

Лекция 11.

Протоколы сетевого уровня

Лекция 11. Протоколы сетевого уровня

- Протокол ICMP (ICMPv4 и ICMPv6)
- Протокол Neighbor Discovery Protocol (NDP)
- Протоколы маршрутизации
- Протокол Routing Information Protocol (RIP)

Internet Control Message Protocol (ICMP)

- ✓ Протокол IP является базовым протоколом сетевого уровня стека TCP/IP, т.к. отвечает за доставку пакетов через составную сеть.
- ✓ Протокол IP доставляет пакеты *без установления соединения, без обеспечения надежности и без подтверждения доставки.*
- ✓ Протокол IP не обладает механизмами отправки служебных сообщений, которые позволяли бы сообщать устройству-отправителю о проблемах, возникающих при передаче, выполнять тестирование соединения.
- ✓ Недостающие функции выполняются протоколом *Internet Control Message Protocol (ICMP).*
- ✓ ICMP является неотъемлемой частью IP и обязателен при реализации стека TCP/IP. Он обеспечивает поддержку IP в форме ICMP-сообщений.
- ✓ ICMP-сообщения используют единый общий формат и инкапсулируются в пакеты IP. Они разделены на разные типы, каждый из которых имеет специальное назначение и формат внутреннего поля (содержание сообщения).

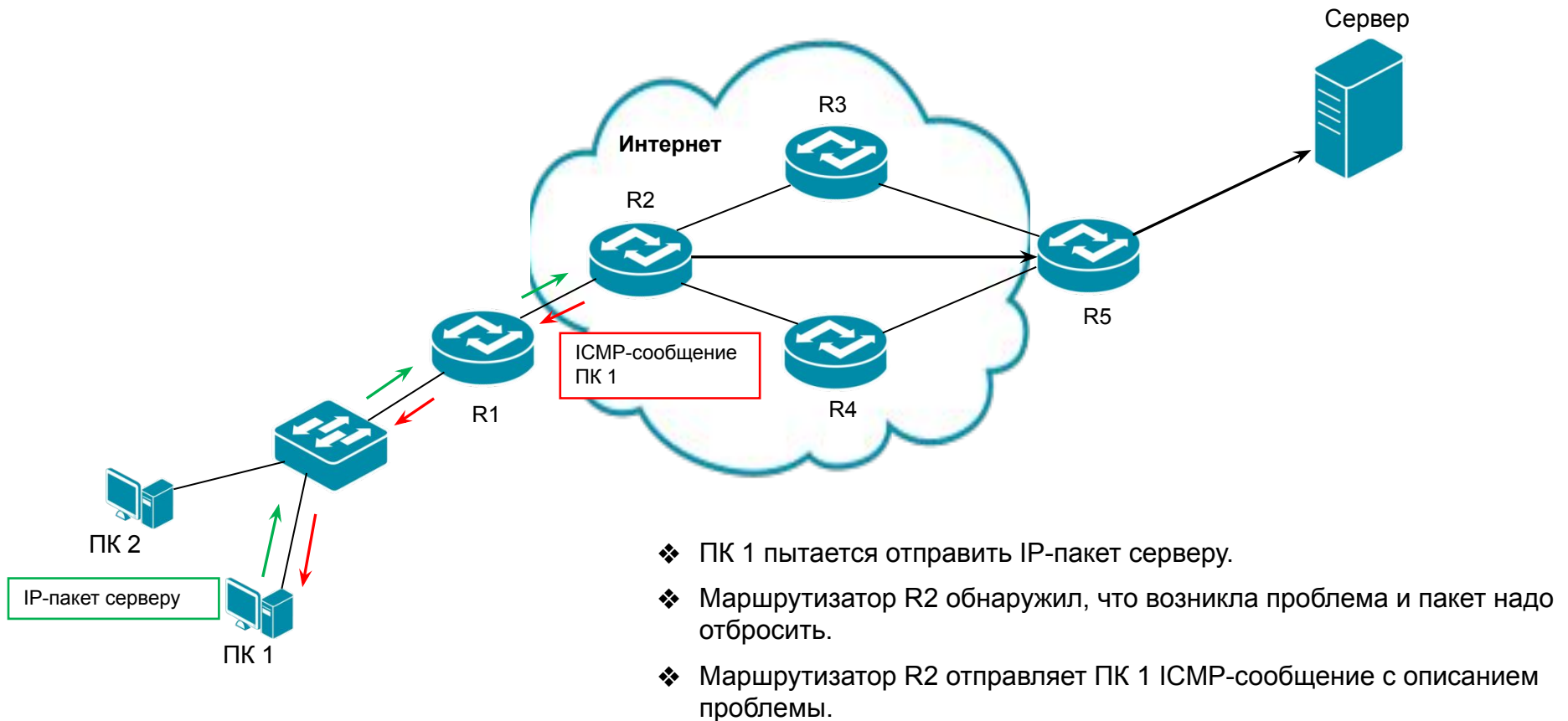
- ❑ Оригинальная версия ICMP для IPv4 называется *ICMPv4*, новая версия для IPv6 называется *ICMPv6*.
- ❑ Базовые операции протоколов ICMPv4 и ICMPv6 описаны в RFC 792 и RFC 2463 соответственно.
- ❑ Обе версии протокола ICMPv4 и ICMPv6 определяют общую систему передачи сообщений, т.е. в дополнение к сообщениям, определенным протоколом ICMP, другие протоколы также могут определять свои типы сообщений ICMP.

Протоколы, определяющие сообщения ICMP

Версия ICMP	RFC	Название	Определяемые типы сообщений ICMP
ICMPv4	950	<u>Internet Standard Subnetting Procedure</u>	Address Mask Request, Address Mask Reply
	1256	<u>ICMP Router Discovery Messages</u>	Router Advertisement, Router Solicitation
	1393	<u>Traceroute Using an IP Option</u>	Traceroute
	1812	<u>Requirements for IP Version 4 Routers</u>	Определяет три кода (подтипа) для сообщения Destination Unreachable.
ICMPv6	2461	<u>Neighbor Discovery for IP Version 6 (IPv6)</u>	Router Advertisement, Router Solicitation, Neighbor Advertisement, Neighbor Solicitation, Redirect
	2894	<u>Router Renumbering for IPv6</u>	Router Renumbering

Общие операции ICMP

- ✓ Протокол ICMP отличается от других протоколов стека TCP/IP тем, что не выполняет определенные задачи. Он определяет механизм, с помощью которого могут передаваться и приниматься различные управляющие сообщения, обеспечивая выполнение разнообразных функций.



- ✓ При обнаружении проблемы ICMP-сообщение отправляется только устройству-источнику пакета.

Формат сообщения ICMP

Сообщения ICMPv4 и ICMPv6 имеют одинаковый базовый формат:

Бит	0-7	8-15	16-32
0	Type	Code	Checksum
32	Содержание сообщения (зависит от значений полей «Type» и «Code»)		

Type (Тип): определяет тип сообщения ICMP.

Code (Код): определяет подтип сообщения внутри ICMP-сообщения каждого типа.

Checksum (Контрольная сумма): вычисляется аналогично контрольной сумме заголовка IPv4.

Классы, типы и коды сообщений ICMP

Сообщения ICMP делятся на два класса:

- ❑ **Сообщения об ошибках:** используются для извещения устройства-отправителя о проблемах, возникших при передаче пакета. Обычно генерируются в ответ на какое-либо событие, возникшее при передаче пакета.
- ❑ **Информационные сообщения:** используются для диагностики, тестирования, обмена информацией и других целей. Не содержит описания ошибок и обычно не отправляется при возникновении какого-либо события, возникшего при передаче пакета. Могут генерироваться соответствующим приложением, либо как ответ на другое информационное сообщение ICMP, либо на постоянной основе для предоставления информации другим устройствам.

Типы сообщений ICMP

- ✓ Каждому сообщению ICMP присваивается уникальное значение типа, которое указывается в 8-битном поле Type пакета ICMP.
- ✓ Для ICMPv4 и ICMPv6 может быть определено до 256 различных типов сообщений (отдельный набор для каждого протокола).
- ✓ В ICMPv4 значения типа назначаются последовательно для информационных сообщений и сообщений об ошибках.
- ✓ В ICMPv6 сообщениям об ошибках в поле Type присваиваются значения с 0 по 127, информационным сообщениям – с 128 по 255.

Коды сообщений ICMP

- ✓ Тип сообщения указывает на общее предназначение каждого сообщения ICMP. Коды, указываемые в 8-битном поле Code пакета ICMP вносят дополнительный уровень детализации.
- ✓ Каждый тип сообщения может иметь до 256 подтипов.

Классы, типы и коды сообщений ICMP

Класс сообщения	Значение Type	Название сообщения	Описание типа сообщения
Сообщения об ошибках ICMPv4	3	<i>Destination Unreachable</i>	Указывает, что пакет не может быть доставлен адресату. Код сообщения указывает причину ошибки.
	5	<i>Redirect</i>	Позволяет маршрутизатору информировать узел о наилучшем маршруте передачи пакета..
	11	<i>Time Exceeded</i>	Отправляется, когда пакет отбрасывается по причине достижения его полем Time To Live (TTL) значения 0.
	12	<i>Parameter Problem</i>	Указывает, что при доставке существуют проблемы с параметрами пакета
Информационные сообщения ICMPv4	0	<i>Echo Reply</i>	Отправляется в ответ на сообщение <i>Echo (Request)</i> , используется для тестирования соединения.
	8	<i>Echo Request</i>	Отправляется устройством при тестировании соединения с другим устройством в сети.
	9	<i>Router Advertisement</i>	Используется маршрутизаторами для объявления о своем существовании и возможностях.
	10	<i>Router Solicitation</i>	Запрос маршрутизатора на отправку <i>Router Advertisement</i> .
	30	<i>Traceroute</i>	Используется для трассировки маршрута утилитой <i>traceroute</i> .
Сообщения об ошибках ICMPv6	1	<i>Destination Unreachable</i>	Указывает, что пакет не может быть доставлен адресату. Код сообщения указывает причину ошибки.
	2	<i>Packet Too Big</i>	Отправляется, когда пакет не может быть передан, т.к. слишком большой для MTU следующего маршрутизатора на пути следования. Это сообщение требуется только в IPv6, т.к. в IPv4 маршрутизатор может фрагментировать большие пакеты.
	3	<i>Time Exceeded</i>	Отправляется, когда пакет отбрасывается по причине достижения его полем <i>Hop Limit</i> значения 0.
	4	<i>Parameter Problem</i>	Указывает, что при доставке существуют проблемы с параметрами пакета.
Информационные сообщения ICMPv6	128	<i>Echo Request</i>	Отправляется устройством при тестировании соединения с другим устройством в сети.
	129	<i>Echo Reply</i>	Отправляется в ответ на сообщение <i>Echo (Request)</i> .
	133	<i>Router Solicitation</i>	Запрос маршрутизатора на отправку <i>Router Advertisement</i> .
	134	<i>Router Advertisement</i>	Используется маршрутизаторами для объявления о своем существовании и возможностях.
	135	<i>Neighbor Solicitation</i>	Отправляется устройством при запросе адреса канального уровня другого устройства.
	136	<i>Neighbor Advertisement</i>	Объявление информации об узле другим устройствам сети
	137	<i>Redirect</i>	Перенаправление передачи от узла ближайшему соседу в сети или маршрутизатору.

Правила генерации сообщений ICMP

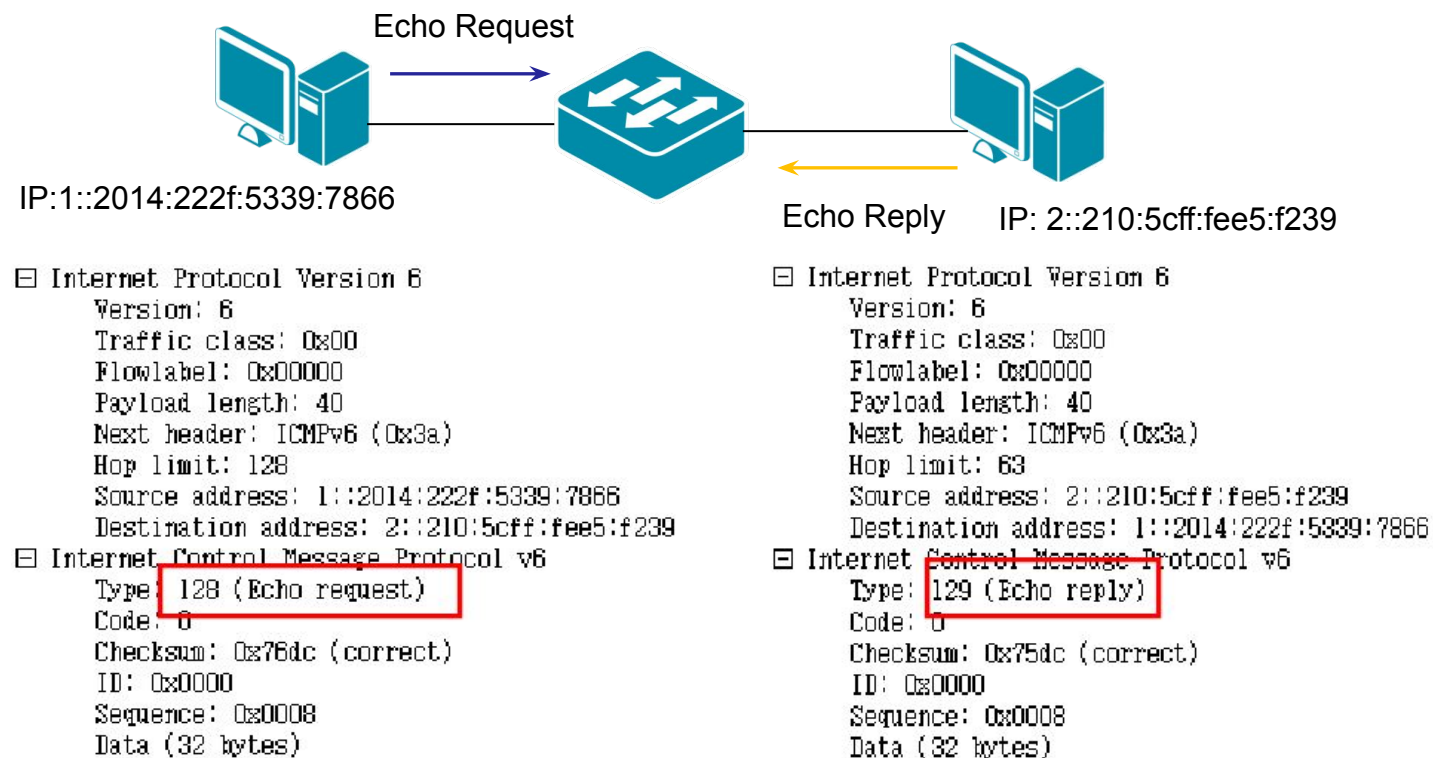
- ❑ Информационные ICMP-сообщения генерируются в соответствии с правилами, установленными использующими их протоколами.
- ❑ ICMP-сообщения об ошибках генерируются в ответ на какое-либо событие, возникшее при передаче пакета. Может возникнуть ситуация, при которой узлы начнут отправлять сообщения об ошибках друг другу, что приведет к петлям или отправке множественных сообщений. Для предотвращения таких проблем, ICMP-сообщения об ошибках **не должны** генерироваться в ответ на:
 - ICMP-сообщения об ошибках.
 - IP-пакеты с широковещательным или групповым адресом, чтобы не вызывать перегрузку в сети («широковещательный шторм»).
 - Фрагменты IP-пакетов за исключением первого – при повреждении фрагментированного IP-пакета ICMP-сообщение отправляется только после получения первого поврежденного фрагмента, поскольку отправитель все равно повторит передачу всего IP-пакета целиком.

Исключения:

- В некоторых случаях сообщение ICMPv6 Packet Too Big может генерироваться в ответ на широковещательный адрес, т.к. это требуется для работы механизма Path MTU Discovery.
- Некоторые сообщения Parameter Problem также могут отправляться на широковещательные или групповые адреса.

Утилита Ping

- Ping** — это утилита для проверки соединений в сетях на основе TCP/IP, которая отправляет запросы ICMP Echo Request указанному узлу сети и фиксирует поступающие ответы ICMP Echo Reply.



Утилита Ping

✓ Утилита ping является одним из основных диагностических средств в сетях TCP/IP.

Практическое применение:

- ❖ Проверка соединения с требуемым узлом: **ping <IP addr>** или **ping <доменное имя>**
- ❖ Определение IP-адреса по доменному имени: **ping -a <доменное имя>**
- ❖ Можно оценить качество канала, посмотрев статистику об отправленных и потерянных пакетах.

```
c:\>ping 173.194.35.223
```

```
Обмен пакетами с 173.194.35.223 по с 32 байтами данных:  
Ответ от 173.194.35.223: число байт=32 время=2мс TTL=57  
Ответ от 173.194.35.223: число байт=32 время=1мс TTL=57  
Ответ от 173.194.35.223: число байт=32 время=2мс TTL=57  
Ответ от 173.194.35.223: число байт=32 время=1мс TTL=57
```

```
Статистика Ping для 173.194.35.223:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 1мсек, Максимальное = 2 мсек, Среднее = 1 мсек
```

```
c:\>ping -a www.google.ru
```

```
Обмен пакетами с www-cs1d.l.google.com [173.194.35.216] с 32 байтами данных:  
Ответ от 173.194.35.216: число байт=32 время=2мс TTL=57  
Ответ от 173.194.35.216: число байт=32 время=5мс TTL=57  
Ответ от 173.194.35.216: число байт=32 время=2мс TTL=57  
Ответ от 173.194.35.216: число байт=32 время=6мс TTL=57
```

```
Статистика Ping для 173.194.35.216:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 2мсек, Максимальное = 6 мсек, Среднее = 3 мсек
```

```
c:\>ping 2001:470:c8eb:1::4204
```

```
Обмен пакетами с 2001:470:c8eb:1::4204 по с 32 байтами данных:  
Ответ от 2001:470:c8eb:1::4204: время<1мс  
Ответ от 2001:470:c8eb:1::4204: время<1мс  
Ответ от 2001:470:c8eb:1::4204: время<1мс  
Ответ от 2001:470:c8eb:1::4204: время<1мс
```

```
Статистика Ping для 2001:470:c8eb:1::4204:
```

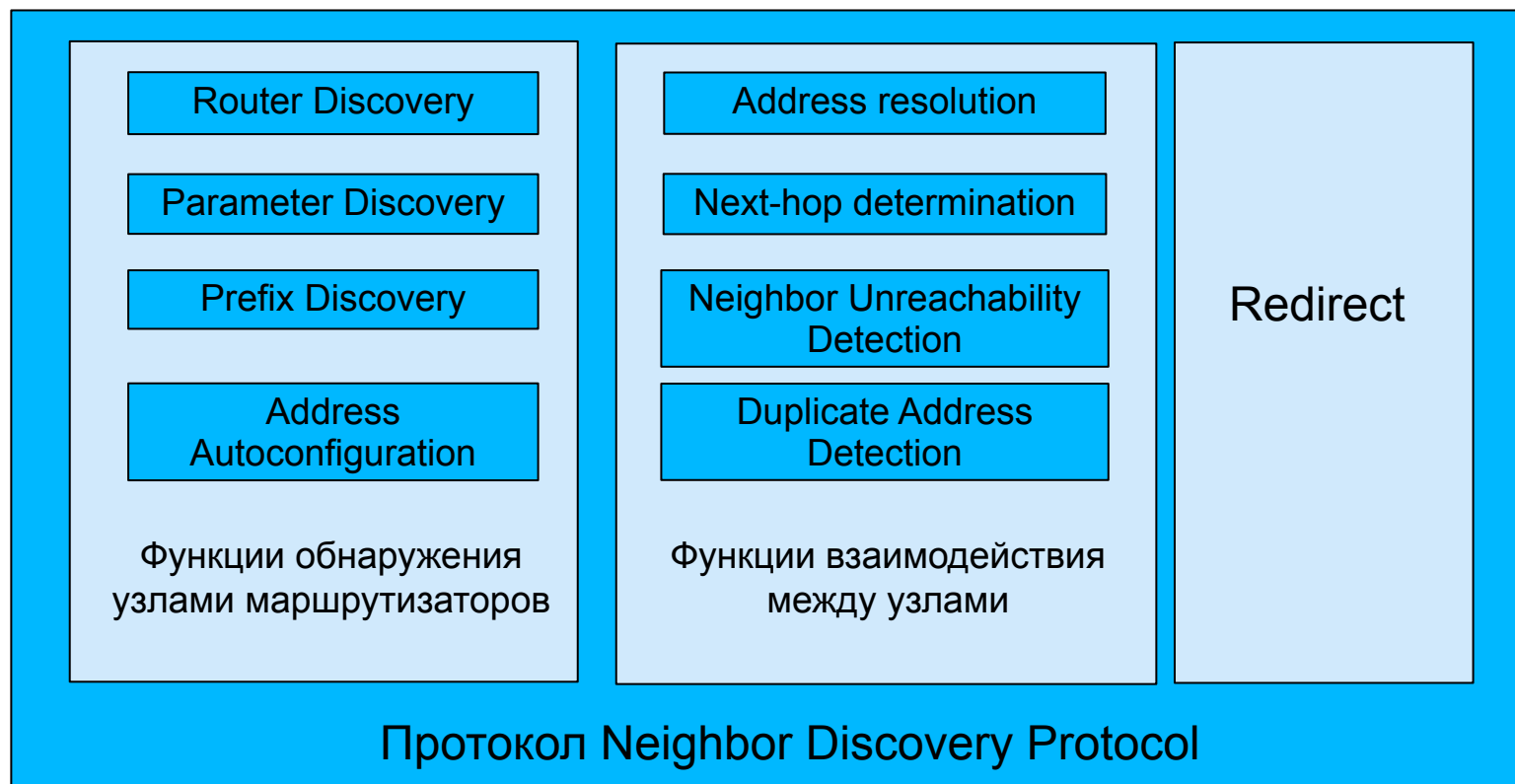
```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Протокол Neighbor Discovery

- Протокол Neighbor Discovery Protocol (NDP) – протокол стека TCP/IP, используемый совместно с IPv6 и определен в RFC 2461.
- Протокол объединяет ряд функций, относящихся к взаимодействию устройств в локальной сети, которые в IPv4 выполняются протоколами ARP и ICMP.
- Протокол NDP предоставляет механизмы для выполнения следующих функций:



Протокол Neighbor Discovery

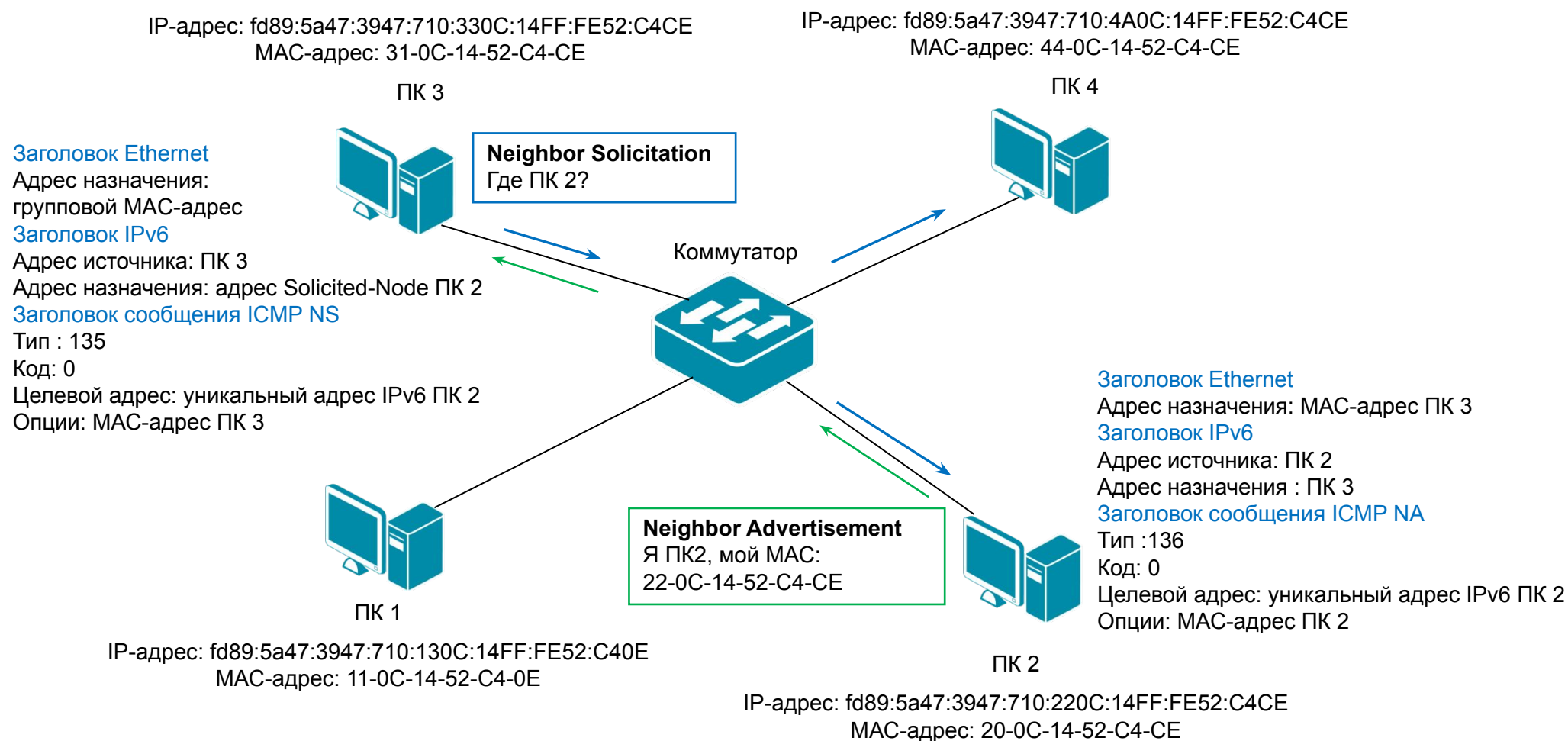
Протокол NDP определяет 5 типов сообщений ICMP:

- **Router Solicitation:** отправляется узлами, для того чтобы запросить любой локальный маршрутизатор мгновенно отправить сообщение Router Advertisement не дожидаясь следующего периодического объявления. Используется при автоконфигурации узла.
- **Router Advertisement:** отправляются маршрутизаторами регулярно, чтобы объявить о своем существовании в сети и предоставить узлам важную информацию о префиксе и/или параметрах, или в ответ на сообщение Router Solicitation.
- **Neighbor Solicitation:** отправляется узлом, чтобы определить адрес канального уровня соседнего устройства или проверить, что сосед все еще доступен через адрес канального уровня, хранимый в кэше. Также используется для определения дублирования адресов (Duplicate Address Detection).
- **Neighbor Advertisement:** отправляется в ответ на сообщение Neighbor Solicitation. Также может быть отправлено узлом при изменении адреса канального уровня.
- **Redirect:** используется маршрутизаторами для уведомления узлов о наилучшем маршруте к пункту назначения.

Разрешение адресов с помощью протокола Neighbor Discovery

Для выполнения функции разрешения адресов в протоколе NDP используется два сообщения ICMPv6:

- *Neighbor Solicitation (NS)* – для того чтобы узнать адрес канального уровня, узел отправляет сообщение на групповой адрес *Solicited-Node* целевого адреса IPv6.
- *Neighbor Advertisement (NA)* – ответ на сообщение Neighbor Solicitation, в котором содержится адрес канального уровня.



Определение недоступности соседа (Neighbor Unreachability Detection)

- *Neighbor Unreachability Detection* (определение недоступности соседа) позволяет отслеживать состояние каналов связи между соседними узлами локальной сети.
- Каждое устройство хранит в кэше (*neighbor cache*) информацию о соседнем устройстве локальной сети (узлах и маршрутизаторах).
- Сосед считается доступным, если от него пришло подтверждение, что отправленный ему пакет был успешно принят. Подтверждение может быть получено с помощью протокола верхнего уровня или при получении сообщения *Neighbor Advertisement* в ответ на отправленное сообщение *Neighbor Solicitation*.
- Каждый раз, когда в результате успешного выполнения разрешения адресов в кэше создается запись о соседе, ей присваивается статус REACHABLE и устанавливается таймер. После истечения таймера, информация о соседе переходит в состояние STALE, и предполагается, что сосед больше не доступен. После того, как будет получено подтверждение доступности соседа, состояние записи изменится на REACHABLE и таймер перезапустится.
- Операции функции Neighbor Unreachability Detection выполняются параллельно с отправкой пакетов соседним устройствам. Если между соседями нет обмена трафиком, сообщения-зонды не отправляются.

Определение дублирования адресов (Duplicate Address Detection, DAD)

- Когда узел использует механизм автоконфигурации IPv6, одним из первых шагов этого процесса является определение того, что адрес Link-Local, который он желает получить, не используется уже другим узлом.
- Duplicate Address Detection (определение дублирования адресов) выполняется путем отправки сообщения Neighbor Solicitation на тот IP-адрес, который устройство хочет использовать.
- Если будет в ответ получено сообщение Neighbor Advertisement, значит, адрес уже используется.

Обнаружение маршрутизатора (Router Discovery)

- Одной из важных функций протокола NDP является реализация процесса обнаружения узлами локальных маршрутизаторов – *Router Discovery*, которая позволяет узлам локальной сети обнаруживать соседние маршрутизаторы и получать от них сетевые параметры, необходимые для автоконфигурации.
- Операция обнаружения узлами маршрутизаторов выполняется с помощью сообщений ICMPv6 *Router Advertisement* и *Router Solicitation*.

□Обработка объявлений:

узлы прослушивают объявления *Router Advertisement*, передаваемые маршрутизаторами по локальной сети через определенные интервалы и обрабатывают их. Объявления содержат список префиксов, в том числе необходимых для автоконфигурации, а также могут включать информацию о шлюзе по умолчанию.

□Генерация запросов:

при определенных условиях узлы могут генерировать сообщения *Router Solicitation* и отправлять их в локальную сеть (например, узел загружается и ему требуются параметры для конфигурации интерфейса). С помощью этого сообщения узел запрашивает любой локальный маршрутизатор о мгновенном предоставлении информации, т.е. отправке узлу сообщения *Router Advertisement*.

□Автоконфигурация:

если в сети настроена функция автоконфигурации, узел будет использовать информацию, полученную от локального маршрутизатора, чтобы автоматически сконфигурировать свой IP-адрес и другие параметры.

- ✓ Формат пакетов сообщений *Router Advertisement* и *Router Solicitation* опционально может включать информацию об адресе канального уровня. Это делается для того, чтобы сэкономить время на операции разрешения адресов и обновить кэш.

Понятие маршрутизации

□ *Маршрутизация* - процесс определения маршрута следования информации от отправителя к получателю в составной сети.

□ Маршрутизация выполняется специальными устройствами — *маршрутизаторами*.

□ Маршрутизаторы принимают решение о том куда передавать пакет на основе его сетевого адреса назначения, который сравнивается с информацией, хранимой в специальных *таблицах маршрутизации*.

□ *Таблица маршрутизации* — электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, описывающая соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора.

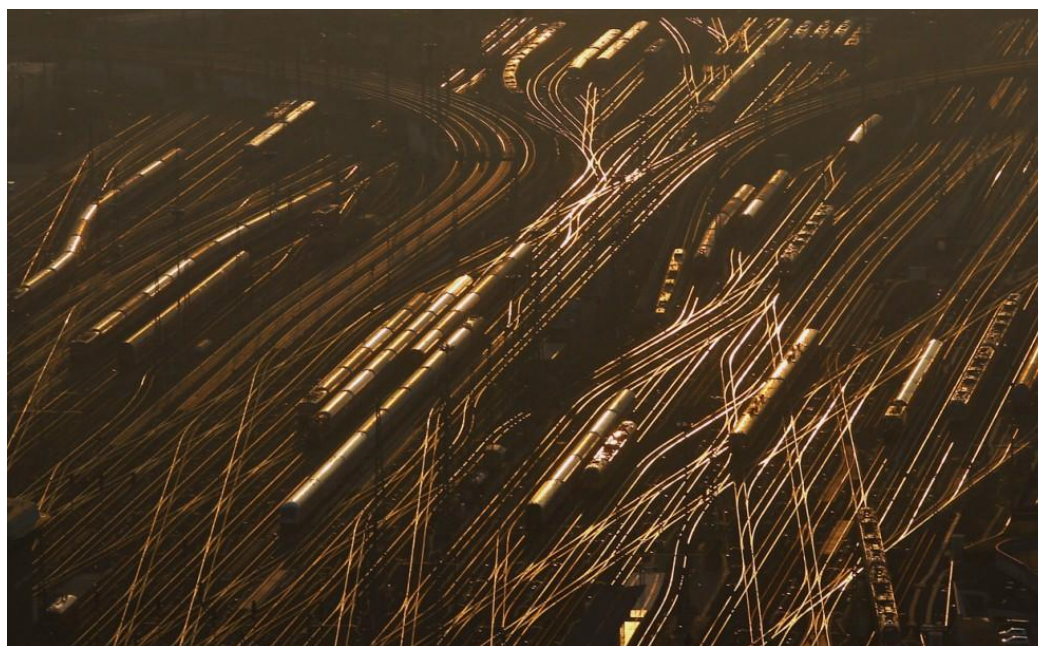


Таблица маршрутизации

- Таблица маршрутизации содержит записи, представляющие собой список наилучших доступных маршрутов.
- Существуют 4 типа записей таблицы маршрутизации:
 - Статический маршрут (Static Route)
 - Динамический маршрут (Dynamic Route)
 - Маршрут по умолчанию (Default Route)
 - Локальный маршрут (Local Route)

```
DGS-3620-28TC:admin#show iproute
Command: show iproute
```

Routing Table

IP Address/Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0/8	0.0.0.0	System	1	Local
172.16.0.0/23	172.16.8.2	iptv-1	2	RIP
172.16.2.0/23	172.16.8.2	iptv-1	2	RIP
172.16.8.0/30	0.0.0.0	iptv-1	1	Local
172.16.8.4/30	0.0.0.0	iptv-2	1	Local
172.16.8.8/30	172.16.8.6	iptv-2	2	RIP
172.16.8.12/30	0.0.0.0	stream	1	Local

```
Total Entries: 7
```

Таблица маршрутизации

- Каждая запись таблицы маршрутизации содержит следующую обязательную информацию:
 - **Адрес назначения** — адрес сети (в некоторых случаях узла) назначения;
 - **Маска сети** — маска, соответствующая адресу назначения (для сетей IPv4 маска /32 (255.255.255.255) позволяет указать единичный узел сети);
 - **Адрес шлюза** — IP-адрес интерфейса следующего транзитного маршрутизатора, находящегося на пути к получателю;
 - **Интерфейс** — идентификатор выходного интерфейса, через который пакет покидает устройство;
 - **Метрика** — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).
 - **Тип протокола** - информация о протоколе маршрутизации, создавшем запись в таблице маршрутизации.

```
DGS-3620-28TC:admin#show iproute
Command: show iproute
```

Routing Table

IP Address/Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0/8	0.0.0.0	System	1	Local
172.16.0.0/23	172.16.8.2	iptv-1	2	RIP
172.16.2.0/23	172.16.8.2	iptv-1	2	RIP
172.16.8.0/30	0.0.0.0	iptv-1	1	Local
172.16.8.4/30	0.0.0.0	iptv-2	1	Local
172.16.8.8/30	172.16.8.6	iptv-2	2	RIP
172.16.8.12/30	0.0.0.0	stream	1	Local

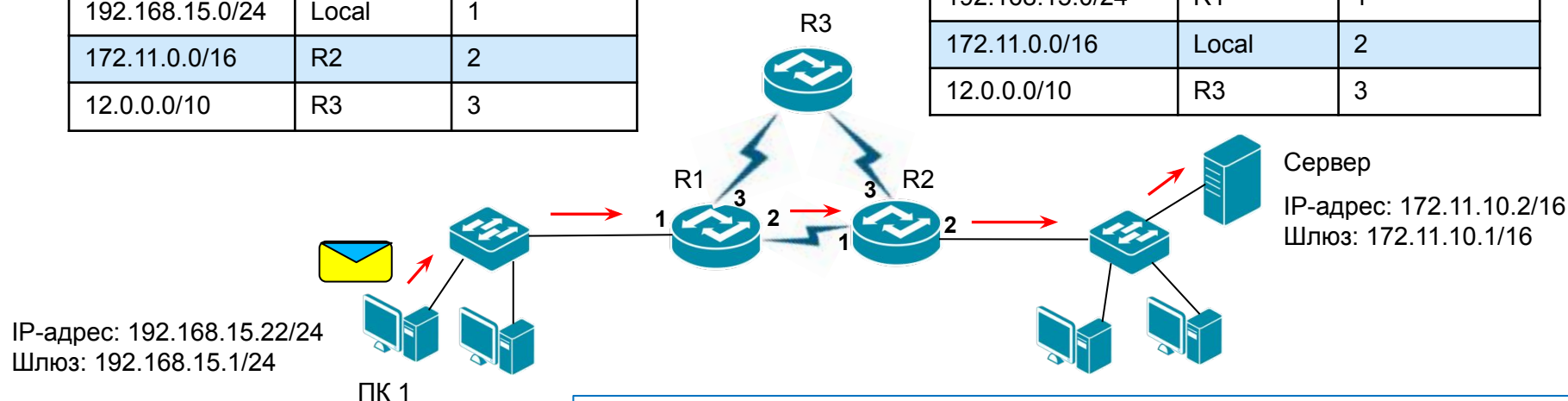
```
Total Entries: 7
```


Процесс обработки пакета маршрутизатором

1. Маршрутизатор получает кадр на интерфейс.
2. Проверяет полученный кадр и если он не поврежден, извлекает из него пакет сетевого уровня.
3. Извлекает из заголовка сетевого уровня IP-адрес получателя.
4. Сравнивает IP-адрес назначения с записями в таблице маршрутизации.
5. Если соответствие найдено, данные передаются на нужный интерфейс, если нет – пакет отбрасывается и отправителю отправляется ICMP-сообщение «Destination Unreachable» (Получатель недоступен).
6. Модифицирует некоторые поля пакета, например TTL, изменяет контрольную сумму.
7. Формирует новый кадр, инкапсулируя в него пакет.
8. Пересылает кадр следующему на пути маршрутизатору.

IP-адрес/маска	Маршрут	Интерфейс
192.168.15.0/24	Local	1
172.11.0.0/16	R2	2
12.0.0.0/10	R3	3

IP-адрес/маска	Маршрут	Интерфейс
192.168.15.0/24	R1	1
172.11.0.0/16	Local	2
12.0.0.0/10	R3	3



Сетевой уровень		192.168.15.22	171.11.10.2			
Канальный уровень		DA Сервер	SA R2.2	192.168.15.22	171.11.10.2	

Процесс поиска маршрута в таблице маршрутизации

1. Маршрутизатор извлекает из заголовка сетевого уровня IP-адрес получателя.
2. К IP-адресу применяется маска подсети первой записи таблицы, выполняется операция логического И, чтобы определить адрес сети.
3. Полученный адрес сети сравнивается с записью в таблице маршрутизации.
4. Если значения совпали, пакет пересылается на соответствующий интерфейс/порт маршрутизатора.
5. Если значения не совпали, то аналогичным описанному выше способом проверяется следующая запись в таблице маршрутизации.
6. Если совпадения не найдено, маршрутизатор проверяет, имеется ли у него маршрут по умолчанию.
7. Если маршрут по умолчанию настроен (Default Route), то пакет передается на соответствующий ему интерфейс/порт маршрутизатора.
8. Если маршрут по умолчанию не найден, пакет отбрасывается и отправителю отправляется сообщение об ошибке с помощью протокола ICMP.

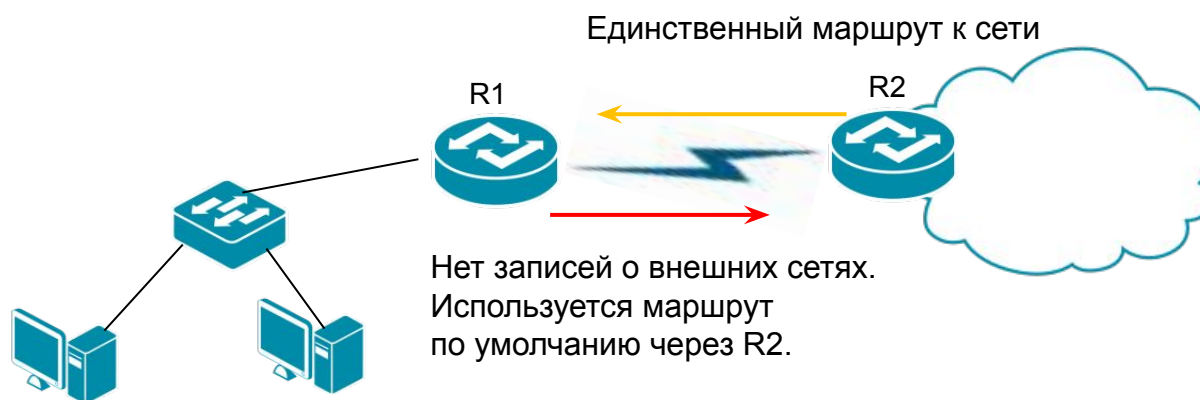
Новые маршруты могут добавляться в таблицу маршрутизации с помощью:

- **Статической маршрутизации:** записи о маршрутах вносятся и изменяются в таблицах маршрутизации вручную.
- **Динамической маршрутизации:** записи о маршрутах заносятся и обновляются в таблицах с помощью протоколов маршрутизации (*routing protocols*).

Статическая маршрутизация

Статическую маршрутизацию полезно использовать в следующих случаях:

- Если к сети имеется небольшое число маршрутов;
- Если по соображениям безопасности необходимо скрыть определенную информацию о сетях с ограниченным доступом;
- Для создания маршрутов по умолчанию.
- *Маршрут по умолчанию* – это маршрут, который используется в том случае, если другой маршрут к пункту назначения неизвестен.



Динамическая маршрутизации

- Динамическая маршрутизация выполняет две важные функции:
 - Обслуживание таблицы маршрутизации;
 - Своевременный обмен данными о маршрутах между маршрутизаторами в форме обновлений.
- Для обмена информацией маршрутизаторы используют протоколы маршрутизации (*Routing protocols*).
- Протоколы маршрутизации определяют наборы правил, используемые маршрутизаторами при взаимодействии друг с другом.
- Маршрутизаторы могут поддерживать сразу несколько протоколов маршрутизации и вести для них отдельные таблицы маршрутизации.

Термины Routed и Routing Protocols

Существуют разница между терминами «маршрутизируемый протоколом» (*Routed protocols*) и «протокол маршрутизации» (*Routing protocols*).

- **Маршрутизируемый протокол** – любой сетевой протокол, который определяет в формате пакета поля, содержащие адресную информацию сетевого уровня, позволяющую осуществлять маршрутизацию. Пример: протоколы IPv4/v6, IPX.
- **Протокол маршрутизации** – поддерживает маршрутизируемые протоколы и используется для обмена маршрутной информацией между маршрутизаторами. Пример: протоколы RIP (Routing Information Protocol), OSPF (Open Shortest Path First).

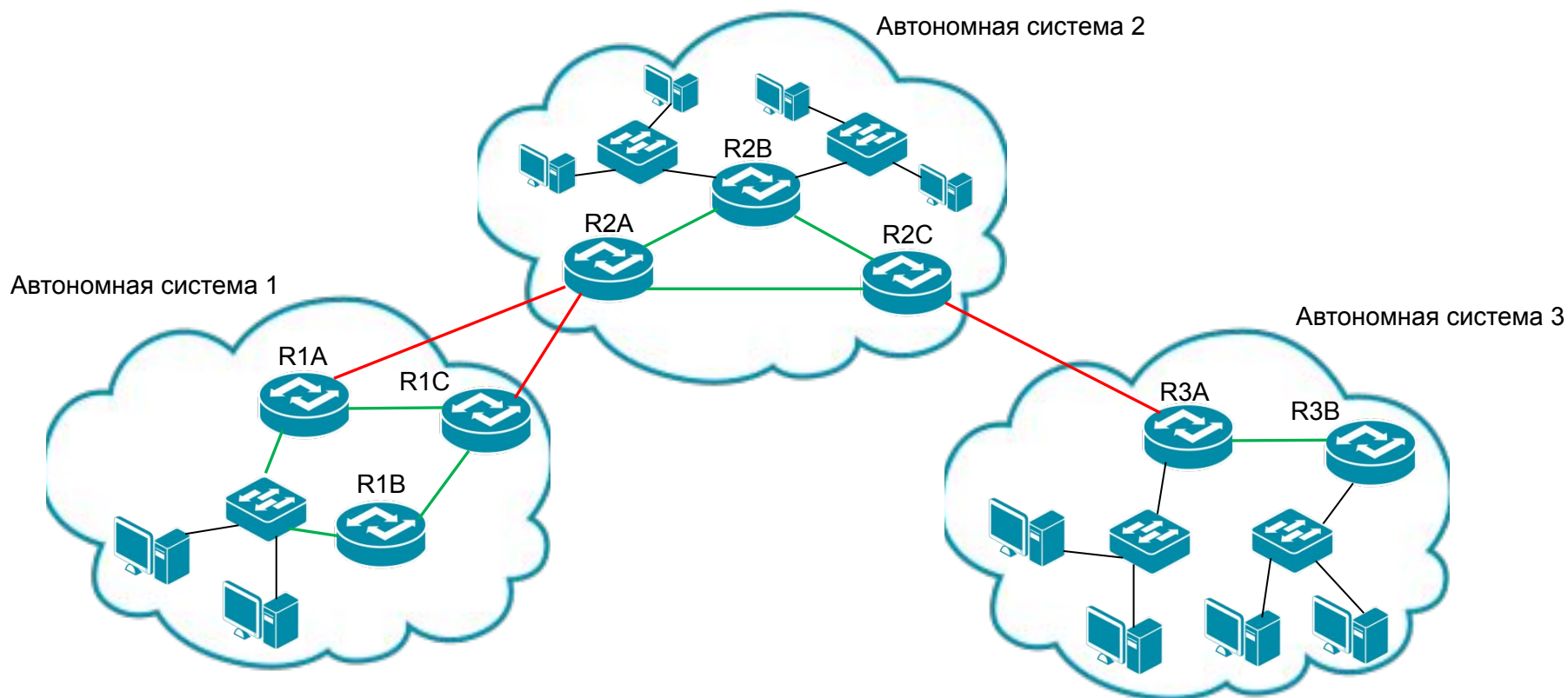
Протоколы маршрутизации

□ Существует два типа протоколов маршрутизации :

■ **Внутренние протоколы маршрутизации** (*Interior Routing Protocols*): используются для обмена маршрутной информацией внутри автономной системы.

■ **Внешние протоколы маршрутизации** (*Exterior Routing Protocols*): используются для обмена маршрутной информацией между автономными системами.

□ **Автономная система** (*Autonomous system, AS*) представляет собой группу маршрутизаторов и IP-сетей, контролируемых одной организацией или находящихся под единым административным управлением, которые используют единую согласованную политику для внутренней маршрутизации.



Понятие метрики

- ✓ Протоколы динамической маршрутизации отличаются используемыми алгоритмами маршрутизации и метриками.
 - ✓ **Алгоритм маршрутизации** – это метод, который протокол маршрутизации использует для определения наилучшего маршрута к месту назначения и последующего включения его в таблицу маршрутизации.
 - ✓ Для каждого маршрута алгоритм вычисляет число, называемое **метрикой** (*metric*).
 - ✓ Для того, чтобы определить среди нескольких маршрутов наилучший маршрут до пункта назначения, алгоритмы маршрутизации сравнивают их метрики. Чем меньше метрика, тем лучше маршрут.
 - ✓ Метрики можно вычислять как на основе одной характеристики сети, так и нескольких.
- Наиболее употребительные метрики следующие:
- Количество переходов (*Hop count*) – количество маршрутизаторов, через которое должен пройти пакет, прежде чем попасть к получателю;
 - Задержка передачи (*Delay*) – время, требуемое на передачу пакета от отправителя получателю;
 - Надежность линии связи (*Reliability*) – обозначает относительное значение количества ошибок для каждого из каналов связи;
 - Загруженность (*Load*) – загруженность маршрутизатора или канала связи;
 - Полоса пропускания (*Bandwidth*) – полоса пропускания канала связи;
 - Стоимость (*Cost*) – значение, обычно вычисляемое на основе пропускной способности, денежной стоимости или других единиц измерения, назначаемых администратором.
- ✓ Каждый протокол маршрутизации использует свои метрики.

Протоколы маршрутизации

□ В зависимости от типа используемого алгоритма, протоколы динамической маршрутизации делятся на:

- **Дистанционно-векторные протоколы**, основанные на алгоритме Distance Vector Algorithm (DVA), который также называют алгоритмом Белмана-Форда (*Bellman-Ford*) – маршрутизация по вектору расстояния, в соответствии с которой определяется направление (вектор) и расстояние до сети;
- **Протоколы с учетом состояния каналов связи**, основанные на алгоритме Link State Algorithm (LSA) – выполняют оценку состояния каналов связи, воссоздают точную топологию сети.
- **Гибридные протоколы маршрутизации** – объединяют характеристики дистанционно-векторных алгоритмов и алгоритмов состояния каналов связи.

Понятие сходимости

- Маршрутизация может быть нарушена при изменении топологии сети.
- Для того чтобы маршрутизация не прерывалась, маршрутизаторы должны владеть непротиворечивыми знаниями о топологии сети.
- Под *сходимостью* сети подразумевают то, что все маршрутизаторы работают с одной и той же информацией.
- Время сходимости - это время, требуемое всем маршрутизаторам в сети для того, чтобы согласовать текущую топологию. Оно зависит от размера сети, используемого протокола динамической маршрутизации, его временных настроек и методов объявления об аварийных ситуациях.

Дистанционно-векторные алгоритмы маршрутизации

- Дистанционно-векторный алгоритм маршрутизации основан на выборе расстояния между сетями.
- Метрика расстояния – число переходов (*Hop count*).
- Маршрутизаторы периодически отправляют свои таблицы маршрутизации (полностью или частично) соседям (непосредственно подключенным маршрутизаторам) и определяют маршрут на основе следующих характеристик:
 - *метрики расстояния* – число переходов до сети назначения;
 - *вектора* – направления, ведущего к сети назначения.
- При получении информации от соседа, маршрутизатор обновляет свою таблицу маршрутизации, увеличивая метрику расстояния. Далее эта таблица передается соседям и таким образом информация о расстоянии распространяется по составной сети.
- Дистанционно-векторные протоколы рассылают периодические обновления, даже в том случае, если изменения в топологии сети не произошли.
- Примеры дистанционно-векторных протоколов:
 - Routing Information Protocol (RIP)
 - Cisco System Interior Gateway Routing Protocol (IGRP)
 - Open Shortest Path First (OSPF)
 - Interdomain System-to-Interdomain System (IS-IS)

Дистанционно-векторные алгоритмы маршрутизации

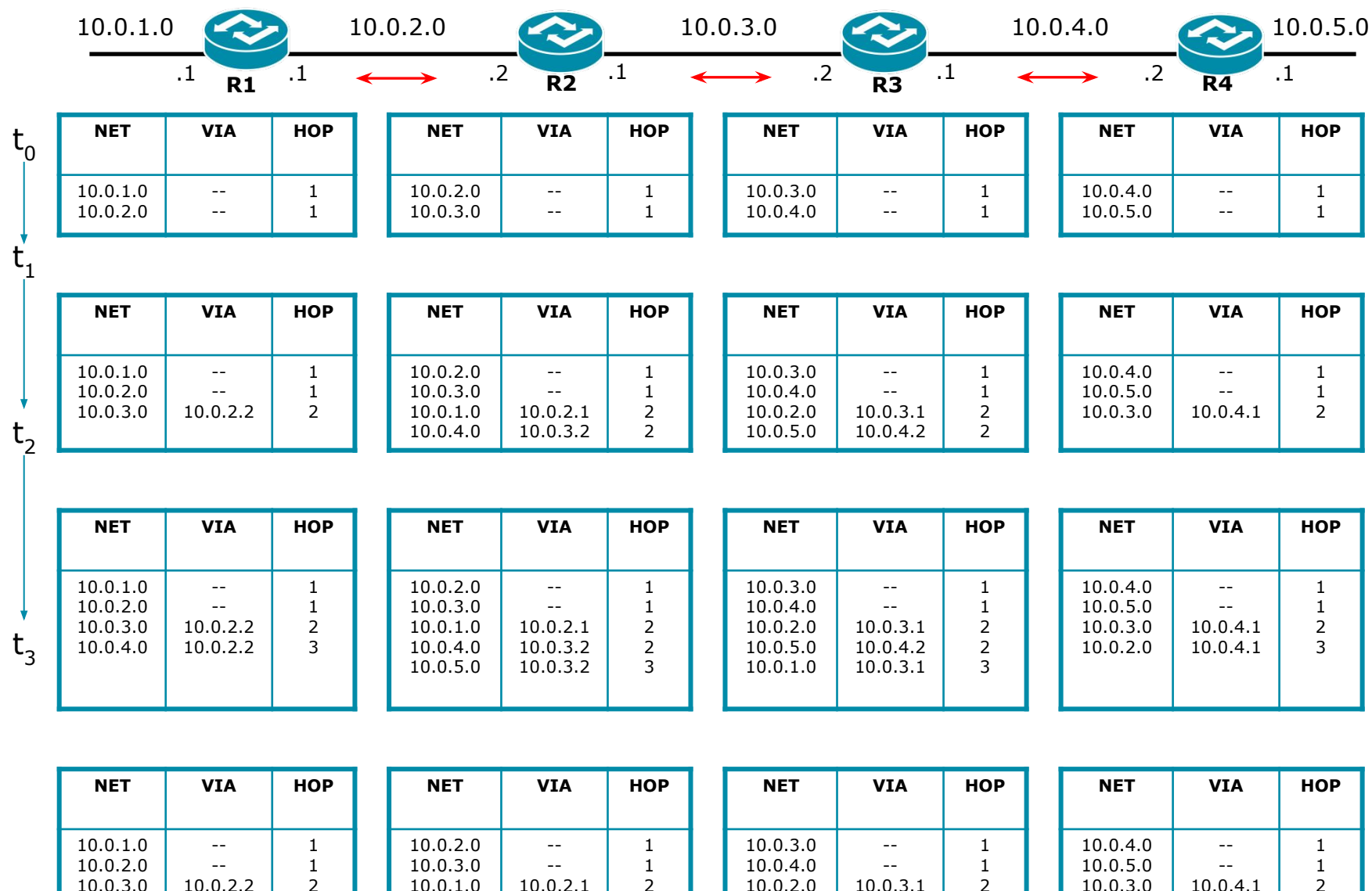
Недостатки:

- ✓ Дистанционно-векторные алгоритмы маршрутизации не позволяют маршрутизаторам знать точную топологию сети и поэтому имеют ограниченную возможность в выборе наилучшего маршрута.
- ✓ Существуют проблемы, связанные с их функционированием, которые можно решить только специальными методами.

Достоинства:

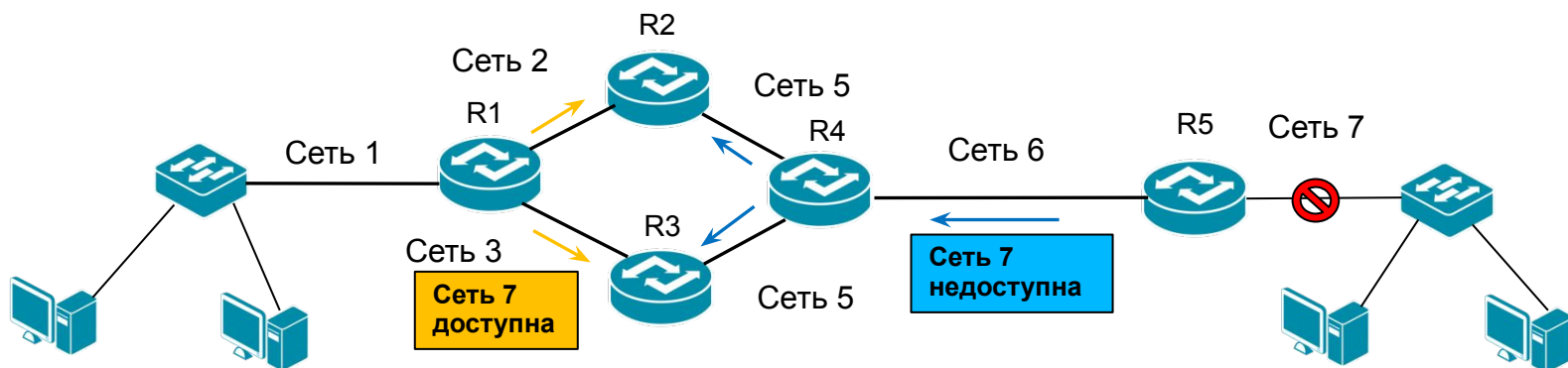
- ✓ Простота в использовании и настройке.

Принцип работы дистанционно-векторного алгоритма маршрутизации



Проблемы при работе дистанционно-векторного алгоритма маршрутизации: Стремление к бесконечности

- В результате медленной сходимости у маршрутизаторов появляется противоречивая информация о маршрутах, в результате чего появляются петли маршрутизации.
- Петли маршрутизации приводят к проблеме, которая называется «стремление к бесконечности».



Для решения этой проблемы используются следующие методы:

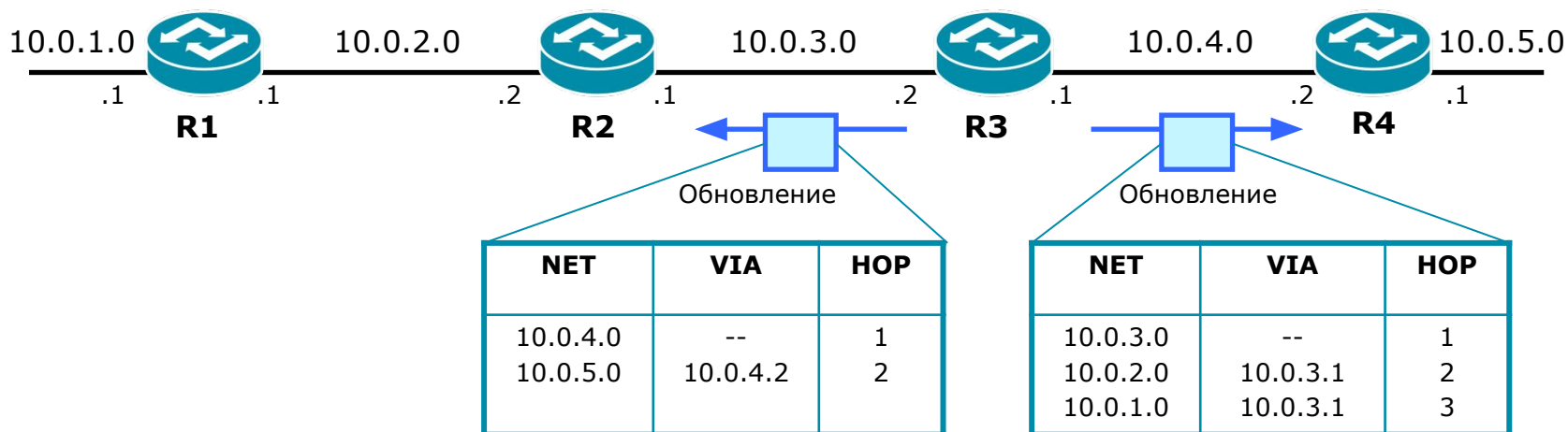
1. Ограничение максимального расстояния (числа переходов).
2. Метод расщепления горизонта (*Split horizon*).
3. Испорченный обратный маршрут (*Poisoned reverse*).
4. Триггерные обновления (*Triggered Update*).
5. Установка таймеров удержания (*Hold-down timer*).

Ограничение максимального расстояния (числа переходов)

- Для того чтобы ограничить «бесконечность» дистанционно-векторные алгоритмы определяют максимальное расстояние между двумя сетями.
- Этот подход не предотвращает петли маршрутизации, а только ограничивает количество переходов.
- При достижении метрикой максимального значения, сеть считается недоступной.

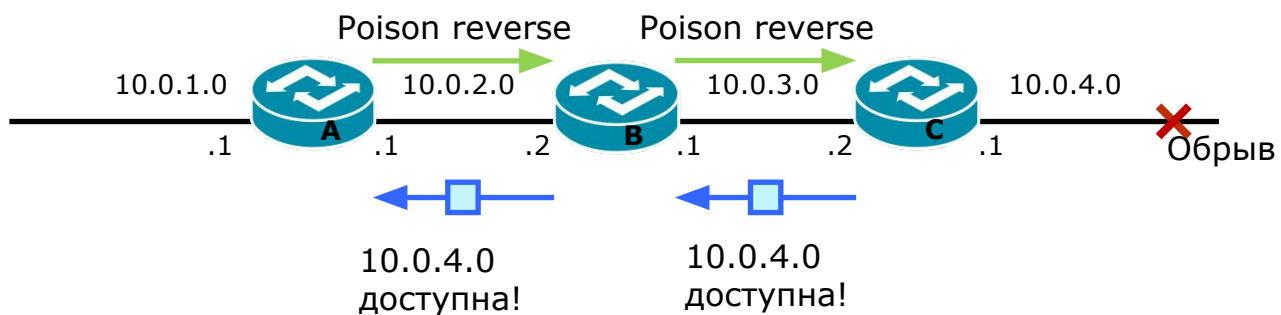
Решение: Расщепление горизонта (Split horizon)

Информация о маршруте никогда не передается в направлении того маршрутизатора, от которого она была получена.



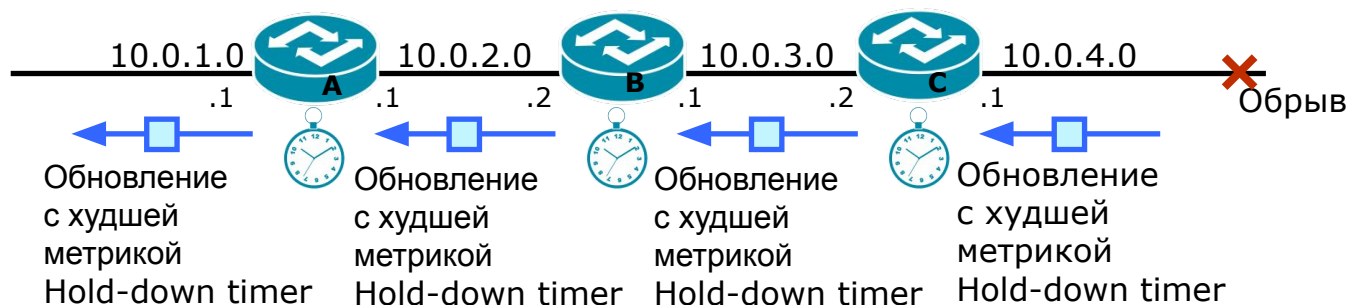
Решение: Испорченный обратный маршрут (Poison reverse)

- Это решение является усовершенствованием метода расщепления горизонта.
- Вместо того, чтобы не включать в периодическое обновление информацию о маршруте при ее передаче в направлении источника, маршрут «портится», т.е. метрике маршрута присваивается максимальное значение.



Решение: Таймер удержания (Hold-down timer)

- Механизм *Hold-down timer* позволяет маршрутизатору запускать таймер при получении от соседа информации о недоступности сети и игнорировать в течение времени, установленного таймером, все полученные от соседних маршрутизаторов обновления о доступности маршрута с худшей метрикой.
- Позволяет всем маршрутизаторам сети получить информацию о сетевом отказе.



Триггерные обновления (Triggered Update)

- В случае обнаружения сбоя в канале связи маршрутизатор:
 - Мгновенно отправляет обновление соседним маршрутизаторам с недостижимым значением метрики для аварийного маршрута.
 - Удаляет запись для аварийного маршрута из своей таблицы маршрутизации, а также все записи для маршрутов, проходящих через него.
 - Соседние маршрутизаторы обновляют свои таблицы маршрутизации и генерируют аварийные обновления.
 - Таким образом обновления распространяются по сети и сокращают время сходимости.
- Триггерные обновления не позволяют избежать петель маршрутизации без использования дополнительных методов.

Протокол Routing Information Protocol (RIP)

- Протокол RIP является внутренним протоколом маршрутизации.
- Наиболее распространен в небольших однородных сетях.
- RIP основан на дистанционно-векторном алгоритме маршрутизации.

Существует 3 версии протокола RIP:

- ✓ RIP version 1 (RIPv1) для протокола IPv4;
- ✓ RIP version 2 (RIPv2) для поддержки бесклассовой адресации протокола IPv4;
- ✓ RIPng (*next generation*) для протокола IPv6.

Протокол RIPv1

- RIPv1 определен в RFC 1058.
- RIP используем метрику «число переходов» (Hop count), максимальное значение которой равно 15. Значение 16 означает недостижимость сети.
- При передаче сообщений RIP используется протокол UDP (порт 520).

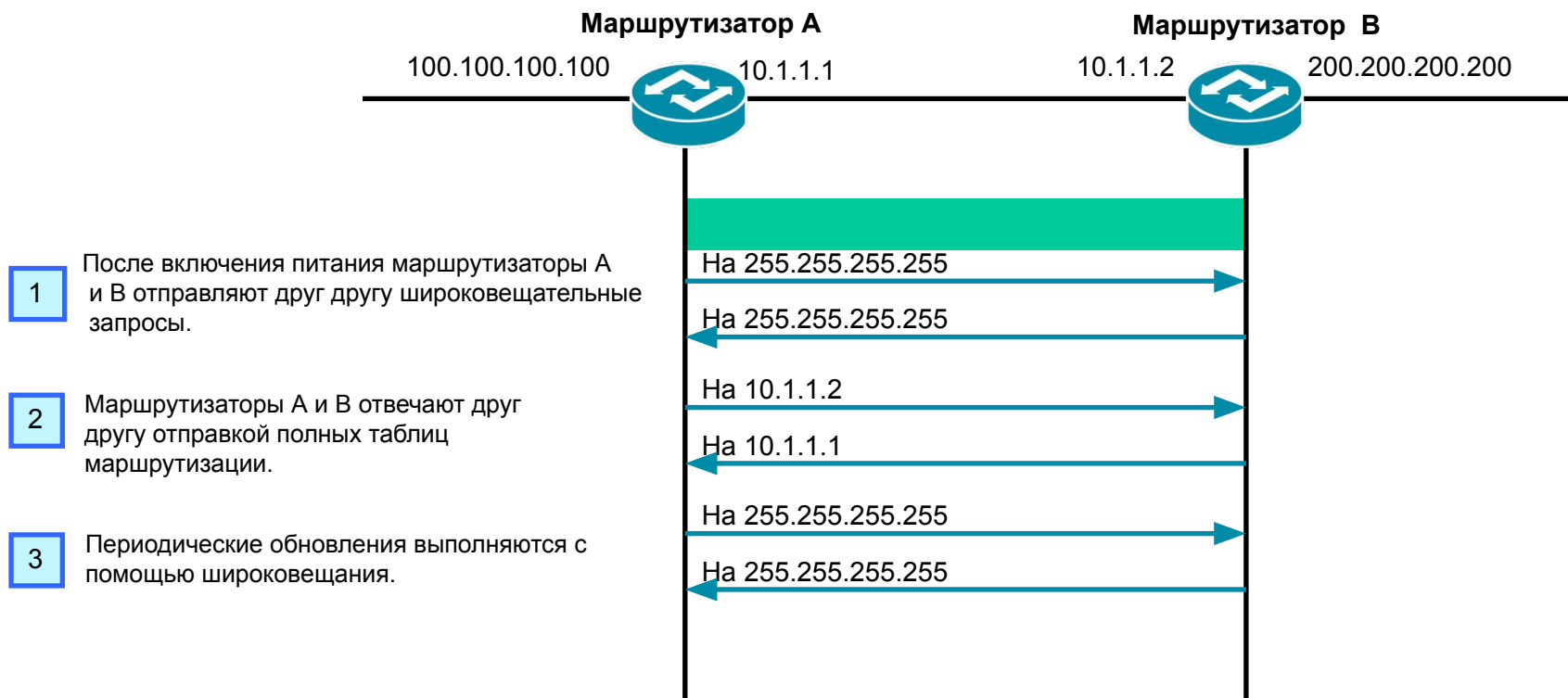
Заголовок канального уровня	Заголовок IP	Заголовок UDP	Заголовок RIP	Данные
-----------------------------	--------------	---------------	---------------	--------

- Обновления передаются с использованием широковещания каждые 30 секунд.
- 0.0.0.0 – используется в качестве маршрута по умолчанию.
- RIPv1 – протокол основанный на классах сетей. Обновления не содержат информации о маске подсети.

Сообщения RIPv1

□ В RIPv1 определены два типа сообщений:

- Request (запрос) – сообщение отправляемое маршрутизатору с просьбой прислать часть или всю таблицу маршрутизации;
- Response (ответ) – сообщение содержащее часть или всю таблицу маршрутизации.



Предотвращение устаревания информации

- Информация о маршруте хранится в таблице маршрутизации определенное время.
- Каждой записи в таблице маршрутизации присваивается время старения, устанавливаемое таймером (*Timeout timer*).
- Таймер старения сбрасывается каждый раз, когда маршрутизатор получает обновление с информацией о соответствующем маршруте.
- Если информация о каком-либо маршруте отсутствует в периодических обновлениях, время, установленное таймером истекает и маршрут помечается как недостижимый (значение метрики устанавливается равным 16).
- По умолчанию значение таймера *Timeout* равно 180 сек.

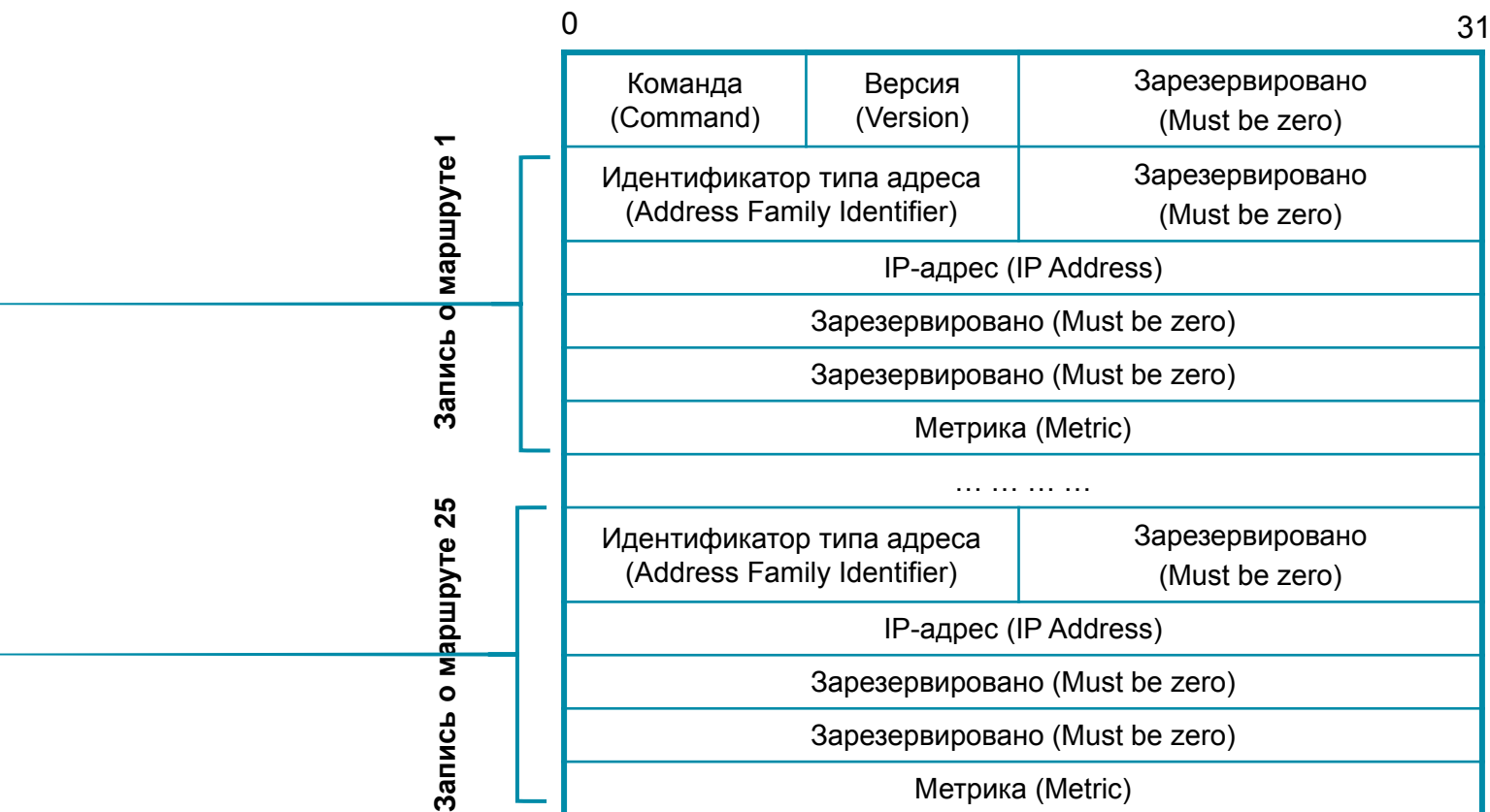
Удаление устаревшей информации

- Когда маршрут помечается как недостижимый, запускается таймер *Garbage-Collection* (сборщик мусора).
- После истечения таймера *Garbage-Collection* недостижимый маршрут полностью удаляется из таблицы маршрутизации.
- По умолчанию значение таймера *Garbage-Collection* равно 120 сек.

```
DGS-3620-28TC:admin#show rip
Command: show rip

RIP Global State      : Enabled
Update Time           : 30 seconds
Timeout Time          : 180 seconds
Garbage Collection Time : 120 seconds
```

Формат пакета протокола RIPv1



1 пакет RIP может содержать максимально 25 записей о маршрутах.

Команда:

- 1: запрос на получение частичной или полной маршрутной информации;
- 2: ответ, содержащий полную или частичную информацию из таблицы маршрутизации отправителя.

Версия: равна 1 для RIPv1

Идентификатор типа адреса:

определяет тип протокола (IP, IPX), используемого в соответствующей сети, для протокола IP значение - 2

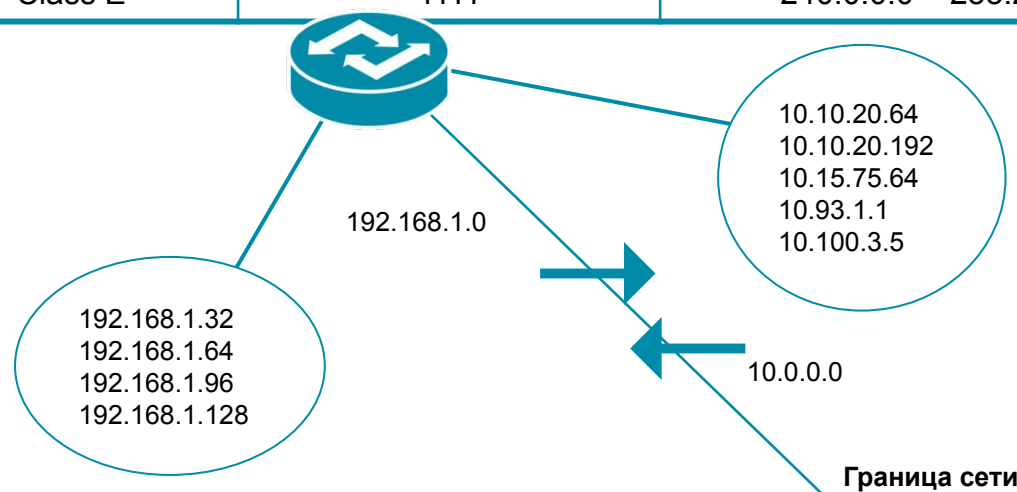
IP-адрес: IP-адрес сети x.

Метрика: расстояние до сети (число переходов), указанной в поле IP-адрес.

Маршрутизация на основе классов

- RIPv1 не передает в таблице маршрутизации информацию о маске подсети.
- На границе сети автоматически создается суммарный маршрут

Класс адреса	Наиболее значащие биты	Диапазон значений
Class A	0000	0.0.0.0 – 126.255.255.255
Class B	1000	128.0.0.0 – 191.255.255.255
Class C	1100	192.0.0.0 – 223.255.255.255
Class D	1110	224.0.0.0 – 239.255.255.255
Class E	1111	240.0.0.0 – 255.255.255.255

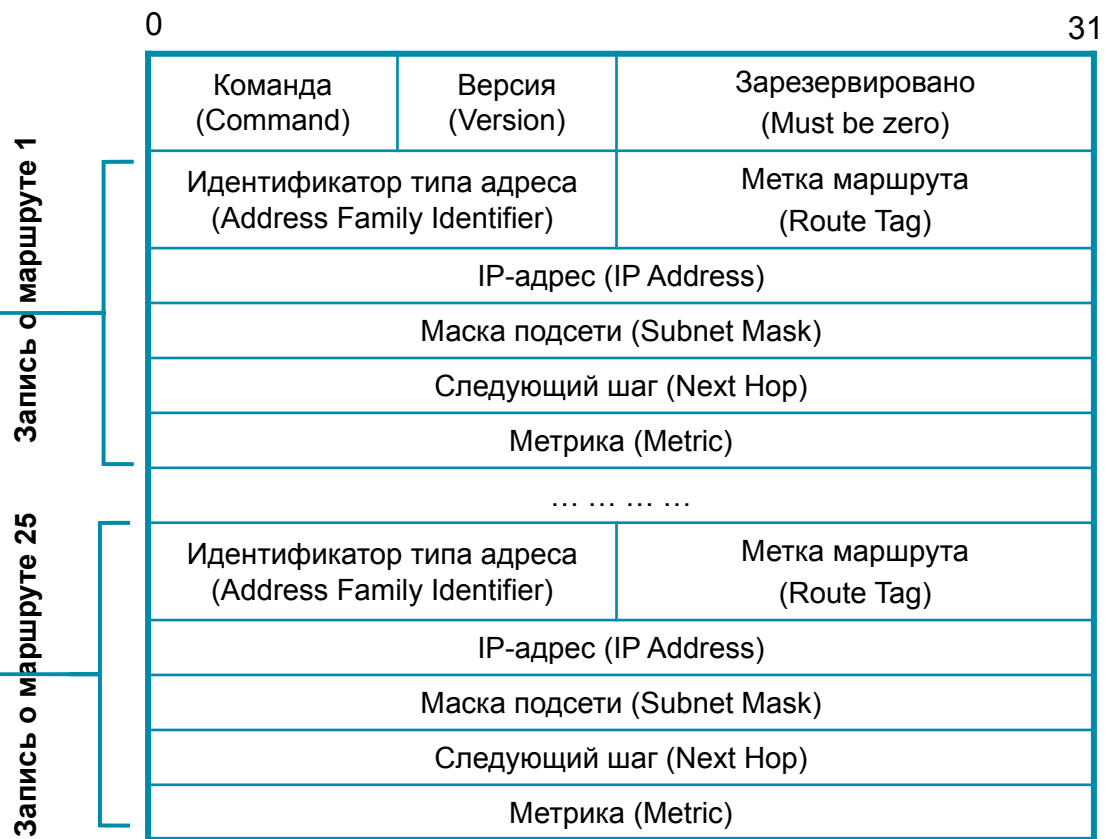


Суммирование маршрутов на граничных маршрутизаторах

Протокол RIPv2

- RIPv2 является расширением базовой версии протокола RIP. Он определен в RFC 2453.
- RIPv2 использует неиспользованные поля формата сообщения RIPv1.
- Основные отличия RIPv2 от RIPv1:
 - **Поддержка бесклассовой адресации:** RIPv2 передает информацию о маске подсети для каждого сетевого адреса. Он поддерживает маски переменной длины (VLSM) и бесклассовую маршрутизацию (CIDR).
 - **Указание адреса следующего маршрутизатора (*Next Hop*):** каждая запись включает точный IP-адрес маршрутизатора, который может быть использован в качестве следующего транзитного маршрутизатора, предназначенного для передачи пакета в целевую сеть. Используется для повышения эффективности маршрутизации.
 - **Аутентификация:** RIPv2 предоставляет базовый механизм аутентификации, который позволяет маршрутизаторам идентифицировать другие маршрутизаторы прежде чем принимать RIP-сообщения от них.
 - **Метки маршрута (*Route Tag*):** каждая запись RIPv2 содержит поле Route Tag (метка маршрута), в котором хранится дополнительная информация о маршруте. Эта информация распространяется в обновлениях. Это поле используется, когда информация о маршрутах изучается из разных автономных систем для идентификации автономной системы, из которой получен маршрут.
- **Использование многоадресной рассылки:** для уменьшения загрузки сети, RIPv2 позволяет рассылать обновления не широковещательно, а на специальный групповой адрес 224.0.0.9.

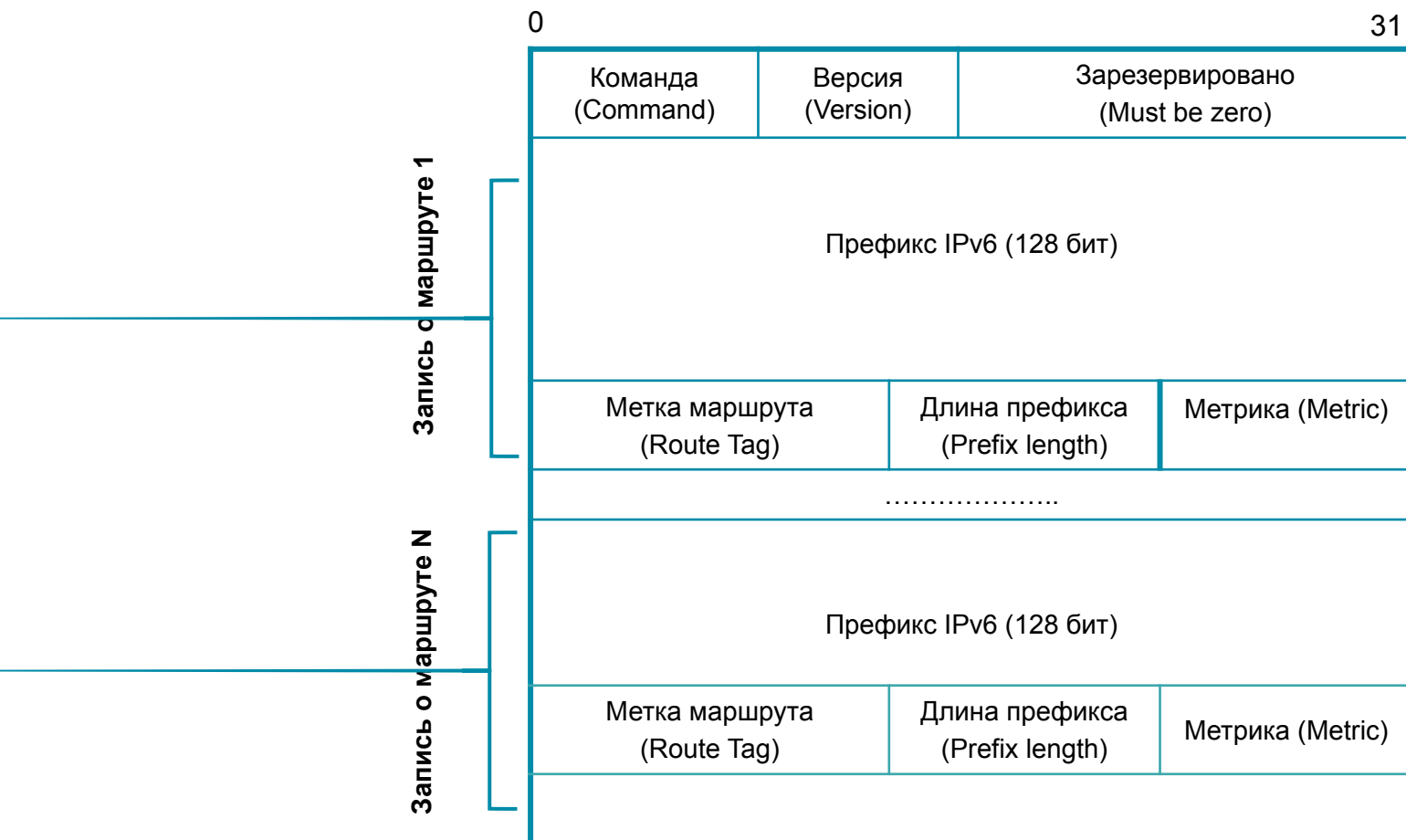
Формат пакета протокола RIPv2



Протокол RIPng

- RIPng является версией протокола RIP, совместимой с IPv6. Он определен в RFC 2080.
- Базовые операции RIPng аналогичны протоколу RIP для IPv4.
 - При передаче сообщений RIPng используется порт 521 протокола UDP.
- RIPng использует аналогичные RIPv2 улучшения базовой версии RIP:
- **Поддержка бесклассовой адресации:** все адреса IPv6 бесклассовые. Вместо поля «маска подсети» используется поле «префикс».
- **Указание адреса следующего маршрутизатора:** из-за большого размера адреса IPv6, это поле является дополнительным. Если необходимо указать адрес транзитного маршрутизатора, он указывается в отдельной записи.
- **Аутентификация:** RIPng не имеет собственного механизма аутентификации, а полагается на стандартную функцию IPSec, определенную для IPv6.
- **Метки маршрута (Route Tag):** аналогично RIPv2.
- **Использование многоадресной рассылки:** сообщения отправляются специальным групповым адресом IPv6 FF02::9.

Формат пакета протокола RIPng



Максимальное количество записей не ограничено 25 как в RIPv1/v2. Оно ограничено только MTU сети, через которую будет передаваться сообщение.

Выводы:

- ICMP является неотъемлемой частью IP и обязателен при реализации стека TCP/IP. Он обеспечивает поддержку IP в форме ICMP-сообщений.
- Существует две версии протокола ICMP: ICMPv4 и ICMPv6.
- Обе версии протокола ICMPv4 и ICMPv6 определяют общую систему передачи сообщений, обеспечивая выполнение разнообразных функций.
- Сообщения ICMP делятся на два класса – сообщения об ошибках и информационные сообщения.
- Протокол Neighbor Discovery Protocol (NDP) – протокол стека TCP/IP, используемый совместно с IPv6 и обеспечивающий функции разрешения адресов, автоконфигурации адресов, обнаружения дублирования адресов в сетях IPv6.
- Маршрутизация - процесс определения маршрута следования информации от отправителя к получателю в составной сети.
- Маршрутизация выполняется специальными устройствами – маршрутизаторами.
- Маршрутизаторы принимают решение о том куда передавать пакет на основе его сетевого адреса назначения, который сравнивается с информацией, хранимой в специальных таблицах маршрутизации.
- Маршруты добавляются в таблицу маршрутизации с помощью статической или динамической маршрутизации.
- При динамической маршрутизации записи о маршрутах заносятся и обновляются в таблицах с помощью протоколов маршрутизации.
- Протоколы маршрутизации бывают двух типов – внутренние и внешние.
- Протоколы динамической маршрутизации отличаются используемыми алгоритмами маршрутизации и метриками.
- Метрика – это числовой показатель, позволяющий определить наилучший маршрут к сети назначения. Чем ниже метрика, тем предпочтительнее маршрут.
- В зависимости от типа используемого алгоритма, протоколы динамической маршрутизации делятся на дистанционно-векторные, протоколы с учетом состояния каналов связи и гибридные.

Выводы:

- Алгоритм дистанционно-векторной маршрутизации определяет направление (вектор) и расстояние (счетчик узлов) для каждого из каналов связи, образующих сеть.
- Маршрутизаторы, использующие дистанционно-векторные протоколы маршрутизации периодически рассылают обновления, содержащие полностью таблицу маршрутизации или ее часть.
- Дистанционно-векторные протоколы маршрутизации не позволяют маршрутизаторам знать точную топологию сети и поэтому имеют ограниченную возможность в выборе наилучшего маршрута.
- При использовании дистанционно-векторных протоколов маршрутизации существуют проблемы, связанные с их функционированием, которые можно решить только специальными методами.
- К дистанционно-векторным протоколам относится протокол RIP .
- Протокол RIP является внутренним протоколом маршрутизации. Он предназначен для использования в небольших однородных сетях.
- В настоящее время существует три версии протокола RIP: RIPv1, RIPv2 для сетей IPv4, RIPv6 для сетей IPv6.