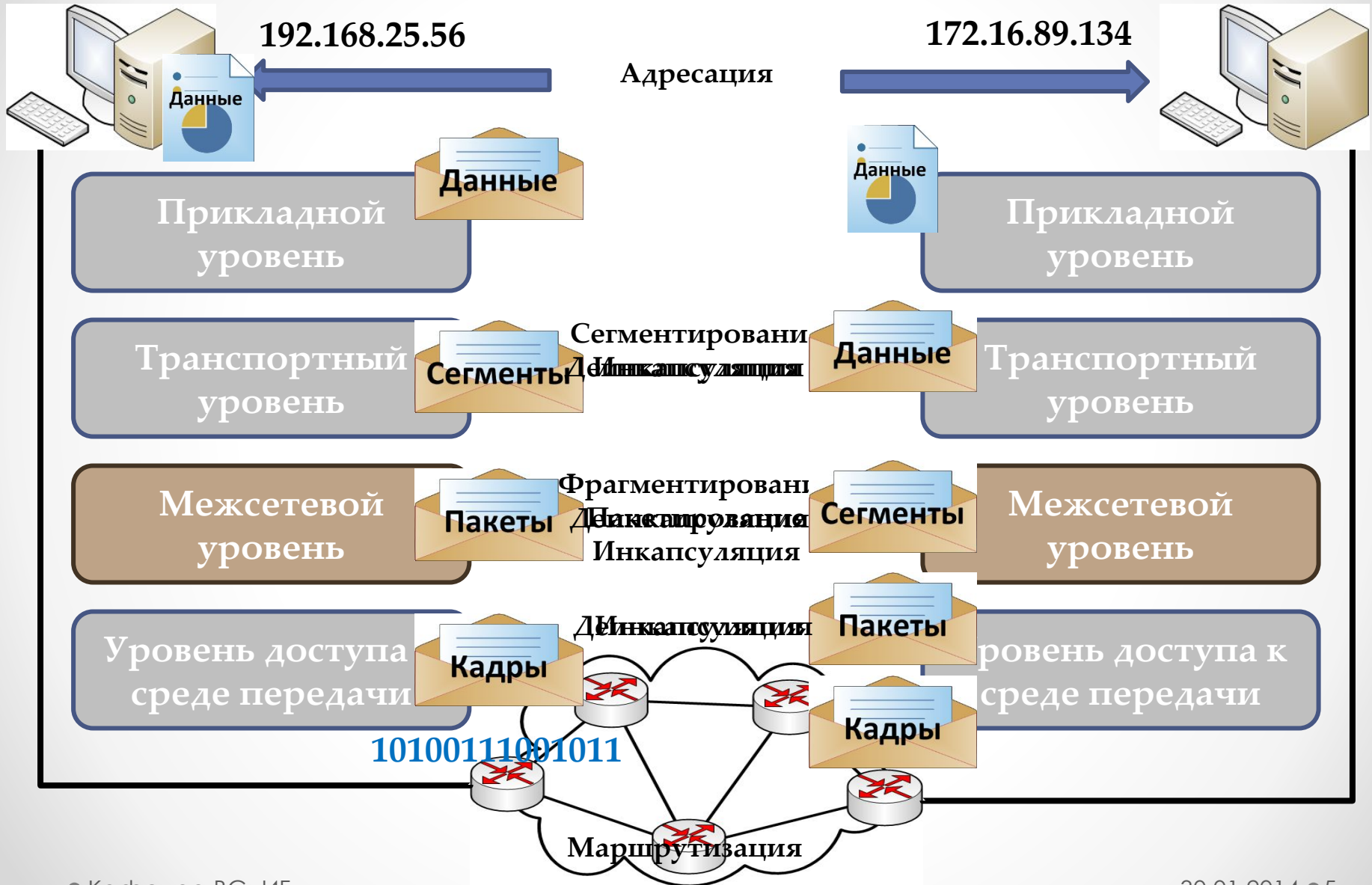
Аппаратное
обеспечение

Функции сетевого уровня

Для информационного обмена в объединенных сетях средства сетевого уровня должны решать следующие задачи:

- обеспечивать инкапсуляцию и деинкапсуляцию данных
- разделение данных на пакеты
- обеспечивать единую систему адресации, не зависящую от сетевой технологии, позволяющую адресовать отдельные сети и узлы
- определять путь (последовательность сетей), по которому должны пройти данные, чтобы достичь получателя
- обеспечивать сквозную передачу данных через сети с разной технологией

Функции сетевого уровня



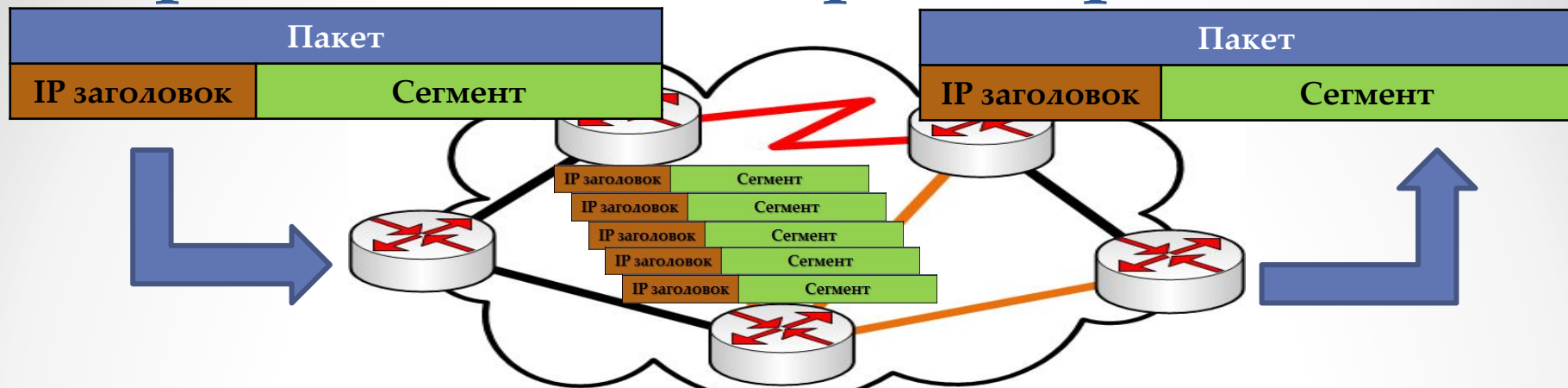
Протоколы сетевого уровня

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

В рамках данного курса мы будем рассматривать протокол IP.

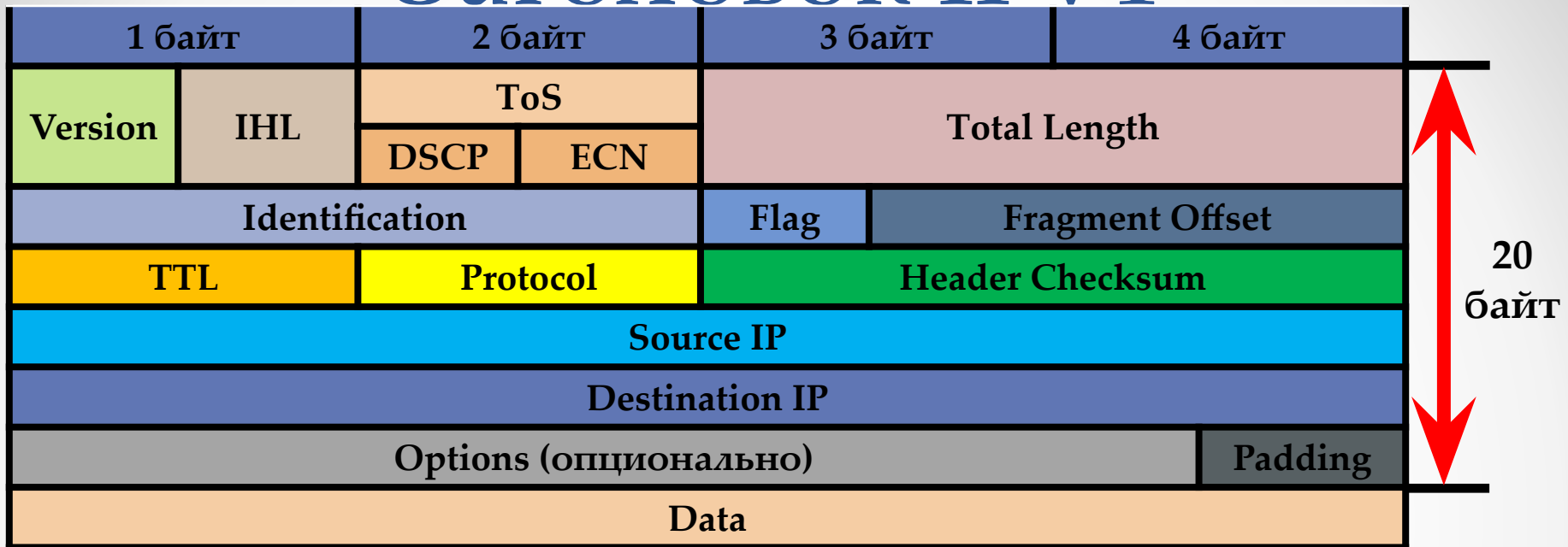
Данный протокол можно сравнить с работой ПОЧТЫ.

Протокол IP (характеристики)



- **Connectionless** – перед отправкой пакетов не устанавливается соединения между конечными устройствами. Отправитель не знает о существовании получателя, о получении им пакета, о возможности прочтения пакета. Получатель не знает когда придет пакет.
- **Best Effort (unreliable)** – не используется подтверждений доставки пакетов, повышая возможности по передаче пакетов. В процессе передачи часть пакетов может потеряться, часть прийти поврежденными, могут прийти в случайном порядке.
- **Media Independent** – независимость от среды передачи данных. IP-пакет может передаваться по различным каналам передачи данных: медь-Ethernet, медь-Serial, оптоволокно, wireless.

Заголовок IPv4



Version – Версия протокола IP (4 или 6); **IHL (Internet Header Length)** – размер заголовка пакета; **Differentiated Services (Type of Service)** – приоритет каждого пакета для реализации QoS; **Total Length** – размер всего пакета (заголовок и данные); **Identification** – уникальный идентификатор фрагмента пакета; **Flag** – фрагментированные пакеты, наличие еще фрагментированных пакетов, запрет фрагментирования пакетов; **Fragment Offset** – смещение фрагмента в пакете относительно начала; **Time to Live** – значение определяющее оставшееся количество хопов; **Protocol** – номер протокола верхнего уровня, инкапсулированного в пакет; **Header Checksum** – контрольная сумма только полей заголовка пакета; **Source Address & Destination Address** – 32-bit значение IP-адреса источника и назначения пакета; **Options** – дополнительные поля пакета, для предоставления доп. услуг; **Padding** – незначащие биты

Адреса IP

Для обмена данными по сети, каждое устройство должно иметь адрес. Изначально под адрес было выделено 32 бита – это широко распространенный на сегодняшний день адрес протокола IPv4.

Но количество устройств все время увеличивается, адресное пространство заканчивается и на смену протоколу IPv4 приходит протокол IPv6 и размер адреса увеличен до 128 бит.



Проблемы нехватки

IP-адресов

На протяжении многих лет, для решения проблем связанных с нехваткой адресов, были выполнены некоторые обновления протокола, а так же разработаны механизмы. Но этого не достаточно и по прежнему остаются не решенными три основные проблемы:

- Недостаток IP-адресов
- Рост таблиц маршрутизации Интернета
- Отсутствие связи любых устройств между собой напрямую (без использования NAT)

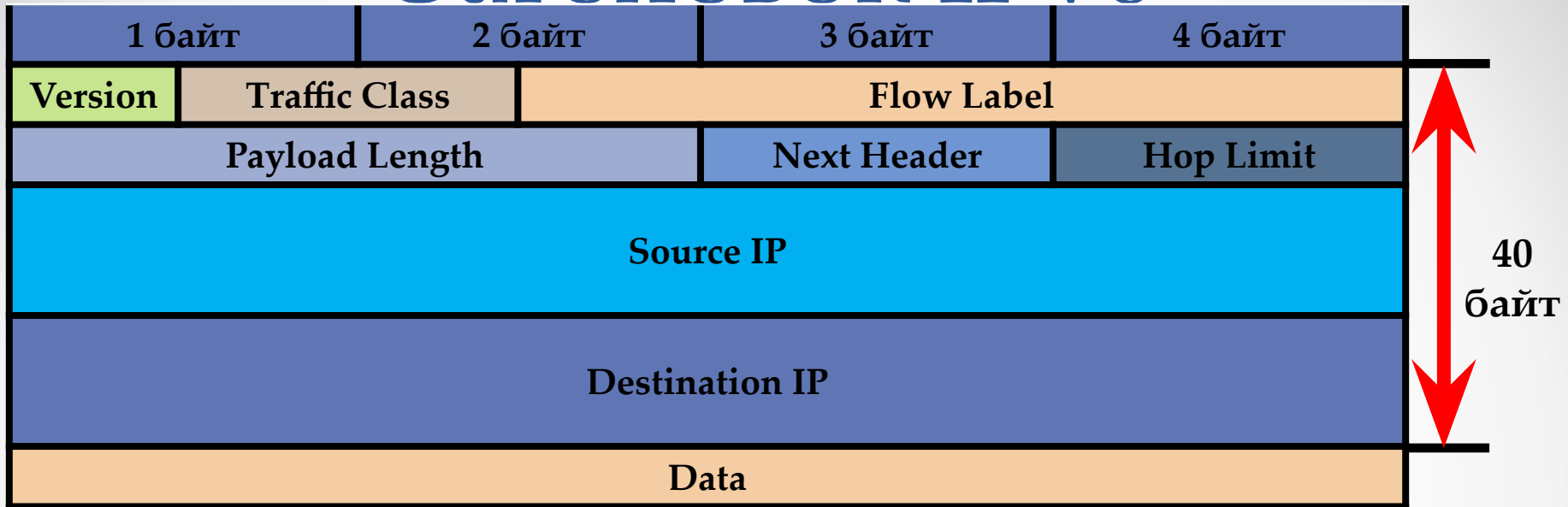
Адресное пространство

Название		Количество нулей
1 тысяча	10^3	1 000
1 миллион	10^6	1 000 000
1 миллиард	10^9	1 000 000 000
	2^{32}	4 294 967 296
1 триллион	10^{12}	1 000 000 000 000
1 квадриллион	10^{15}	1 000 000 000 000 000
1 квинтиллион	10^{18}	1 000 000 000 000 000 000
1 секстиллион	10^{21}	1 000 000 000 000 000 000 000
1 септиллион	10^{24}	1 000 000 000 000 000 000 000 000
1 октиллион	10^{27}	1 000 000 000 000 000 000 000 000 000
1 нониллион	10^{30}	1 000 000 000 000 000 000 000 000 000 000
1 дециллион	10^{33}	1 000 000 000 000 000 000 000 000 000 000 000
1 ундециллион	10^{36}	1 000 000 000 000 000 000 000 000 000 000 000 000
	2^{128}	340 282 366 920 938 463 463 374 607 431 768 211 456

IPv6

- Увеличение адресного пространства до **128 разрядов**, что позволяет забыть о нехватке адресов на неопределенный срок, так как количество адресов соизмеримо с количеством молекул на планете Земля
- Улучшение в маршрутизации и передачи пакетов, в виду изменения заголовка пакета, заголовок стал проще. Так же данный заголовок обеспечивает поддержку расширений в будущем
- Устраняет проблему IPv4 с необходимостью использования технологии NAT
- Комплексная безопасность. В отличии от IPv4 в протоколе IPv6 изначально заложены **механизмы обеспечения безопасных соединений, поддержка аутентификации и конфиденциальности**

Заголовок IPv6



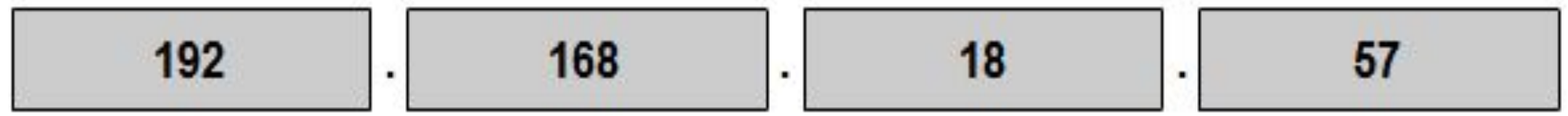
Version – Версия протокола IP (4 или 6); **Traffic Class** – приоритет пакета, аналог поля Type of Service; **Flow Label** – метка потока, служит для упрощения процедуры маршрутизации одного потока пакетов; **Payload Length** – полезный размер данных без учета фиксированного заголовка пакета; **Next Header** – задаёт тип расширенного заголовка, протокол верхнего уровня инкапсулированный в IP пакет; **Hop Limit** – аналог поля Time To Live в IPv4, оставшееся количество хопов; **Source Address & Destination Address** – 128 битный IPv6 адрес отправителя и получателя

IPv4 адрес

← 32 bits →



← 8 bits (Octet) → ← 8 bits (Octet) → ← 8 bits (Octet) → ← 8 bits (Octet) →



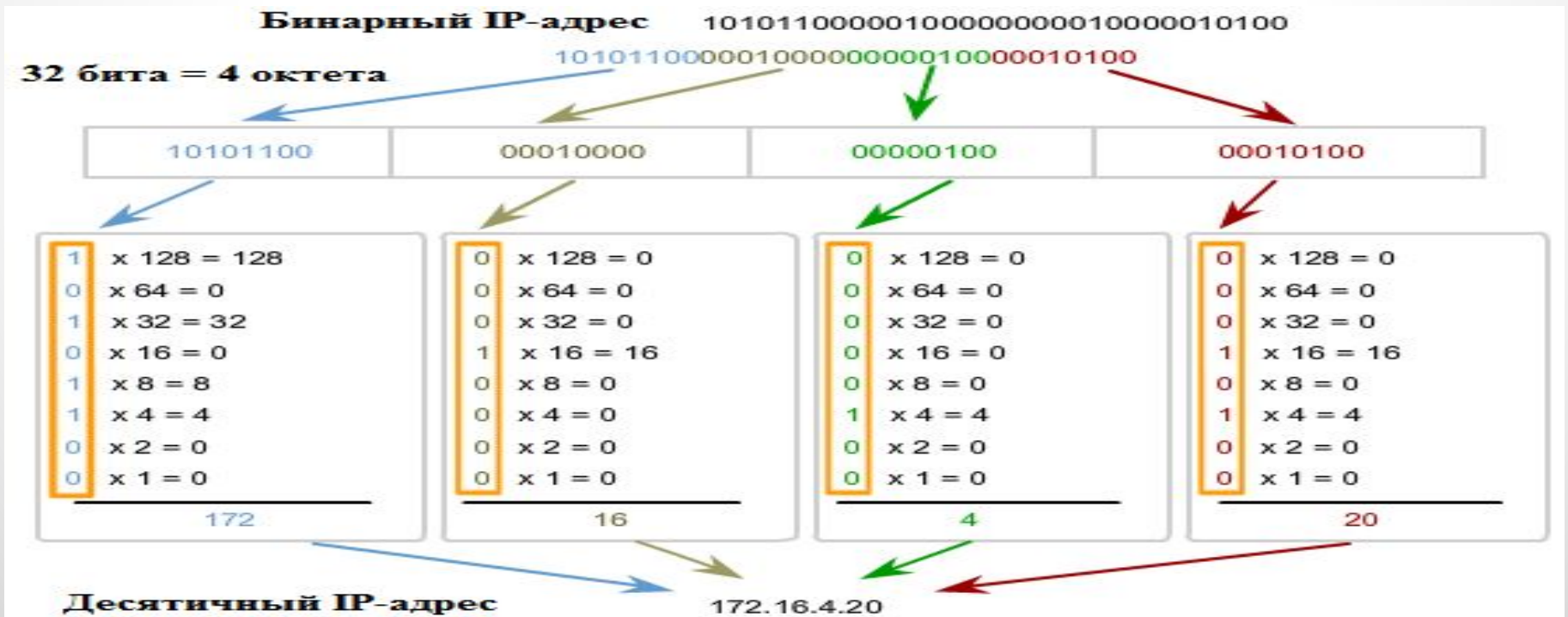
IPv4 адрес

Представление IPv4 адреса

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Пример: число 245

128	64	32	16	0	4	0	1
1	1	1	1	0	1	0	1



Типы адресов

Тип	Network			Host
Адрес сети	10	0	0	0
	00001010	00000000	00000000	00000000
Направленный широковещательный адрес	10	0	0	255
	00001010	00000000	00000000	11111111
Адрес хоста	10	0	0	1
	00001010	00000000	00000000	00000001
Маска сети префикс = 24	255	255	255	0
	11111111	11111111	11111111	00000000

- **Адрес сети** – Сетевая часть IP-адреса (номер сети)
- **Адрес хоста** – Хостовая часть IP-адреса (номер хоста)
- **Маска сети (подсети)** - битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети
- **Широковещательный адрес** – IP-адрес, который используется для передачи пакетов сразу всем компьютерам в сети

Адресное пространство IPv4

Тип адреса	Диапазон		
Все адресное пространство IPv4	0.0.0.0	–	255.255.255.255
Адреса хостов	0.0.0.0	–	223.255.255.255
Мультикаст	224.0.0.0	–	239.255.255.255
Экспериментальные адреса	240.0.0.0	–	255.255.255.254
Ограниченный широковещательный адрес	255.255.255.255		

Все пространство IPv4-адресов разделено на 2 части:

- **публичные адреса**, которые распределяются между Интернет-провайдерами и компаниями, международной организацией **Internet Assigned Numbers Authority** (сокращенно **IANA**)
- **приватные адреса**, которые не контролируются **IANA** и могут назначаться внутрикорпоративным узлам по усмотрению сетевых администраторов.

Если какая-либо компания приобрела IP-адреса в публичной сети, то ее сетевые узлы могут напрямую маршрутизировать сетевой трафик в сеть Интернет и могут быть прозрачно доступны из Интернета.

Internet Assigned Numbers Authority



- Global coordination organization (IANA)

<http://www.iana.org/numbers>

- Regional Internet Registry (RIR)
- National Internet Registry (NIR)
- Local Internet registry (LIR)

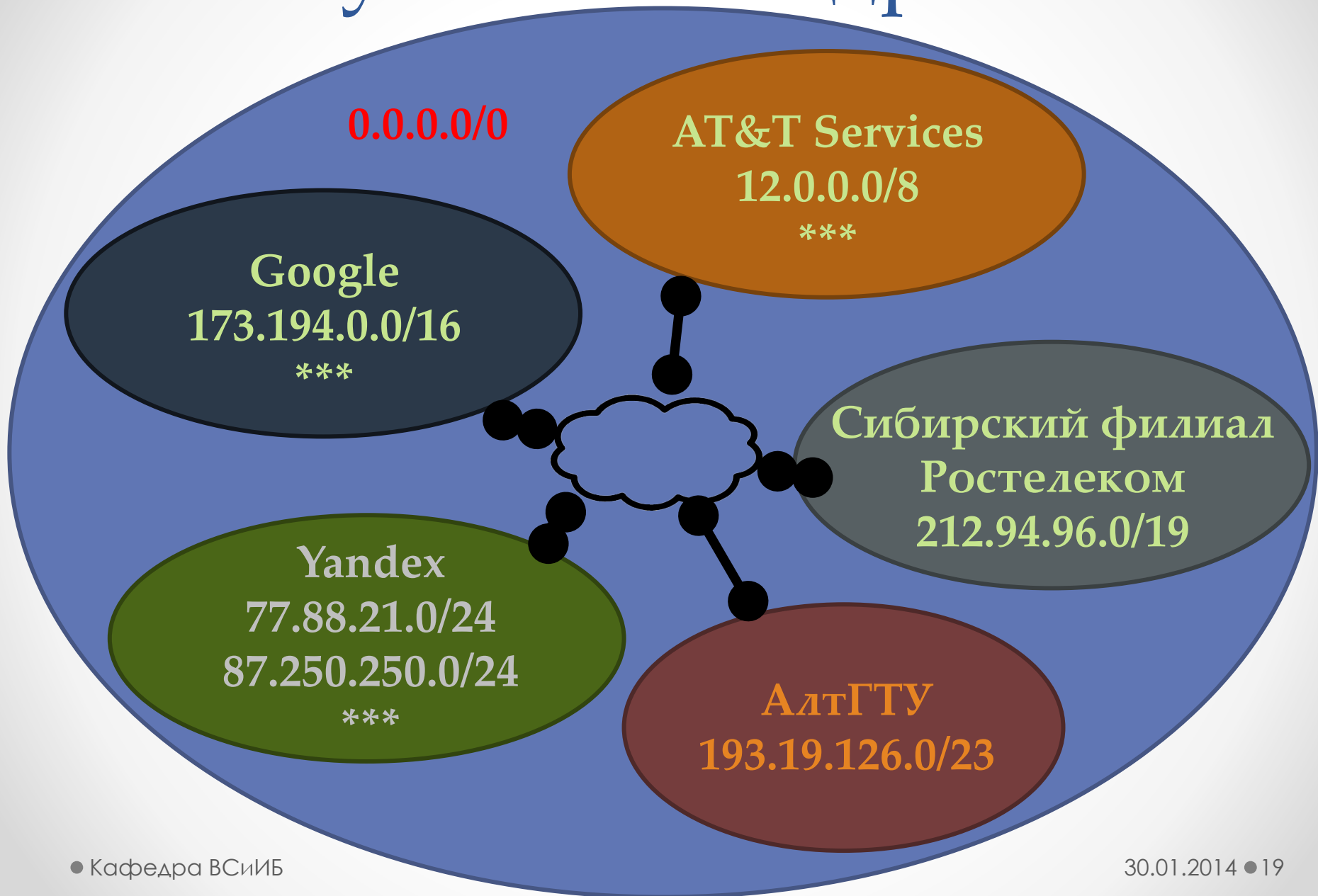
- Address space

<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

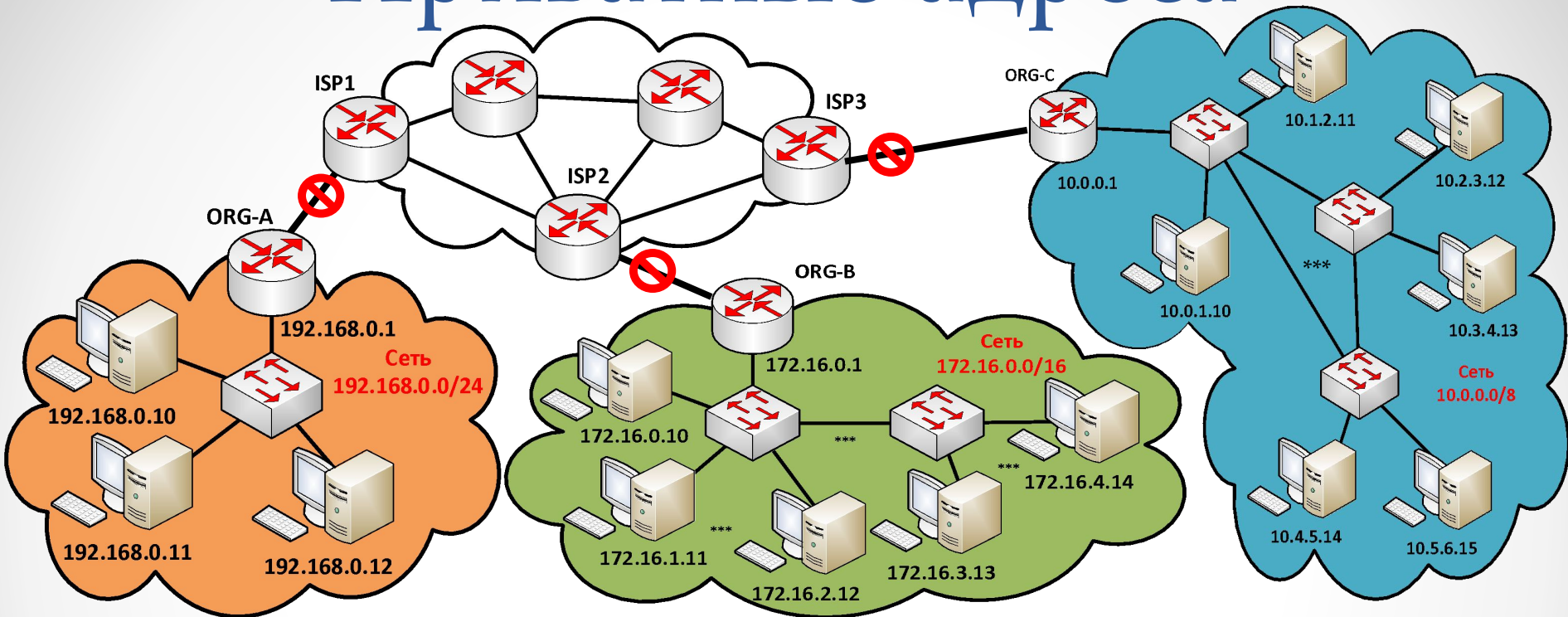
- Special Purpose Address

<http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xml>

Публичные адреса



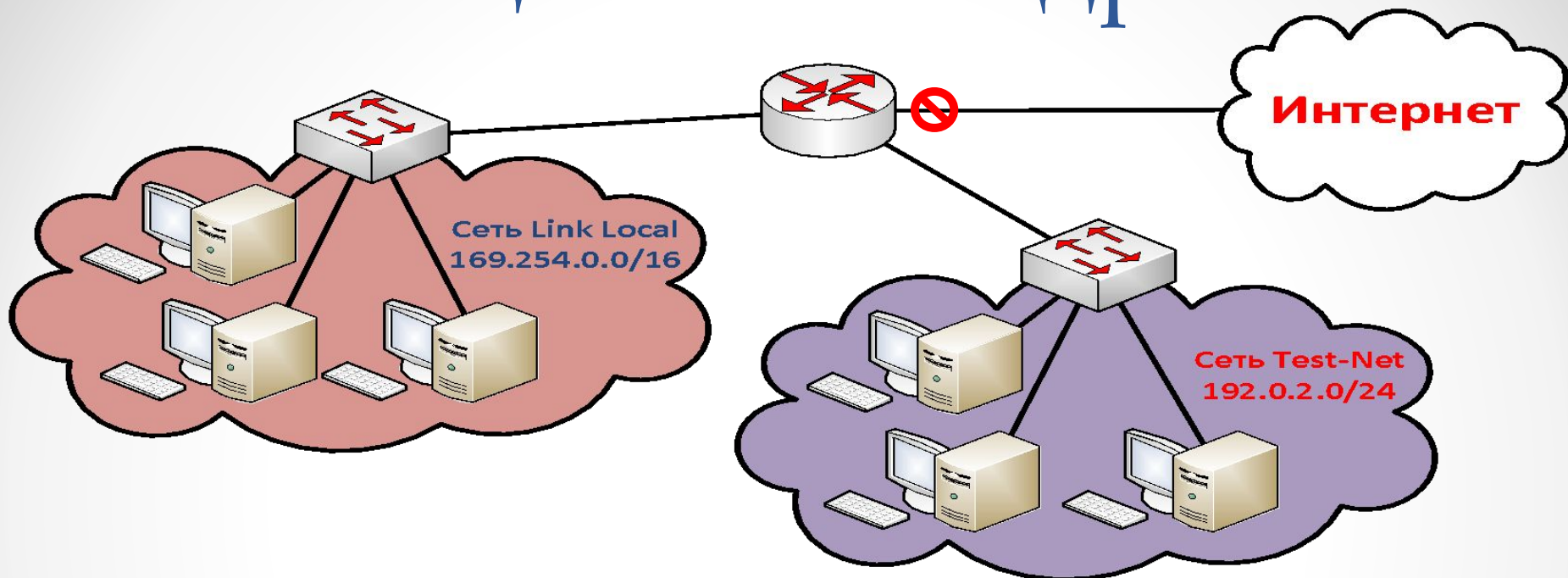
Приватные адреса



- **192.168.0.0 – 192.168.255.255 (192.168.0.0/16)**
- **172.16.0.0 – 172.31.255.255 (172.16.0.0/12)**
- **10.0.0.0 – 10.255.255.255 (10.0.0.0/8)**

Приватные адреса конфигурируются сетевыми администраторами и не маршрутизируются в сети Интернет. Для осуществления доступа к сети Интернет с частных адресов используются технология NAT (PAT) или прокси-сервера.

Специальные адреса

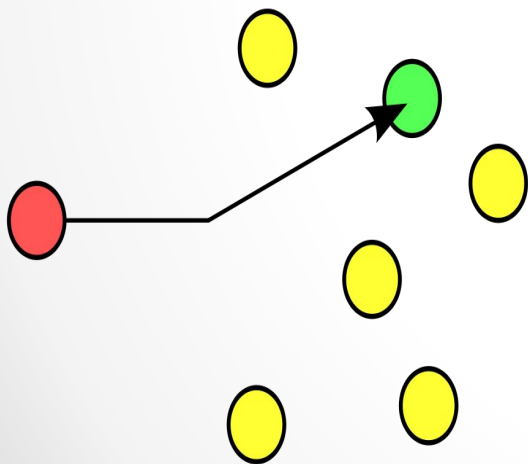


- **0.0.0.0 – 0.255.255.255 (0.0.0.0/8)** – Адреса источников пакетов собственной сети, предназначены для локального использования на хосте при создании сокетов. Адрес **0.0.0.0/32** используется для указания адреса источника самого хоста.
- **127.0.0.0 – 127.255.255.255 (127.0.0.0/8)** – Подсеть для коммуникаций внутри хоста (localhost). **127.0.0.1** – loopback.
- **169.254.0.0 – 169.254.255.255 (169.254.0.0/16)** – Подсеть используется для автоматического конфигурирования адресов IP в случае отсутствия сервера DHCP.
- **192.0.2.0 – 192.0.2.255 (192.0.2.0/24)** – Подсеть для тестирования и для примеров в документации.

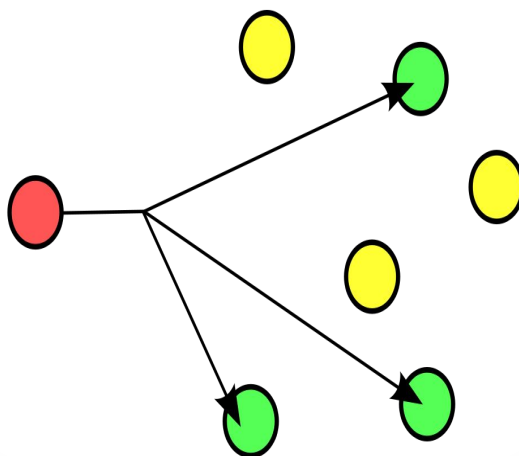
Типы передачи данных

В сетях IP существует 3 основных способа передачи данных:
Unicast, Broadcast, Multicast.

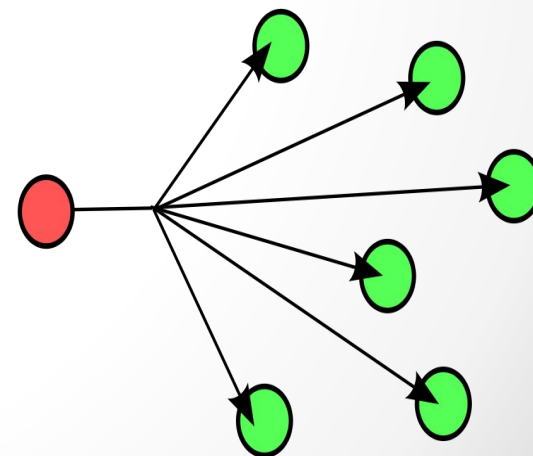
- **Unicast** – процесс отправки пакета от одного хоста к другому хосту (передача конкретному адресату).
- **Multicast** – процесс отправки пакета от одного хоста к некоторой ограниченной группе хостов (видео и аудио рассылка, обмен информацией о маршрутах, распространение программного обеспечения).
- **Broadcast** – процесс отправки пакета от одного хоста ко всем хостам в сети (создание карты принадлежности адресов, запрос адреса, протоколы маршрутизации).



Unicast



Multicast



Broadcast

Классовая адресация

Класс	1й октет (Dec)	1й октет (Bin)	Сетевая и хостовая части	Маска подсети	Количество сетей и хостов
A	1 – 127*	00000000 – 01111111	N.N.N.N	255.0.0.0	$2^7 = 128$ $2^{24} - 2 = 1677214$
B	128 – 191	10000000 – 10111111	N.N.N.N	255.255.0.0	$2^{14} = 16384$ $2^{16} - 2 = 65534$
C	192 – 223	11000000 – 11011111	N.N.N.N	255.255.255.0	$2^{21} = 2097150$ $2^8 - 2 = 254$
D	224 – 239	11100000 – 11101111	N/A (multicast)		
E	240 – 255**	11110000 – 11111111	N/A (experimental)		

* Для сетей класса А – адреса 0.0.0.0 и 127.255.255.255 не допустимы.

** Адрес 255.255.255.255 из сети класса Е – является широковещательным адресом.

Без классовая адресация

Classless InterDomain Routing - Бесклассовая интердоменная маршрутизация, или **Classless Internet Direct Routing** - прямая бесклассовая маршрутизация в Интернет.

В случае адресации вне классов, с произвольным положением границы сеть-хост внутри IP-адреса, к IP-адресу прилагается 32-битовая маска, которую называют маской сети (netmask) или маской подсети (subnet mask).

Сетевая маска конструируется по следующему правилу:

- на позициях, соответствующих номеру сети, биты установлены;
- на позициях, соответствующих номеру хоста, биты сброшены.

Пример без классовой адресации - **137.158.128.0/19**:

IP-адрес: 10001001 . 10011110 . 100 00000 . 00000000

Маска: 11111111 . 11111111 . 111 00000 . 00000000

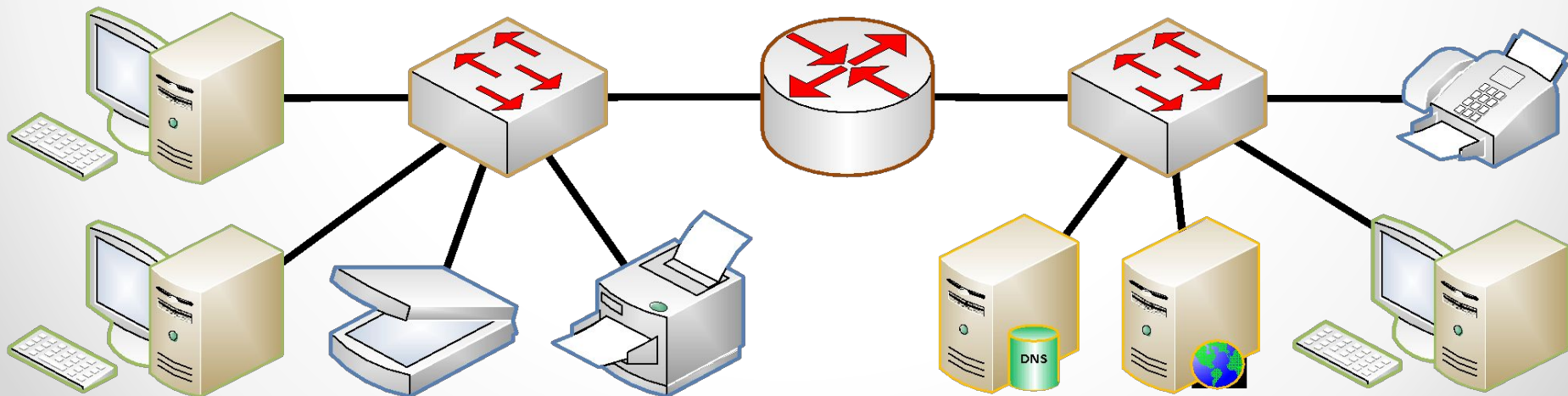
255 . 255 . 224 . 0

Без классовая адресация

255 . 255 . 255 . 255	11111111 . 11111111 . 11111111 . 11111111	/32	Host (single addr)
255 . 255 . 255 . 254	11111111 . 11111111 . 11111111 . 11111110	/31	Unuseable
255 . 255 . 255 . 252	11111111 . 11111111 . 11111111 . 11111100	/30	2 useable
255 . 255 . 255 . 248	11111111 . 11111111 . 11111111 . 11111000	/29	6 useable
255 . 255 . 255 . 240	11111111 . 11111111 . 11111111 . 11110000	/28	14 useable
255 . 255 . 255 . 224	11111111 . 11111111 . 11111111 . 11100000	/27	30 useable
255 . 255 . 255 . 192	11111111 . 11111111 . 11111111 . 11000000	/26	62 useable
255 . 255 . 255 . 128	11111111 . 11111111 . 11111111 . 10000000	/25	126 useable
255 . 255 . 255 . 0	11111111 . 11111111 . 11111111 . 00000000	/24	"Class C" 254 useable
255 . 255 . 254 . 0	11111111 . 11111111 . 11111110 . 00000000	/23	2 Class C's
255 . 255 . 252 . 0	11111111 . 11111111 . 11111100 . 00000000	/22	4 Class C's
255 . 255 . 248 . 0	11111111 . 11111111 . 11111000 . 00000000	/21	8 Class C's
255 . 255 . 240 . 0	11111111 . 11111111 . 11110000 . 00000000	/20	16 Class C's
255 . 255 . 224 . 0	11111111 . 11111111 . 11100000 . 00000000	/19	32 Class C's
255 . 255 . 192 . 0	11111111 . 11111111 . 11000000 . 00000000	/18	64 Class C's
255 . 255 . 128 . 0	11111111 . 11111111 . 10000000 . 00000000	/17	128 Class C's
255 . 255 . 0 . 0	11111111 . 11111111 . 00000000 . 00000000	/16	"Class B"
255 . 254 . 0 . 0	11111111 . 11111110 . 00000000 . 00000000	/15	2 Class B's
255 . 252 . 0 . 0	11111111 . 11111100 . 00000000 . 00000000	/14	4 Class B's
255 . 248 . 0 . 0	11111111 . 11111000 . 00000000 . 00000000	/13	8 Class B's
255 . 240 . 0 . 0	11111111 . 11110000 . 00000000 . 00000000	/12	16 Class B's
255 . 224 . 0 . 0	11111111 . 11100000 . 00000000 . 00000000	/11	32 Class B's
255 . 192 . 0 . 0	11111111 . 11000000 . 00000000 . 00000000	/10	64 Class B's
255 . 128 . 0 . 0	11111111 . 10000000 . 00000000 . 00000000	/9	128 Class B's
255 . 0 . 0 . 0	11111111 . 00000000 . 00000000 . 00000000	/8	"Class A"
254 . 0 . 0 . 0	11111110 . 00000000 . 00000000 . 00000000	/7	2 Class A's
252 . 0 . 0 . 0	11111100 . 00000000 . 00000000 . 00000000	/6	4 Class A's
248 . 0 . 0 . 0	11111000 . 00000000 . 00000000 . 00000000	/5	8 Class A's
240 . 0 . 0 . 0	11110000 . 00000000 . 00000000 . 00000000	/4	16 Class A's
224 . 0 . 0 . 0	11100000 . 00000000 . 00000000 . 00000000	/3	23 Class A's
192 . 0 . 0 . 0	11000000 . 00000000 . 00000000 . 00000000	/2	64 Class A's
128 . 0 . 0 . 0	10000000 . 00000000 . 00000000 . 00000000	/1	128 Class A's
0 . 0 . 0 . 0	00000000 . 00000000 . 00000000 . 00000000	/0	IP space

Политика распределения адресов

Использование	Первый адрес	Последний адрес	Суммарный адрес
Сетевой адрес	172.16.x.0	...	172.16.x.0/25
Пользовательские компьютеры (DHCP)	172.16.x.1	172.16.x.127	
Сервера (Static)	172.16.x.128	172.16.x.191	172.16.x.128/26
Периферия	172.16.x.192	172.16.x.223	172.16.x.128/26
Сетевые устройства	172.16.x.224	172.16.x.253	172.16.x.224/27
Маршрутизатор	172.16.x.254	...	
Широковещательный адрес	172.16.x.255	...	



Конфигурирование IPv4

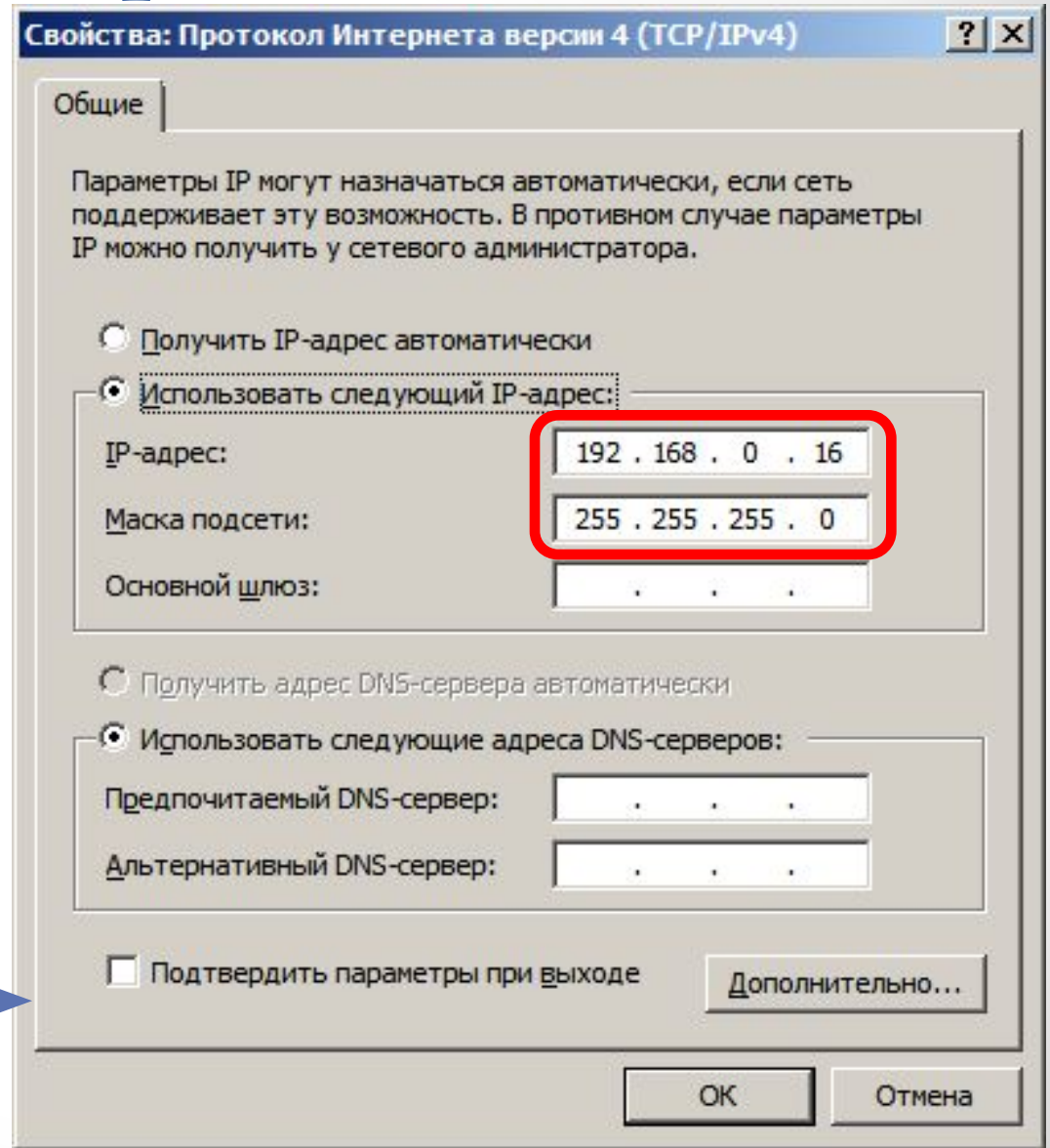
Пуск

Панель управления

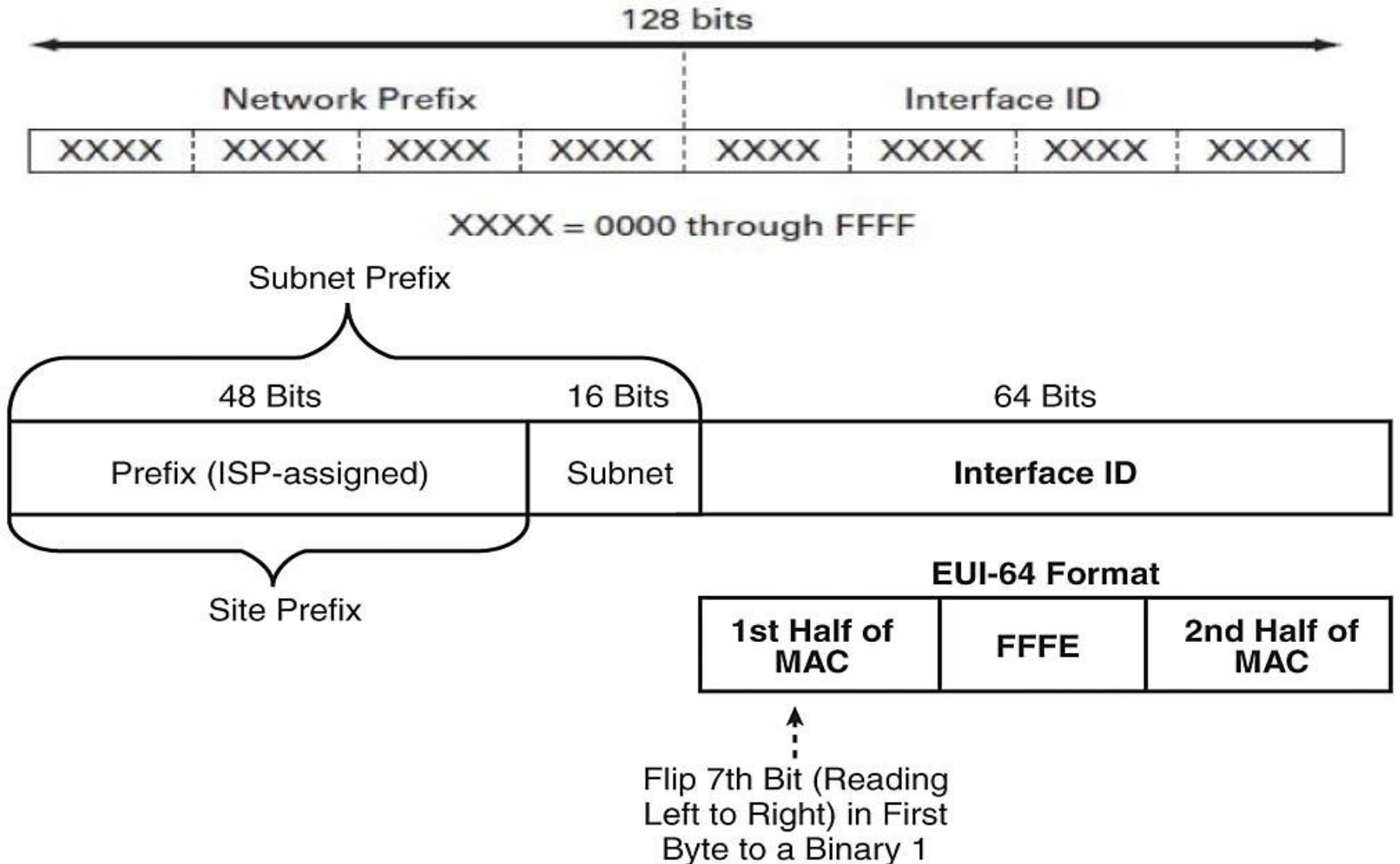
Центр управления сетями и общим доступом

Изменение параметров адаптера

Свойства: Подключение по локальной сети



IPv6 адрес



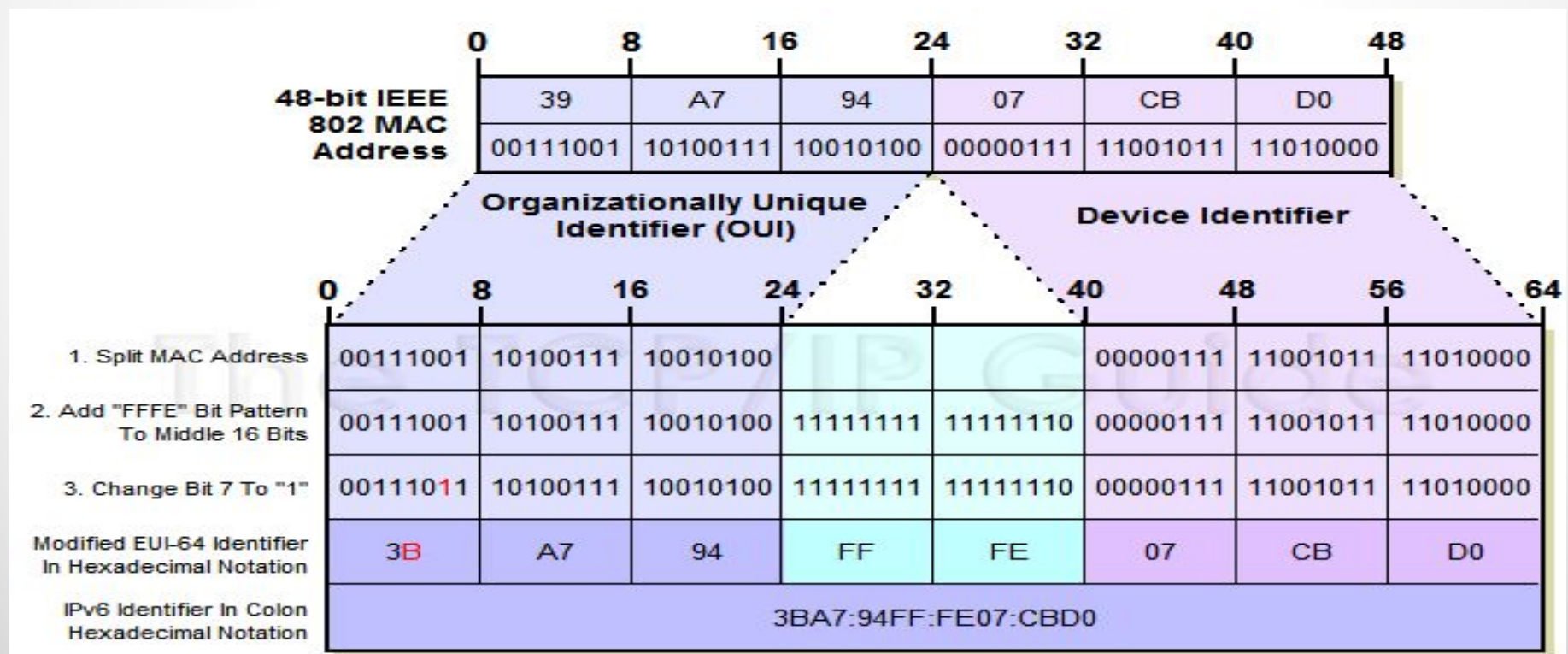
Представление IPv6 адреса

2001:0DB8:AC10:FE01:0000:0000:1428:57AB

2001:0DB8:AC10:FE01::1428:57AB

0010000000000001:0000110110111000:101011000010000:1111111000000001:0000000000000000:0000000000000000:0001010000101000:0101011110101011

0010000000000001:0000110110111000:101011000010000:1111111000000001::0001010000101000:0101011110101011



Типы IPv6-адресов

- **Unicast** адреса идентифицируют только один сетевой интерфейс. Протокол IPv6 доставляет пакеты, отправленные на такой адрес, на конкретный интерфейс.
- **Anycast** адреса назначаются группе интерфейсов, обычно принадлежащих различным узлам. Пакет, отправленный на такой адрес, доставляется на один из интерфейсов данной группы, как правило наиболее близкий к отправителю с точки зрения протокола маршрутизации.
- **Multicast** адрес также используется группой узлов, но пакет, отправленный на такой адрес, будет доставлен каждому узлу в группе.

В IPv6 не реализованы широковещательные адреса. Традиционная роль широковещательной рассылки реализована с помощью групповой рассылки на адрес ff02::1, однако использование этой группы не рекомендуется.

Специальные адреса

- **Локальные адреса:**
 - `::/128` - адрес со всеми нулями является неопределенным адресом, и будет использоваться только в ПО (соответствует 0.0.0.0 в IPv4).
 - `::1/128` – адрес внутренней петли (loopback) localhost (соответствует 127.0.0.1 в IPv4).
 - `fe80::/10` - локальный префикс, указывает, что адрес является действительным только внутри местной физической сети (link-local, аналог 169.254.0.0/16 в IPv4).
- **Местные адреса:**
 - `fc00::/7` - уникальные локальные адреса (ULA) являются маршрутизируемыми только в рамках набора взаимодействующих сайтов (site-local).
- **IPv4**
 - `::ffff:0:0/96` - это префикс используется для подключаемых адресов IPv4.
 - `2001::/32` - используется для Teredo-туннелей (Teredo — сетевой протокол, предназначенный для передачи IPv6 пакетов через сети IPv4).
 - `2002::/16` - это префикс используется для 6to4-адресации.
- **Групповые:**
 - `ff00::/8` - многоадресный префикс используется для широковещания.
- **Используемые в примерах, нерекомендуемые или устаревшие:**
 - `::/96` - нулевой префикс, использовался для IPv4-совместимых адресов.
 - `2001:db8::/32` - используется в документации.
 - `fec0::/10` - местный префикс, указывает, что адрес является действительным только внутри сети организации. Не используется с сентября 2004 года.
- **ORCHID (Overlay Routable Cryptographic Hash Identifiers):**
 - `2001:10::/28` – немаршрутизируемые IPv6-адреса, используемые для криптографических хэш-идентификаторов.

Конфигурирование IPv6

Пуск

Панель управления

Центр управления сетями и общим доступом

Изменение параметров адаптера

Свойства: Подключение по локальной сети

Свойства: Протокол Интернета версии 6 (TCP/IPv6)

Общие

Параметры IPv6 можно задавать автоматически, если сеть поддерживает такую возможность. В противном случае параметры IPv6 можно узнать у сетевого администратора.

Получить IPv6-адрес автоматически

Использовать следующий IPv6-адрес:

IPv6-адрес: 2001:0DB8:AC10:FE01::1428:57AB

Длина префикса подсети: 64

Основной шлюз:

Получить адрес DNS-сервера автоматически

Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

Подтвердить параметры при выходе

Дополнительно...

OK Отмена

ICMP

Internet Control Message Protocol (протокол межсетевых управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

Правила генерации ICMP-пакетов:

- При потере ICMP-пакета никогда не генерируется новый.
- ICMP-пакеты никогда не генерируются в ответ на IP-пакеты с широковещательным или групповым адресом, чтобы не вызывать перегрузку в сети (так называемый «широковещательный шторм»).
- При повреждении фрагментированного IP-пакета ICMP-сообщение отправляется только после получения первого повреждённого фрагмента, поскольку отправитель всё равно повторит передачу всего IP-пакета целиком.

Заголовок ICMP

байт 1	байт 2	байт 3	байт 4
Тип	Код	Контрольная сумма	
Данные (формат зависит от значений полей «Код» и «Тип»)			

Типы ICMP

Тип	Код	Сообщение	Данные	
0	0	Эхо-ответ	Идентификатор	Номер последовательности
			Данные	
3	Адресат недоступен		Заголовок IP	
	0	Сеть недостижима		
	1	Узел недостижим		
	2	Протокол недостижим		
	3	Порт недостижим		
4	0	Сдерживание источника	Заголовок IP	

Типы ICMP

Тип	Код	Сообщение	Данные	
5	Перенаправление		Адрес маршрутизатора Заголовок IP	
	0	Перенаправление пакетов в сеть		
	1	Перенаправление пакетов к узлу		
	2	Перенаправление для каждого типа обслуживания (ToS)		
	3	Перенаправление пакета к узлу для каждого типа обслуживания		
8	0	Эхо-запрос	Идентификатор	Номер послед-ти
			Данные	
11	Время жизни дейтаграммы истекло		Заголовок IP	
	0	Время жизни пакета (TTL) истекло при транспортировке		
	1	Время жизни пакета истекло при сборке фрагментов		
12	Неверный параметр в заголовке IP		Заголовок IP	
	0	Указатель говорит об ошибке		
	1	Отсутствует требуемая опция		
	2	Некорректная длина		

Использование ICMP-сообщений

- ICMP-сообщения (тип 12) генерируются при нахождении ошибок в заголовке IP-пакета (за исключением самих ICMP-пакетов, дабы не привести к бесконечно растущему потоку ICMP-сообщений об ICMP-сообщениях).
- ICMP-сообщения (тип 3) генерируются маршрутизатором при отсутствии маршрута к адресату.
- Утилита Ping, служащая для проверки возможности доставки IP-пакетов, использует ICMP-сообщения с типом 8 (эхо-запрос) и 0 (эхо-ответ).
- Утилита Traceroute, отображающая путь следования IP-пакетов, использует ICMP-сообщения с типом 11.
- ICMP-сообщения с типом 5 используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя.
- ICMP-сообщения с типом 4 используются получателем (или маршрутизатором) для управления скоростью отправки сообщений отправителем.

Информация о сетевых интерфейсах

```
Администратор: Командная строка
Microsoft Windows [Version 6.1.7601]
(с) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Georgy Chugunov>ipconfig

Настройка протокола IP для Windows

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

    DNS-суффикс подключения . . . . . : energy.astu
    Локальный IPv6-адрес канала . . . . : fe80::4505:e56a:1e86:2844%12
    IPv4-адрес . . . . . : 10.1.100.16
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 10.1.100.1

Ethernet adapter Подключение по локальной сети:

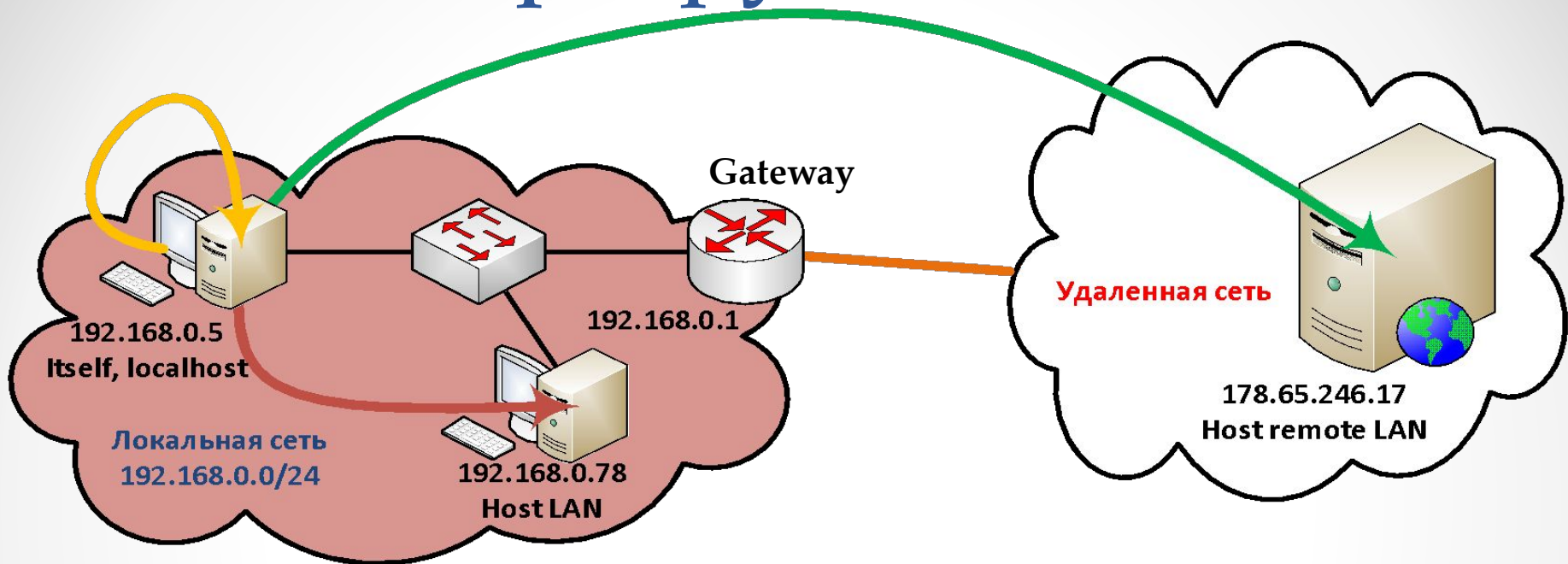
    Состояние среды . . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Ethernet adapter VirtualBox Host-Only Network:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::20c2:3af6:f31a:81ec%25
    IPv4-адрес . . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

C:\Users\Georgy Chugunov>
```

Маршрутизация

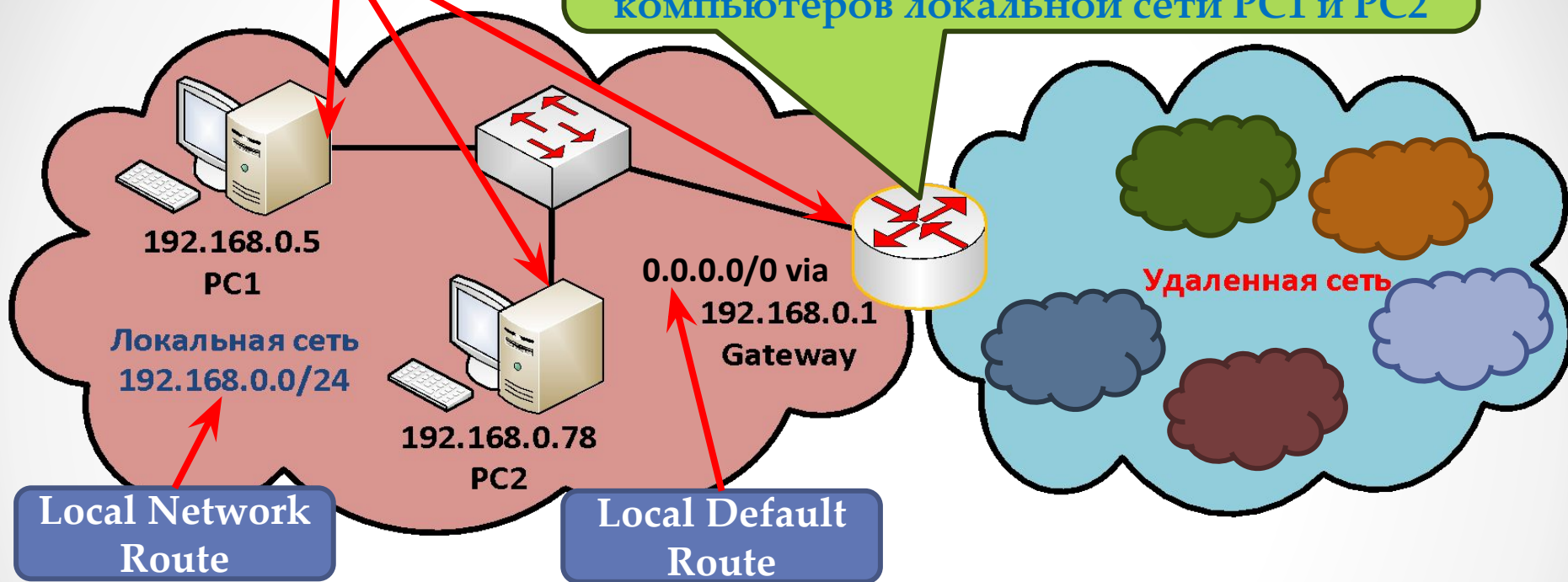


- **Itself (localhost, локальный хост)** – устройство может посылать пакеты самому себе на специальный адрес 127.0.0.1 (localhost)
- **Local Host (Host LAN, хост в локальной сети)** – устройство может посылать пакеты устройствам находящимся в тоже самой локальной сети
- **Remote Host (хост в удаленной локальной сети)** – устройство может посылать пакеты устройствам находящимся в других локальных сетях

Основной шлюз

Direct connection

IP-адрес интерфейса данного устройства является шлюзом по умолчанию для компьютеров локальной сети PC1 и PC2

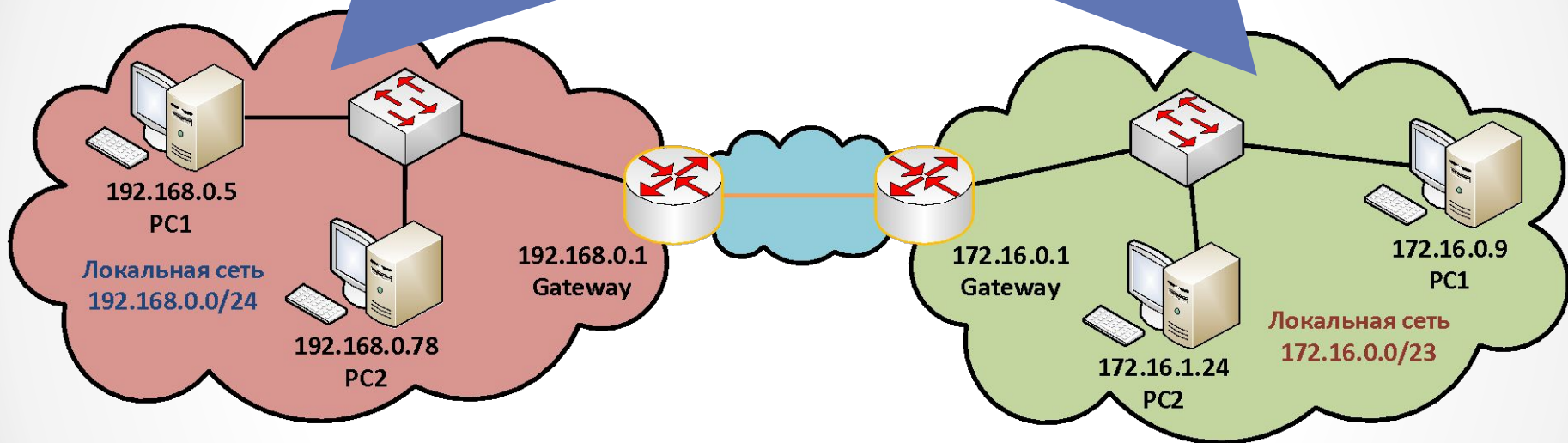


Для SOHO сетей шлюз по умолчанию часто используется для доступа в сеть Интернет.

Для определения к какой сети принадлежит IP-адрес назначения (локальной или удаленной) применяется маска сети (сравниваются сетевые части IP-адресов).

Понятие шлюза

- * Устройства в одной сети знают физические адреса устройств только в пределах этой сети
- * Если физический адрес устройства не известен, то пакет отсылается устройству логический адрес которого указан в качестве маршрута по умолчанию



Не все устройства в сети обязаны иметь шлюз по умолчанию. Например, для сетевых принтеров и сканеров, доступ к которым осуществляется только из локальной сети, можно не указывать шлюз по умолчанию.

Конфигурирование шлюза

Пуск

Панель управления

Центр управления сетями и общим доступом

Изменение параметров адаптера

Свойства: Подключение по локальной сети

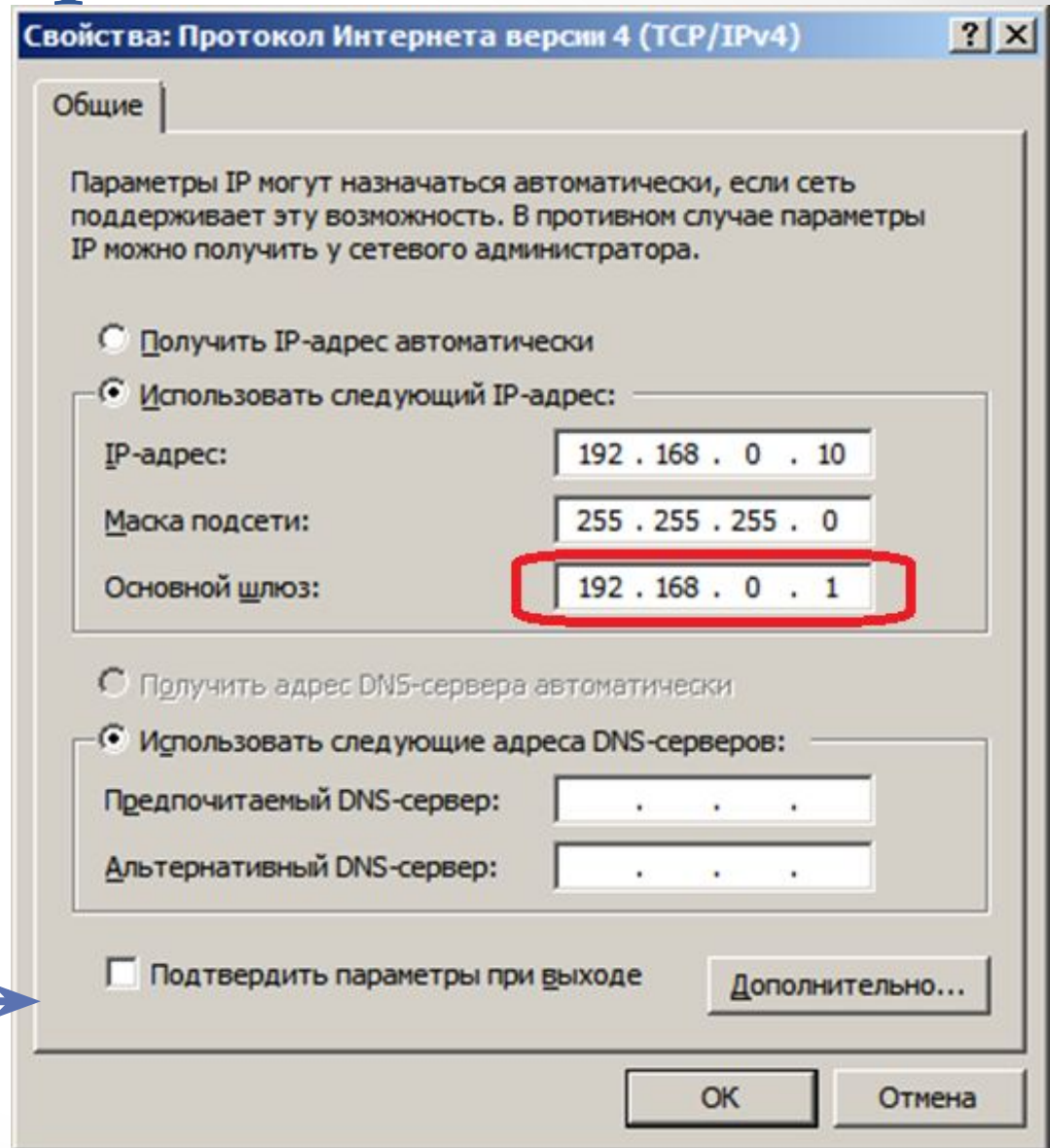


Таблица маршрутизации на хосте

Команда

Интерфейсы

Сетевой адрес – список доступных сетей

Маска сети – список масок сетей для определения размеров сетей

Адрес шлюза – список адресов куда следует отправлять пакеты для передачи пакетов в нужную сеть

Интерфейс – список сетевых интерфейсов через которые необходимо отправлять пакеты

Метрика – стоимость маршрута в сеть

```
Администратор: Командная строка
C:\>netstat -nr
-----
Список интерфейсов
11...74 46 a0 b7 a6 5f .....Intel(R) 82579LM Gigabit Network Connection
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 00 e0 Адаптер Microsoft ISATAP #2
-----

IPv4 таблица маршрута
-----
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0        10.129.0.245     10.129.0.31    266
10.129.0.0        255.255.240.0  On-link          10.129.0.31    266
10.129.0.31      255.255.255.255 On-link          10.129.0.31    266
10.129.15.255    255.255.255.255 On-link          10.129.0.31    266
127.0.0.0        255.0.0.0      On-link          127.0.0.1      306
127.0.0.1        255.255.255.255 On-link          127.0.0.1      306
127.255.255.255  255.255.255.255 On-link          127.0.0.1      306
224.0.0.0        240.0.0.0      On-link          127.0.0.1      306
224.0.0.0        240.0.0.0      On-link          10.129.0.31    266
255.255.255.255  255.255.255.255 On-link          127.0.0.1      306
255.255.255.255  255.255.255.255 On-link          10.129.0.31    266
-----
Постоянные маршруты:
Сетевой адрес      Маска      Адрес шлюза      Метрика
0.0.0.0            0.0.0.0      10.129.0.245    По умолчанию
-----

IPv6 таблица маршрута
-----
Активные маршруты:
Метрика  Сетевой адрес      Шлюз
1        306  ::1/128            On-link
11       266  fe80::/64          On-link
11       266  fe80::25ec:5aae:7a92:a248/128 On-link
1        306  ff00::/8           On-link
11       266  ff00::/8           On-link
-----
Постоянные маршруты:
Отсутствует
C:\>
```

Таблица маршрутизации на хосте

IPv4 таблица маршрута

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.4	25
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.0.0	255.255.255.0	On-link	192.168.0.4	281
192.168.0.4	255.255.255.255	On-link	192.168.0.4	281
192.168.0.255	255.255.255.255	On-link	192.168.0.4	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.0.4	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.0.4	281

- **0.0.0.0** – маршрут по умолчанию, все пакеты не соответствующие всем остальным адресам, присутствующим в таблице, передаются на шлюз.
- **127.0.0.0** – **127.255.255.255** – Loopback адреса, используются для представления сервисов на локальном компьютере.
- **192.168.0.0** – **192.168.0.255** – Локальная сеть.
- **224.0.0.0** – Специальные адреса multicast класса “D”.
- **255.255.255.255** – Ограниченный широковещательный адрес.

Понятие маршрутизатора

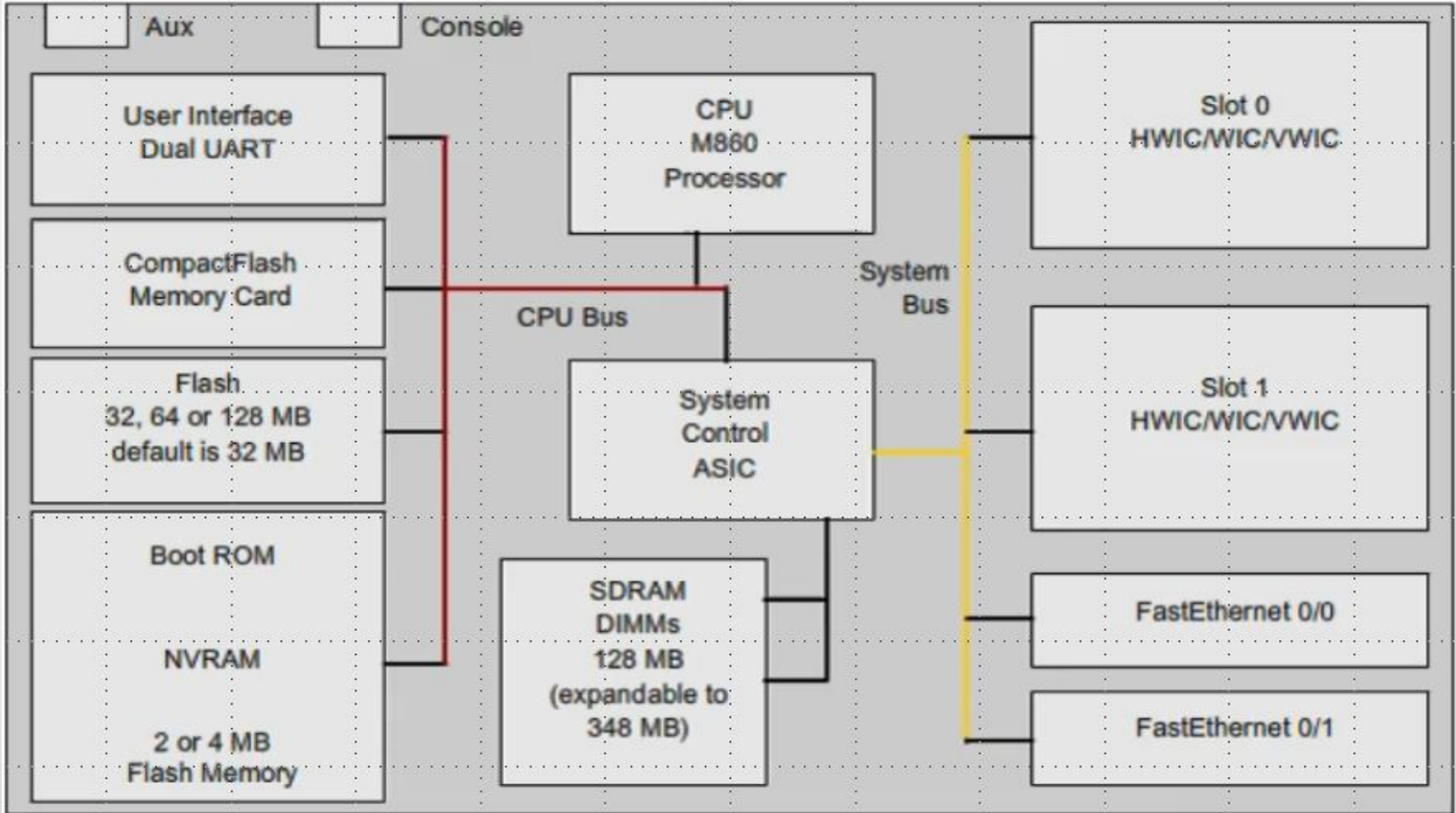
Маршрутизатор – специализированный сетевой компьютер или отдельное устройство, имеющее минимум два сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

Маршрутизатор, как и компьютер имеет следующие компоненты:

- CPU
- RAM
- ROM
- Operation System

Маршрутизатор объединяет различные сегменты сетей, разделяет сети на широковежательные домены. С помощью маршрутизатора осуществляется подключение локальной сети к сети Интернет для этого маршрутизатор имеет сетевой интерфейс LAN - для подключения локальных устройств и сетевой интерфейс для подключения к сети провайдера (ISP) – WAN интерфейс.

Логическая диаграмма маршрутизатора



Интерфейсы и сети



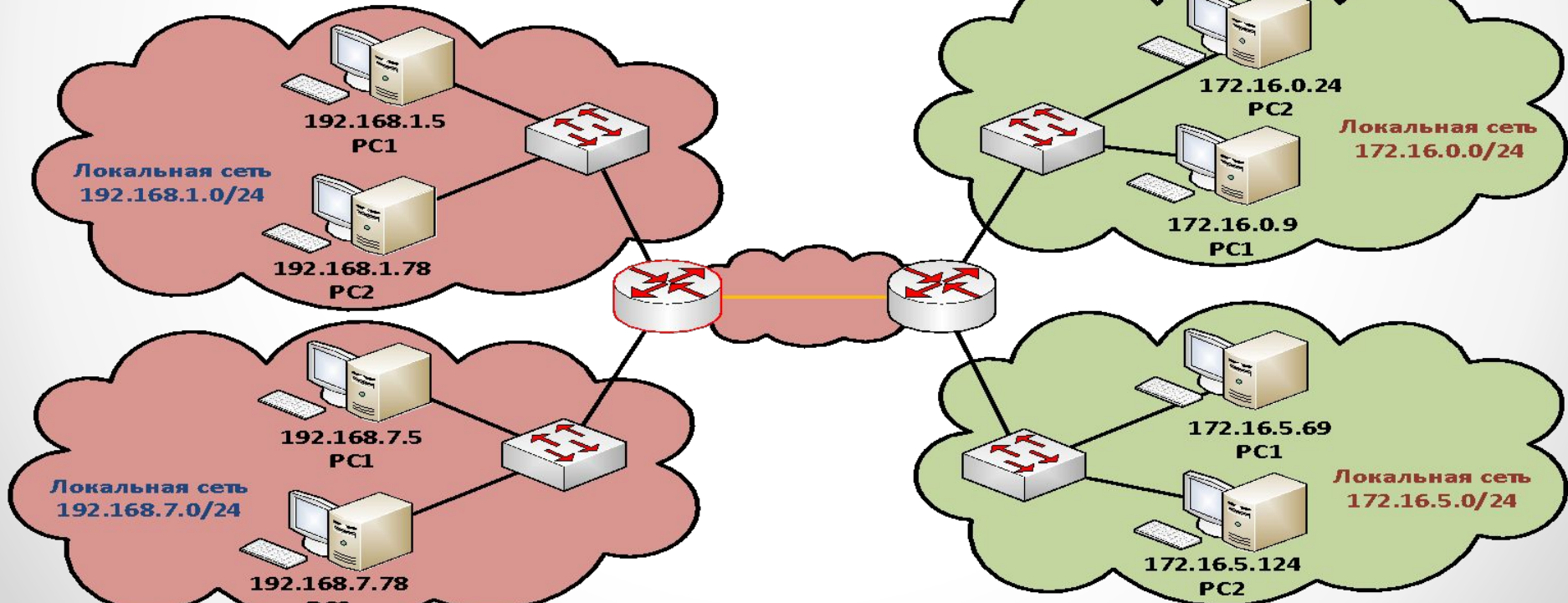
Directly connected
Network

LAN interfaces

WAN interfaces

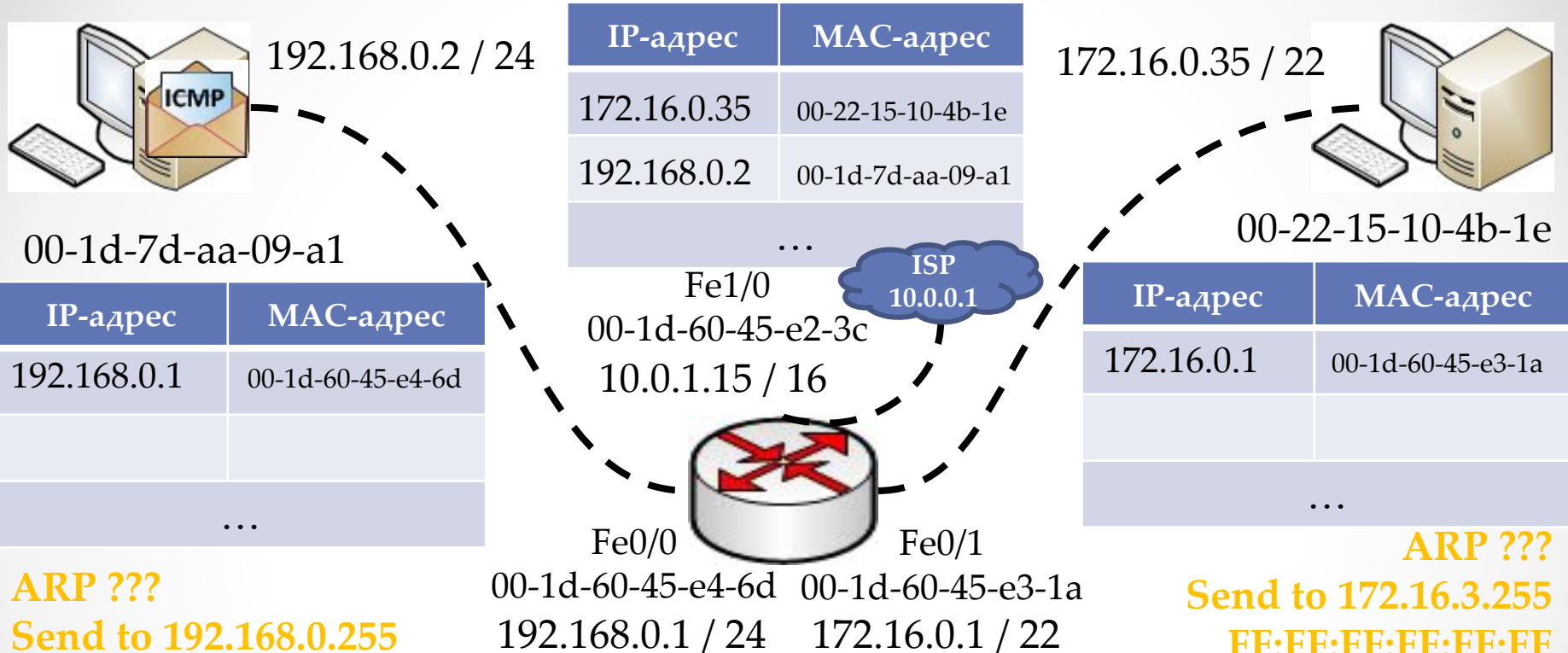
Concole port

AUX port



Remote Network

Функционирование маршрутизатора



ARP ???
Send to 192.168.0.255
FF:FF:FF:FF:FF:FF

route add default
0.0.0.0 10.0.0.1

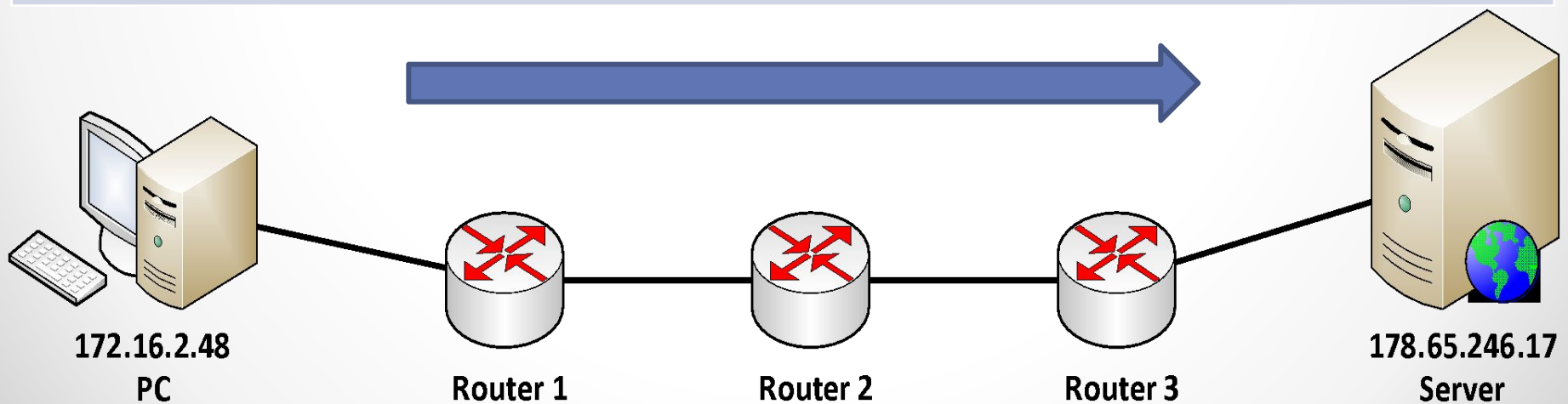
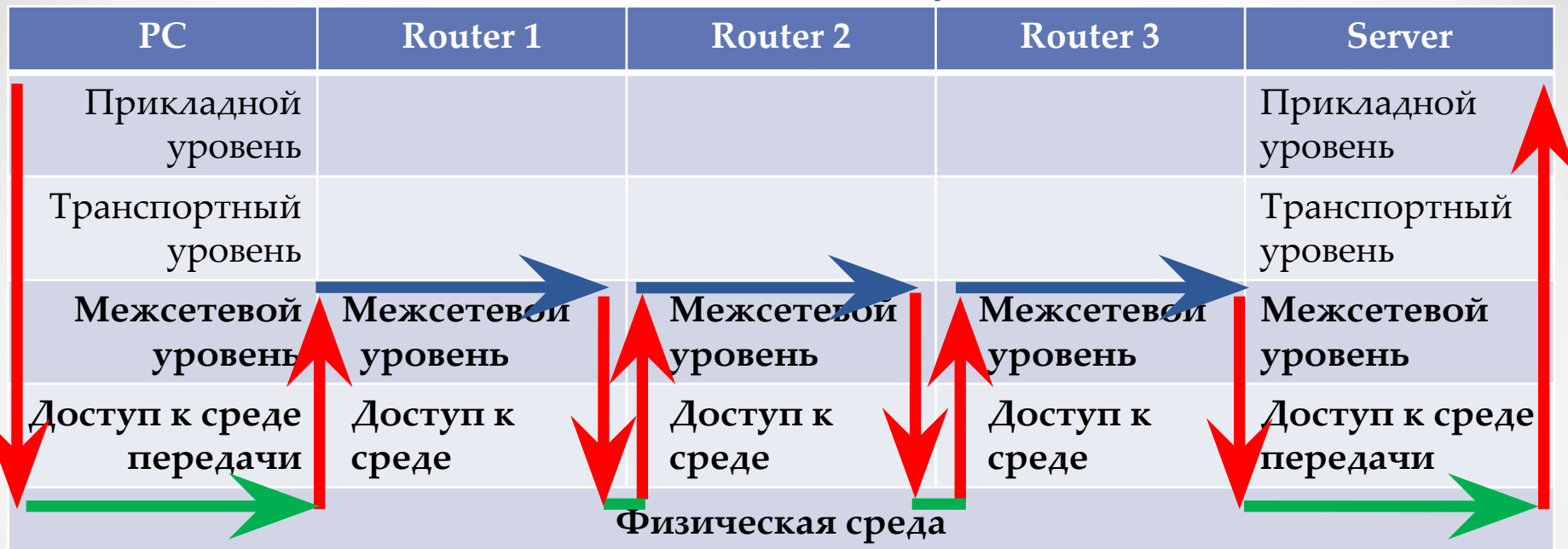
C:\>ping 172.16.0.35

ОТВЕТ ОТ 172.16.0.35
Ping successful

ARP ???
Send to 172.16.3.255
FF:FF:FF:FF:FF:FF

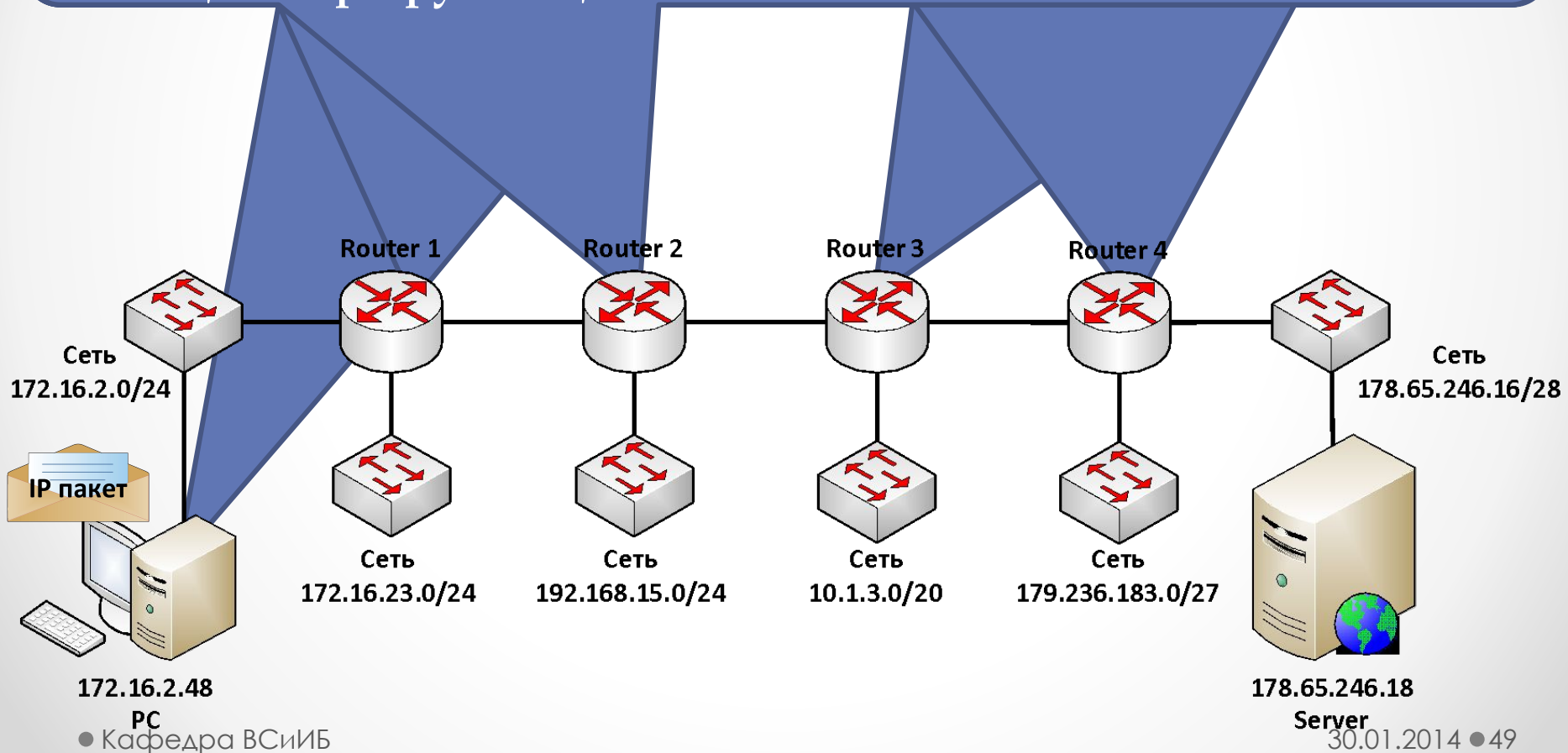
Сеть	Маска	Шлюз	Интерфейс	Метрика
192.168.0.0	255.255.255.0	Directly conn.	FastEthernet 0/0	0
172.16.0.0	255.255.252.0	Directly conn.	FastEthernet 0/1	0
10.0.0.0	255.255.0.0	Directly conn.	FastEthernet 1/0	0
default	0.0.0.0	10.0.0.1	FastEthernet 1/0	1

Маршрутизатор и модель стека TCP/IP

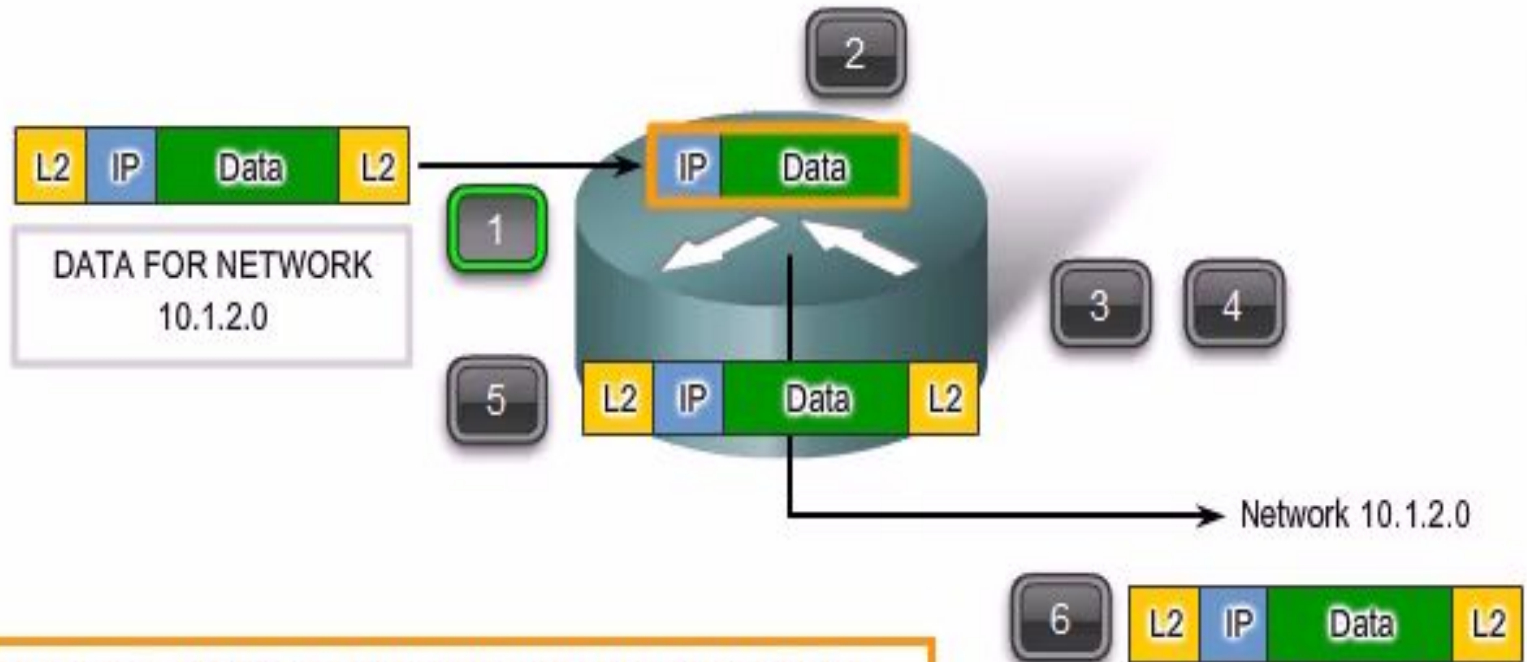


Понятие маршрутизации

- * Этот пакет не предназначен непосредственно подключенным устройствам
- * Отправляем его устройству через интерфейс в соответствии с таблицей маршрутизации



Принцип работы маршрутизатора



1. Маршрутизатор удаляет заголовок канального уровня

2. Маршрутизатор извлекает IP-адрес назначения

3. Маршрутизатор проверяет таблицу маршрутизации на соответствие

4. Запись сети 10.1.2.0 найдена в таблице маршрутизации

5. Маршрутизатор реинкапсурирует пакет во фрейм канального уровня

6. Пакет отправляется в сеть 10.1.2.0 по соответствующему интерфейсу

Содержимое таблицы маршрутизатора

- **Directly Connected Routes** – прямо подключенные маршруты
- **Static Routes** – статические маршруты
- **Dynamic Routes** – динамические маршруты

```
HQ#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
10.0.0.0/30 is subnetted, 8 subnets
```

```
O 10.0.0.0 [110/65] via 172.16.0.2, 00:00:35, FastEthernet0/1  
O 10.0.0.4 [110/65] via 172.16.0.4, 00:00:35, FastEthernet0/1  
O 10.0.0.8 [110/128] via 10.0.0.26, 00:01:05, Serial10/0/0  
O 10.0.0.12 [110/128] via 10.0.0.30, 00:01:05, Serial10/0/1  
O 10.0.0.16 [110/128] via 10.0.0.30, 00:01:05, Serial10/0/1  
O 10.0.0.20 [110/128] via 10.0.0.26, 00:01:05, Serial10/0/0
```

```
C 10.0.0.24 is directly connected, Serial10/0/0  
C 10.0.0.28 is directly connected, Serial10/0/1
```

```
172.16.0.0/24 is subnetted, 1 subnets
```

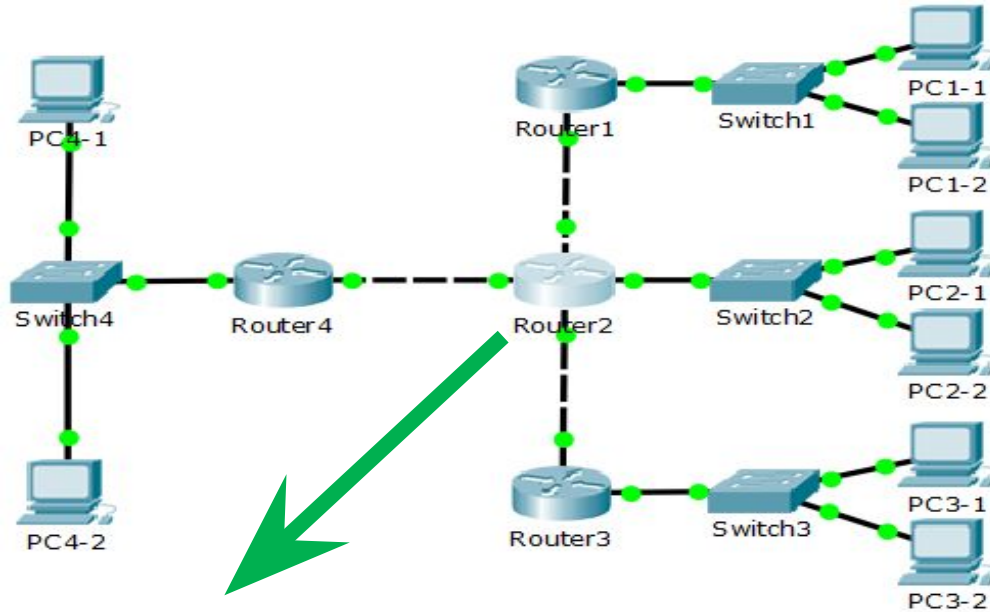
```
C 172.16.0.0 is directly connected, FastEthernet0/1
```

```
212.94.124.0/30 is subnetted, 1 subnets
```

```
C 212.94.124.0 is directly connected, Serial10/1/0
```

```
S* 0.0.0.0/0 is directly connected, Serial10/1/0
```

Содержимое таблицы маршрутизатора



- Как сеть была получена
- Сеть назначения
- Административная дистанция
- Метрика сети
- Следующий маршрутизатор
- Время с момента получения сети
- Выходной интерфейс

```
Router2#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 10.0.0.6 to network 0.0.0.0
```

Code	Network	Administrative Distance	Metric	Next Hop	Time	Interface
C	10.0.0.0			is directly connected,		FastEthernet0/1
C	10.0.0.4			is directly connected,		FastEthernet0/0
C	10.0.0.36			is directly connected,		FastEthernet1/1
R	192.168.1.0/24	[120 / 1]		via 10.0.0.1,	00:00:28,	FastEthernet0/1
C	192.168.2.0/24			is directly connected,		FastEthernet1/0
O	192.168.3.0/24	[110 / 2]		via 10.0.0.6,	00:28:01,	FastEthernet0/0
D	192.168.4.0/24	[90 / 30720]		via 10.0.0.38,	00:03:01,	FastEthernet1/1
S+	0.0.0.0/0	[1 / 0]		via 10.0.0.6		

Прямо подключенные сети

Данные маршруты в таблице появляются автоматически, при условии что на маршрутизаторе сконфигурированы соответствующие интерфейсы (указан IP-адрес и маска сети), активированы интерфейсы и получен несущий сигнал от другого устройства (хаба, свитча, роутера, компьютера и пр.). Таким образом маршрутизатор становится частью сети и является одним из хостов данной сети.

Данные маршруты содержат: адрес сети, маску сети и выходной интерфейс.

Информация об удаленных сетях добавляется в таблицу с помощью конфигурирования статических маршрутов или с использованием механизмов динамической маршрутизации.

Статические маршруты

Маршруты указываются в явном виде при конфигурировании маршрутизатора. При задании статического маршрута указывается:

- Адрес сети (на которую маршрутизируется трафик)
- Маска сети
- Адрес шлюза (узла), который отвечает за дальнейшую маршрутизацию (или подключен к маршрутизируемой сети напрямую)
- (опционально) метрика (иногда называется "ценой") маршрута. При наличии нескольких маршрутов на одну и ту же сеть некоторые маршрутизаторы выбирают маршрут с минимальной метрикой, некоторые маршрутизаторы при совпадении маршрутов в сеть, используют балансировку нагрузки.

В некоторых маршрутизаторах возможно указывать интерфейс, на который следует направить трафик сети и указать дополнительные условия, согласно которым выбирается маршрут.

Достоинства и недостатки

Достоинства

- Лёгкость отладки и конфигурирования в малых сетях.
- Отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации)
- Мгновенная готовность (не требуется интервал для конфигурирования/подстройки)
- Низкая нагрузка на процессор маршрутизатора
- Предсказуемость в каждый момент времени

Недостатки

- Очень плохое масштабирование (добавление (N+1)-ой сети потребует сделать $2*(N+1)$ записей о маршрутах, причём на большинстве маршрутизаторов таблица маршрутов будет различной, при $N > 3-4$ процесс конфигурирования становится весьма трудоёмким).
- Низкая устойчивость к повреждениям линий связи (особенно, в ситуациях, когда обрыв происходит между устройствами второго уровня и порт маршрутизатора не получает статус down).
- Отсутствие динамического балансирования нагрузки.
- Необходимость в ведении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

Применение статических маршрутов

- Сеть состоит из нескольких маршрутизаторов (1–3)
- Сеть подключается к Интернет только через одного провайдера
- Большая корпоративная сеть построена по принципу hub-and-spoke топологии, когда множество филиалов имеют только единственное подключение к центральному офису.

Перед использованием статической маршрутизации должны быть сконфигурированы сетевые интерфейсы маршрутизатора, активированы, получен несущий сигнал на интерфейсе и в таблице маршрутизации присутствуют записи о прямо подключенных сетях.

Динамические маршруты

Маршруты в таблицу маршрутизации заносятся автоматически, с помощью программных средств.

Динамические протоколы маршрутизации используются маршрутизаторами для обмена информацией о достижимости и статусе удаленных сетей.

Динамические протоколы маршрутизации представляют следующие услуги:

- **Сетевое обнаружение**
- **Обновление и поддержание таблицы маршрутизации**

Протоколы динамической маршрутизации:

- **RIP** (Routing Information Protocol, протокол маршрутной информации)
- **OSPF** (Open Shortest Path First, открыть кратчайший путь первым – алгоритм Дейкстры)
- **EIGRP** (Enhanced Interior Gateway Routing Protocol, усовершенствованный протокол маршрутизации внутренних шлюзов – алгоритм DUAL)
- **BGP** (Border Gateway Protocol, протокол граничного шлюза)
- **IS-IS** (Intermediate System to Intermediate System, протокол маршрутизации промежуточных систем)

Классификация протоколов динамической маршрутизации

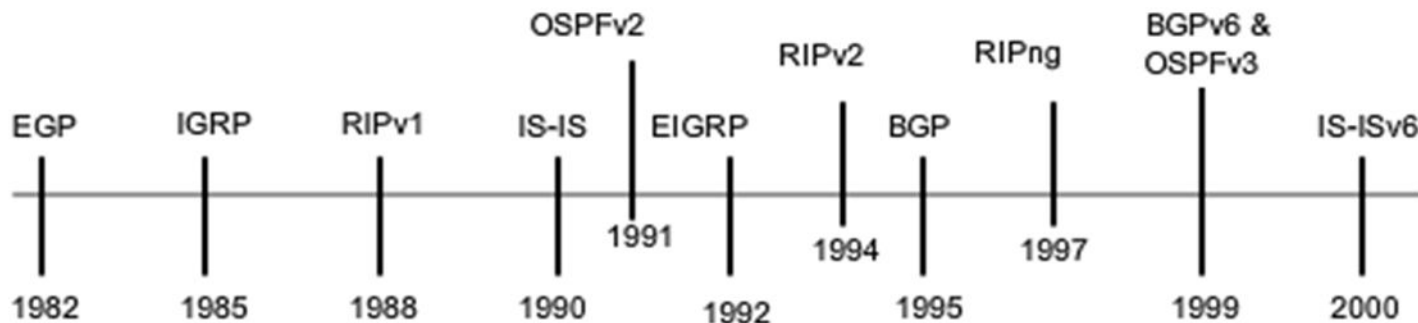
По алгоритмам:

- Дистанционно-векторные протоколы (Distance-vector Routing Protocols):
RIP
- Протоколы состояния каналов связи (Link-state Routing Protocols):
OSPF IS-IS
- Усовершенствованные дистанционно-векторные протоколы (advanced distance-vector):
EIGRP

По области применения:

- Междоменной маршрутизации:
BGP
- Внутридоменной маршрутизации:
OSPF RIP EIGRP IS-IS

Протоколы динамической маршрутизации



Interior Gateway Protocols

Exterior Gateway Protocols

Distance Vector Routing Protocols

Link State Routing Protocols

Path Vector

Classful	RIP	IGRP		EGP
Classless	RIPv2	EIGRP	OSPFv2	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	BGPv4 for IPv6
			IS-IS for IPv6	

Принципы маршрутизации

- Каждый маршрутизатор принимает решение о перенаправлении пакета самостоятельно, основываясь только на собственной таблице маршрутизации.
- Тот факт, что один маршрутизатор имеет определенные записи в своей таблице маршрутизации, не означает что другие маршрутизаторы имеют такие же записи в таблице.
- Маршрутная информация о пути следования пакетов из одной сети в другую, не предусматривает наличия маршрутной информации об обратном пути.

Достоинства и недостатки

Недостатки

- Более сложная отладка и конфигурирование.
- Наличие дополнительных накладных расходов (памяти и процессорного времени)
- Необходимо некоторое время после конфигурирования, прежде чем сеть заработает (время сходимости сети)
- Нагрузка на процессор маршрутизатора
- Повышенные требования навыков конфигурирования для администраторов

Достоинства

- Очень хорошее масштабирование (добавление (N+1)-ой сети потребует конфигурирования только добавляемой сети).
- Повышенная устойчивость к повреждениям линий связи (особенно, в ситуациях, когда обрыв происходит между устройствами второго уровня и порт маршрутизатора не получает статус down).
- Наличие динамической балансировки нагрузки.
- Необходимость в ведении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

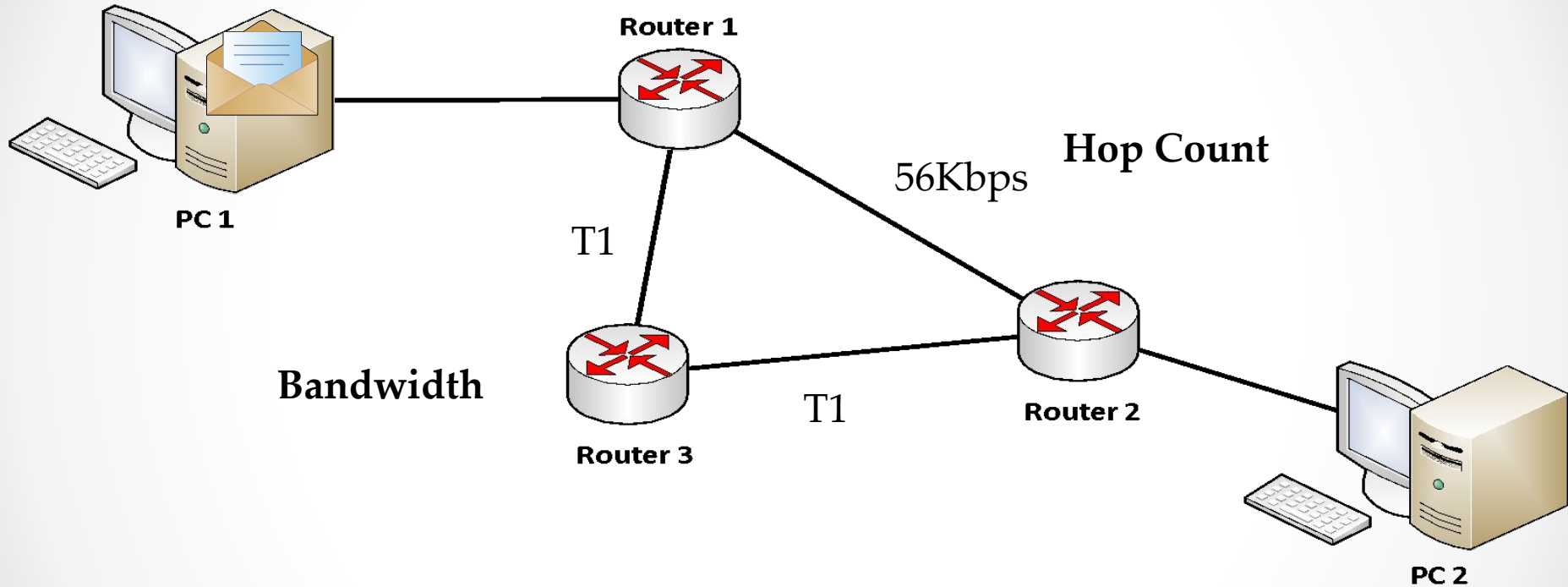
Метрика маршрута

Числовое значение, влияющее на выбор маршрута в компьютерных сетях.

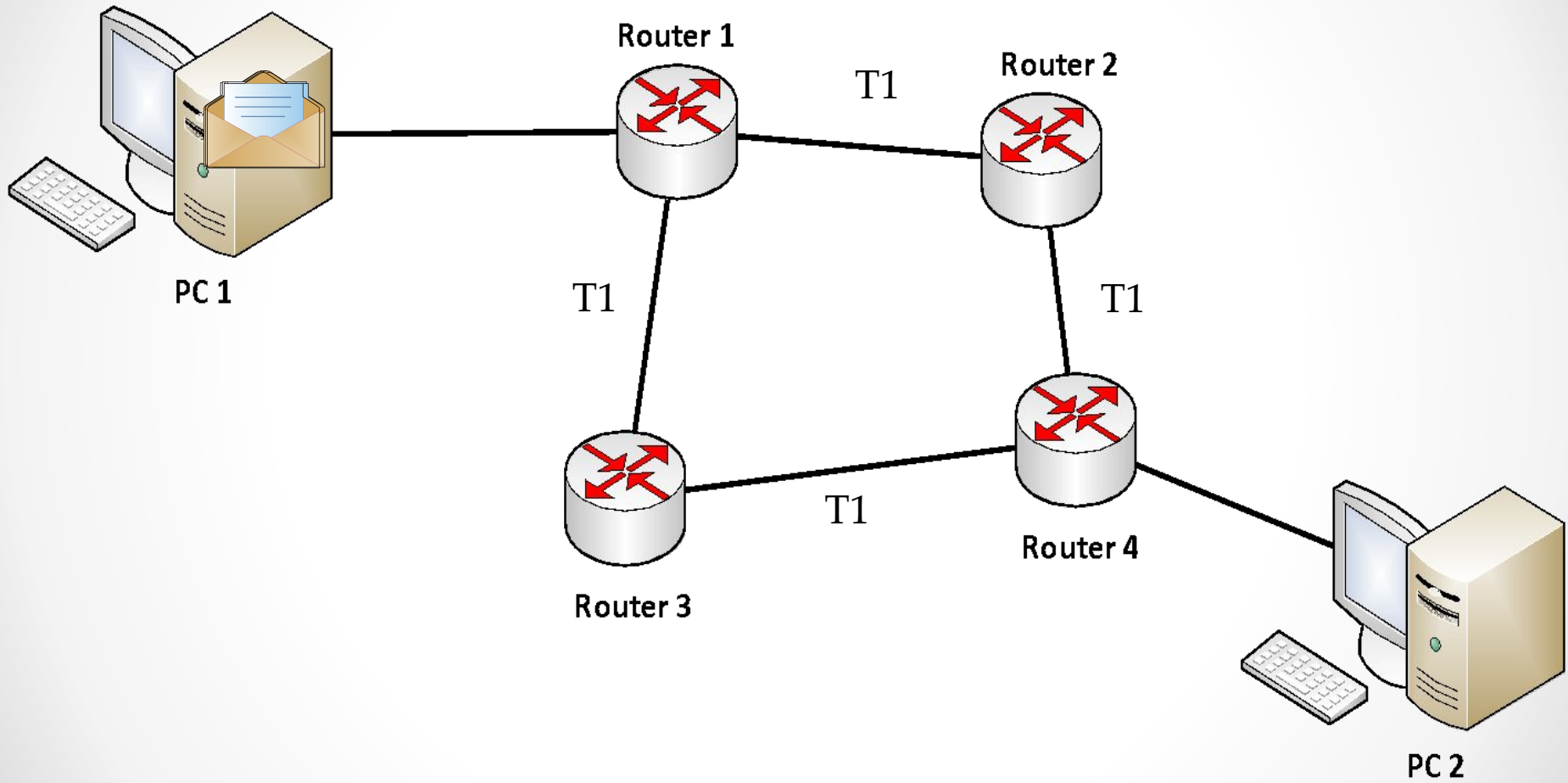
В статической маршрутизации метрика может задаваться вручную при конфигурировании статического маршрута или присваивается в виде значения по умолчанию.

Некоторые протоколы динамической маршрутизации (например, RIP) используют в качестве метрики количество «прыжков» до сети назначения. Другие протоколы, такие как OSPF, определяют кратчайший путь по вычислению суммарной ширины канала, каждого link'a между сетью источника и сетью назначения.

Метрика маршрута



Балансировка нагрузки



Программная и аппаратная маршрутизация

Первые маршрутизаторы представляли собой специализированное ПО, обрабатывающее приходящие IP-пакеты специфичным образом. Это ПО работало на компьютерах, у которых было несколько сетевых интерфейсов, входящих в состав различных сетей (между которыми осуществляется маршрутизация). В дальнейшем появились маршрутизаторы в форме специализированных устройств.

Компьютеры с маршрутизирующим ПО называют *программные маршрутизаторы*, оборудование – *аппаратные маршрутизаторы*.

В современных аппаратных маршрутизаторах для построения таблиц маршрутизации используется специализированное ПО ("прошивка" или специальная операционная система), для обработки же IP-пакетов используется коммутационная матрица (или другая технология аппаратной коммутации), расширенная фильтрами адресов в заголовке IP-пакета.

Аппаратная маршрутизация

Выделяют два типа аппаратной маршрутизации:

- **Статические шаблоны потоков** подразумевают разделение всех входящих в IP-пакетов на виртуальные потоки; каждый поток характеризуется набором признаков: IP-адресами отправителя и получателя, TCP/UDP-порт отправителя и получателя (если маршрутизатор поддерживает L4), физический порт (сетевой интерфейс). Оптимизация маршрутизации заключается в том, что все пакеты с одинаковыми признаками обрабатываются одинаково, при этом признаки проверяются только для первого пакета в потоке (при появлении пакета с другим набором признаков – создаётся новый поток), по результатам анализа пакета формируется статический шаблон, который используется для определения правил коммутации приходящих пакетов (внутри потока). Время хранения не используемого шаблона ограничено. Ключевым недостатком подобной схемы является то, что в случае существующего потока изменение правил маршрутизации пакетов не будет "замечены" до момента удаления шаблона).
- **Динамически адаптируемые таблицы** используют правила маршрутизации "напрямую", используя маску и номер сети из таблицы маршрутизации для проверки пакета и определения порта, на который нужно передать пакет. При этом изменения в таблице маршрутизации (в результате работы, например, протоколов маршрутизации/резервирования) сразу же влияют на обработку всех ново пришедших пакетов. Динамически адаптируемые таблицы также позволяют легко реализовывать быструю (аппаратную) проверку списков доступа (ACL).

Программная маршрутизация

Программная маршрутизация выполняется либо специализированным ПО маршрутизаторов (в случае, когда аппаратные методы не могут быть использованы, например, в случае организации туннелей), **либо программным обеспечением на компьютере (например, сервере)**. В общем случае, любой компьютер осуществляет маршрутизацию своих собственных исходящих пакетов (как минимум, для разделения пакетов, отправляемых на шлюз по умолчанию и пакетов, предназначенных узлам в локальном сегменте сети).

Для маршрутизации чужих IP-пакетов, а также построения таблиц маршрутизации используется различное ПО:

- **Сервис RRAS** (*Routing and remote access service*) в Windows Server
- **Демоны routed, gated, quagga** в Unix-подобных операционных системах (Linux, FreeBSD и т.д..)

Вопросы для подготовки к защите лабораторных работ

1. Основные понятия эталонной модели ISO/OSI. Стандарт ISO 7498
2. Соответствие модели стека протоколов TCP/IP модели OSI
3. Сетевой уровень модели стека протоколов TCP/IP
4. Функции сетевого уровня
5. Протоколы сетевого уровня. Протокол IP
6. IPv4 и IPv6 адрес. Конфигурирование протокола IPv4 и IPv6 в Windows и Linux
7. Заголовки протоколов IPv4 и IPv6
8. Адресное пространство IPv4. Типы адресов
9. IANA. Виды сетей IPv4 (публичные, приватные, специальные)
10. Типы передачи данных на сетевом уровне (unicast, multicast, broadcast)
11. Классовая и бесклассовая адресация
12. Протоколы сетевого уровня. Протокол ICMP
13. Использование протокола ICMP. Типы ICMP сообщений
14. Понятие маршрутизации. Понятие шлюза. Конфигурирование шлюза
15. Понятие таблицы маршрутизации. Основные столбцы таблицы маршрутизации. Виды записей в таблице маршрутизации

Вопросы для подготовки к защите лабораторных работ

16. Понятие маршрутизатора. Физическое устройство маршрутизатора. Логическая диаграмма маршрутизатора
17. Интерфейсы и сети маршрутизатора
18. Маршрутизатор и модель стека TCP/IP. Функционирование маршрутизатора
19. Содержимое таблицы маршрутизации на маршрутизаторе (прямо подключенные сети, статические маршруты, динамические маршруты)
20. Понятие маршрутизации. Статическая маршрутизация. Достоинства и недостатки. Применение
21. Понятие маршрутизации. Динамическая маршрутизация. Достоинства и недостатки. Применение
22. Динамическая маршрутизация. Протоколы динамической маршрутизации. Классификация протоколов динамической маршрутизации
23. Принципы маршрутизации. Метрика маршрута. Балансировка нагрузки
24. Понятие маршрутизации. Аппаратная маршрутизация и программная маршрутизация

**СПАСИБО ЗА
ВНИМАНИЕ!**

ВОПРОСЫ?

