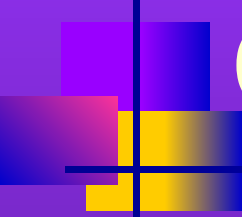


Информационные сети

Архитектура TCP/IP
Протоколы сетевого уровня.
ARP, RARP, ICMP.
Маршрутизация



Содержание

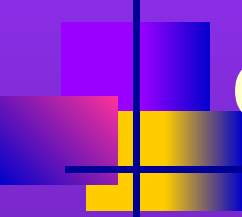
- Обзор архитектуры TCP/IP
 - История возникновения
 - Основные понятия
 - Уровни архитектуры

TCP/IP

История

- 1970-е гг. – группа американских исследователей предложило понятие "интерсеть" и попытались определить набор протоколов, позволяющих организовать взаимодействие приложений вне зависимости от типа физической среды, технологии передачи и операционной системы
- Работы проводились по заказу Defense Advanced Research Projects Agency (DARPA) и привели к созданию сети, объединяющей ряд учреждений Министерства Обороны США – ARPANET
 - В качестве основного протокола использовался NCP
- 1978 г. – разработан стек протоколов TCP/IP
- 1980 г. – начинается перевод ARPANET на TCP/IP
- 1983 г. – принят стандарт для протоколов TCP/IP (военный стандарт), с этого момента все узлы ARPANET должны поддерживать стек протоколов TCP/IP
 - в 1983 г. вышел BSD UNIX (Berkley Software Distribution), включающий в себя реализацию TCP/IP
- 1989 г. – ARPANET соединился с NSFNET, что и стало прообразом современного Интернета

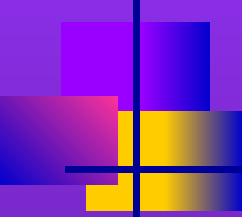
- Internet Society (ISOC)
 - Internet Architecture Board (IAB)
 - Internet Engineering Steering Group (IESG)
 - Internet Engineering Task Force (IETF)
 - Internet Research Steering Group (IRSG)
 - Internet Research Task Force (IRTF)
 - Internet Corporation for Assigned Names and Numbers (ICANN)
 - Internet Assigned Numbers Authority (IANA)



TCP/IP

Организационные структуры Интернет

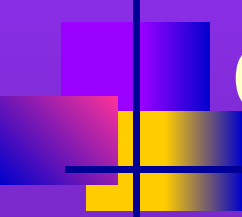
- Internet Society (ISOC) – профессиональное сообщество, которое занимается общими вопросами эволюции и роста Internet
- Internet Architecture Board (IAB) – техническая наблюдательная группа ISOC (координирует направление исследований и новых разработок для стека TCP/IP и является конечной инстанцией при определении новых стандартов Internet)
- Internet Engineering Task Force (IETF) – инженерная группа, которая занимается решением наиболее актуальных технических проблем Интернет и определяет спецификации, которые затем становятся стандартами Интернет
- Internet Engineering Steering Group (IESG) – управляющая структура IETF



TCP/IP

Организационные структуры Интернет

- Internet Research Task Force (IRTF) – координирует долгосрочные исследовательские проекты по протоколам TCP/IP
- Internet Research Steering Group (IRSG) – управляющая структура IRTF
- Internet Corporation for Assigned Names and Numbers (ICANN) – обеспечение универсальных возможностей связи в Интернете, надзор и координация адресного пространства IP и DNS
- Internet Assigned Numbers Authority (IANA) – надзор за выделением IP-адресов, управление системой DNS (все доменные имена выдаются от имени IANA или делегированных регистраторов)

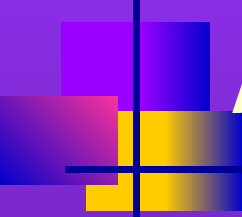


TCP/IP Стандарты

- Стандарты Интернет оформляются и публикуются в виде RFC (Request For Comments)
- В настоящее время первичную публикацию RFC выполняет IETF
 - <http://www.ietf.org/rfc.html>
- Рассматриваемые протоколы имеют состояние и статус
 - Состояния: Стандартный, Предварительный, Предлагаемый, Экспериментальный, Ознакомительный, Устаревший
 - Статус: Обязательный, Рекомендуемый, Выбираемый, Ограниченного использования, Нерекондуемый

TCP/IP

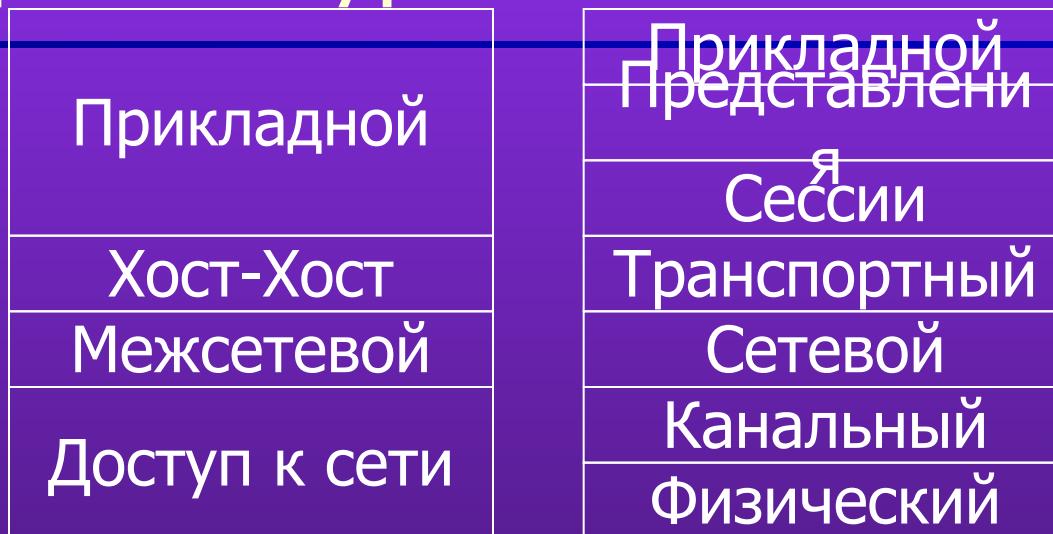
Архитектура



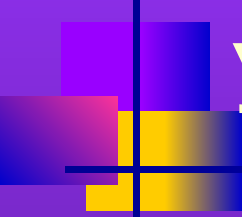
Прикладной
Хост-Хост
Межсетевой
Доступ к сети

- TCP/IP использует 4-уровневую архитектуру и содержит следующие уровни
 - Прикладной
 - Хост-Хост
 - Межсетевой
 - Доступ к сети

TCP/IP Архитектура



- На рисунке представлено сравнительное местоположение уровней TCP/IP и уровней ISO/OSI
- Учтите, мы сравниваем местоположение уровней, а не выполняемые ими функции!



TCP/IP

Уровень доступа к сети

Доступ к сети

Канальный
Физический

- Обе модели (TCP/IP и ISO/OSI) могут использовать различные протоколы для передачи между узлами в сети
- Модель TCP/IP изначально разрабатывалась для работы в сетях с различными технологиями, поэтому она определяет требования к технологии передачи
- Как правило, не требуется много усилий для того, чтобы реализовать поддержку TCP/IP в новой технологии
- Если технология поддерживает определение типа вышележащего протокола, TCP/IP может использовать ее совместно с другими протоколами

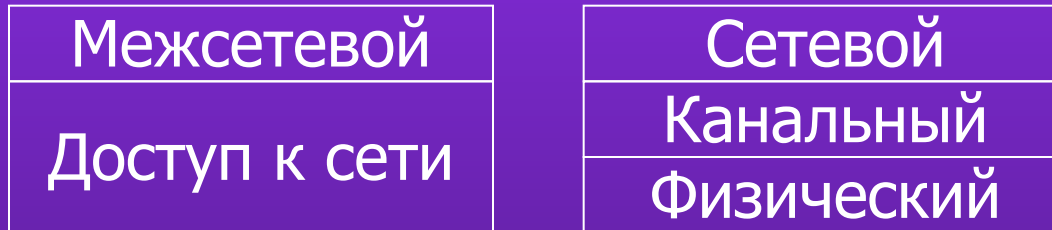
TCP/IP

Уровень доступа к сети

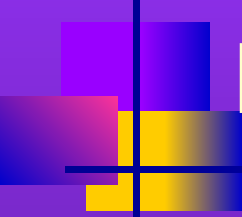
Прикладной						
Хост-Хост						
Межсетевой						
Ethernet	Token Ring	FDDI	Frame Relay	SLIP	PPP	ATM

TCP/IP

Межсетевой уровень



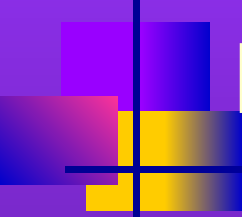
- Основная функция межсетевого уровня – доставка пакета от узла-отправителя до узла-получателя через несколько физических сетей (маршрутизация)
- Основным протоколом межсетевого уровня в архитектуре TCP/IP является Internet Protocol (IP)



TCP/IP

Межсетевой уровень

- IP – это ненадежный, максимально обеспеченный, датаграммный пакетный протокол
- IP обеспечивает 3 важнейшие функции
 - Определяет основную единицу передачи данных в интерсети. Любые другие данные межсетевого и вышележащих уровней инкапсулируются в IP-пакеты
 - Выполняет функцию маршрутизации
 - Включает правила ненадежной доставки, которые определяют, как хосты и маршрутизаторы должны обрабатывать пакеты, и при каких условиях можно уничтожать пакет
- IP использует IP-адреса, состоящие из двух частей: адреса сети и адреса узла в сети
- Адрес сети уникален и назначается IANA



TCP/IP

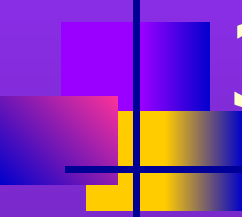
Межсетевой уровень

- IP не ожидает от нижележащих протоколов ничего кроме возможности доставки пакетов к адресуемому узлу
- IP
 - не добавляет надежности
 - IP-пакеты (датаграммы) могут потеряться, продублироваться, поменять порядок следования
 - не исправляет ошибки
 - не выполняет контроль трафика

TCP/IP

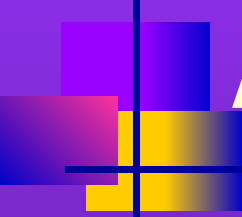
Межсетевой уровень





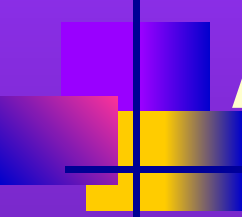
Заключение

- TCP/IP – самый распространенный в настоящий момент стек протоколов
- Он имеет многоуровневую архитектуру и содержит 4 уровня
- В дальнейшем мы будем изучать принципы работы высокоуровневых протоколов на примере протоколов и стека TCP/IP



ARP

- Протоколы определяют, происходит ли передача данных через сетевой уровень к верхним уровням эталонной модели OSI.
- Для осуществления передачи необходимо, чтобы пакет содержал MAC и IP-адреса отправителя и получателя.
- Для решения вопросов определения MAC-адреса искомого устройства по известному IP-адресу применяется протокол преобразования адресов (address resolution protocol, ARP – **RFC 826**).



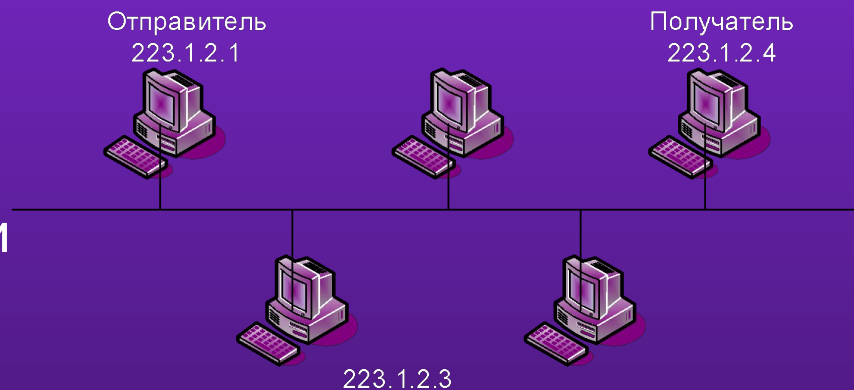
ARP-таблицы

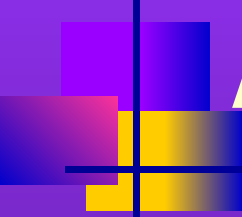
- *ARP* используется для определения соответствия IP-адреса адресу Ethernet.
- Протокол используется в локальных сетях. Отображение осуществляется только в момент отправления IP-пакетов, так как только в этот момент создаются заголовки IP и Ethernet.
- Отображение адресов осуществляется путем поиска в ARP-таблице. Упрощенно, ARP-таблица состоит из двух столбцов (см. рисунок).
- Таблица соответствия необходима, так как адреса выбираются произвольно и нет какого-либо алгоритма для их вычисления. Если машина перемещается в другой сегмент сети, то ее ARP-таблица должна быть изменена.

IP-адрес	Ethernet-адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

ARP-таблицы

- Когда отправитель определил IP-адрес получателя, то на основании ARP-таблицы определяется его MAC-адрес.
- Между MAC- и IP-адресами устанавливается соответствие, которое используется при инкапсуляции данных.
- Таблицу ARP можно посмотреть, используя команду `arp`, с ключом `-a`.

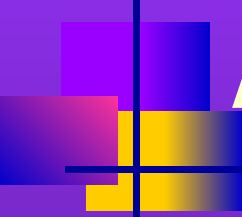




ARP-запросы

- ARP-таблица заполняется автоматически. Если нужного адреса в таблице нет, то в сеть посылается широковещательный запрос типа "чей это IP-адрес?".
- Все сетевые интерфейсы получают этот запрос, но отвечает только владелец адреса. При этом существует два способа отправки IP-пакета, для которого ищется адрес: пакет ставится в очередь на отправку или уничтожается.
 - В первом случае за отправку отвечает модуль ARP,
 - во втором случае модуль IP, который повторяет посылку через некоторое время.
- Широковещательный запрос выглядит следующим образом (см. рисунок).
- MAC-адрес широковещания имеет вид FF-FF-FF-FF-FF-FF.

IP-адрес отправителя	223.1.2.1
Ethernet-адрес отправителя	08:00:39:00:2F:C3
Искомый IP-адрес	222.1.2.2
Искомый Ethernet-адрес	<пусто>



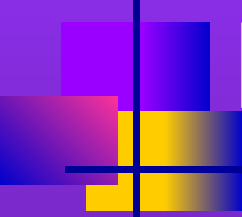
ARP-ответы

- Поскольку пакет ARP-запроса посылается в режиме широковещания, то его принимают все устройства в локальной сети и передают для анализа на сетевой уровень.
- Если IP-адрес устройства соответствует IP-адресу получателя, устройство формирует сообщение, называемое ARP-ответом.
- Структура ARP-ответа представлена на рисунке.
- Полученный таким образом адрес будет добавлен в ARP-таблицу.

IP-адрес отправителя	222.1.2.2
Ethernet-адрес отправителя	08:00:28:00:38:A9
IP-адрес получателя	223.1.2.1
Ethernet-адрес получателя	08:00:39:00:2F:C3

ARP-таблицы маршрутизаторов

- Если машина соединена с несколькими сетями, т.е. она является шлюзом, то в таблицу ARP вносятся строки, которые описывают как одну, так и другую IP-сети.
- При использовании Ethernet и IP каждая машина имеет как минимум один адрес Ethernet и один IP-адрес.
- Собственно Ethernet-адрес имеет не компьютер, а его сетевой интерфейс. Таким образом, если компьютер имеет несколько интерфейсов, то это автоматически означает, что каждому интерфейсу будет назначен свой Ethernet-адрес. IP-адрес назначается для каждого драйвера сетевого интерфейса.
- Каждой сетевой карте Ethernet соответствуют один MAC-адрес и один IP-адрес. IP-адрес уникален в рамках всего Internet.



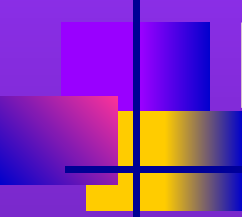
RARP

- Чтобы получатель, принимающий данные, знал кто их отправил, пакет данных должен содержать MAC и IP-адреса источника.
- Протокол обратного преобразования адресов (Reverse Address Resolution Protocol, RARP) используется для определения собственного IP-адреса по известному MAC-адресу устройства.
- Для решения данной задачи в сети должен присутствовать RARP-сервер, отвечающий на RARP-запросы.
- Структура RARP-запроса подобна структуре ARP-запроса и включает MAC и IP-заголовки и сообщение запроса.
- RARP-запрос отправляется в режиме широковещания и доступен всем сетевым устройствам, подключенным в сеть. Однако только специальный RARP-сервер отвечает на данный запрос.
- RARP-ответ имеет такую же структуру, что и ARP-ответ. Он включает в себя сообщение RARP-ответа, MAC- и IP-заголовки.

Маршрутизаторы и ARP-таблицы

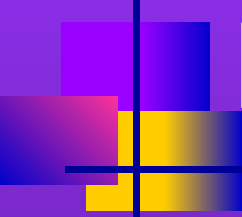


- Интерфейс, с помощью которого маршрутизатор подключается к сети, является частью данной сети. Для отправки и получения пакетов данных маршрутизаторы строят собственные ARP-таблицы, в которых отображаются IP-адреса на MAC-адреса.
- Маршрутизатор может быть подключен к нескольким подсетям и строит ARP-таблицы, описывающие все сети, подключенные к нему. Кроме карт соответствия IP-адресов MAC-адресам в таблицах маршрутизаторов отображаются порты.
- Для осуществления маршрутизации в сетях IP, маршрутизаторы содержат MAC- и IP-адреса других маршрутизаторов, которые используются для перенаправления пакетов.



Шлюз по умолчанию

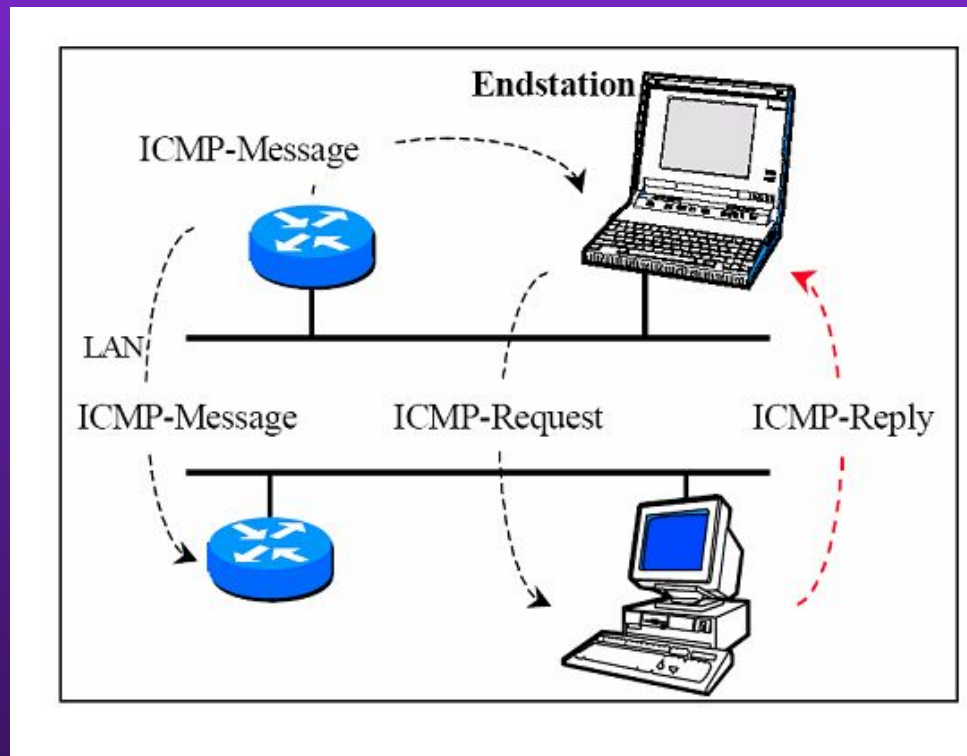
- Если источник источник расположен в сети с номером, отличным от номера сети назначения, и источник не знает MAC-адреса получателя, то для доставки пакета, источник пользуется услугами маршрутизатора.
- Если маршрутизатор используется подобным образом, то его называют *шлюзом по умолчанию (default gateway)*.
- При передаче пакета через шлюз, источник инкапсулирует данные, помещая в них в качестве MAC-адреса назначения физический адрес шлюза, в качестве IP-адреса устанавливается адрес получателя, а не шлюза.
- Шлюз получив пакет, отбрасывает информацию канального уровня и анализирует IP-заголовок. Поскольку IP-адрес отличается от его собственного, то маршрутизатор анализирует таблицу маршрутизации и пересылает пакет на соответствующий хост, инкапсулируя в пакет канального уровня и добавляя заголовок с новым MAC-адресом.



Протокол ICMP

- Данный протокол наряду с IP и ARP относят к сетевому уровню.
- Протокол используется для рассылки информационных и управляющих сообщений. При этом используются следующие виды сообщений:
 - **Flow control** - если принимающий хост (шлюз или реальный получатель информации) не успевает перерабатывать информацию, то данное сообщение приостанавливает отправку пакетов по сети.
 - **Detecting unreachable destination** - если пакет не может достичь места назначения, то шлюз, который не может доставить пакет, сообщает об этом отправителю пакета. Информировать о невозможности доставки сообщения может и машина, чей IP-адрес указан в пакете.
 - **Redirect routing** - это сообщение посылается в том случае, если шлюз не может доставить пакет, но у него есть на этот счет некоторые соображения, а именно адрес другого шлюза.
 - **Checking remote host** - в этом случае используется так называемое ICMP Echo Message. Если необходимо проверить наличие стека TCP/IP на удаленной машине, то на нее посылается сообщение этого типа. Как только система получит это сообщение, она немедленно подтвердит его получение.

Протокол ICMP



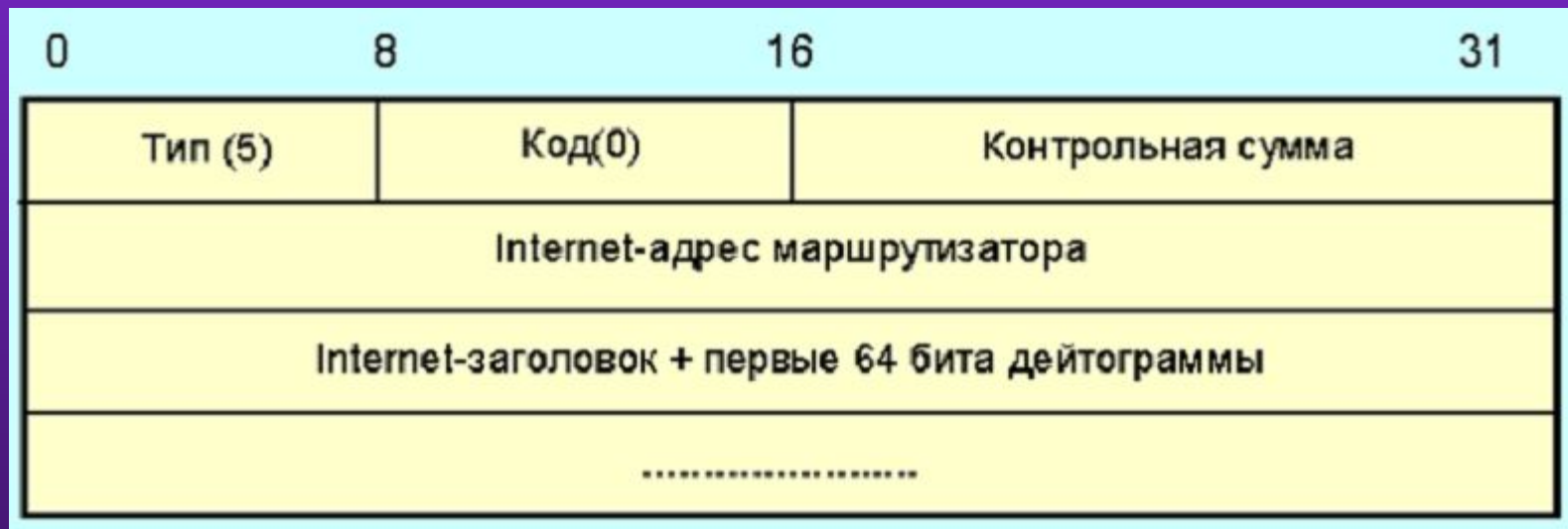
Протокол ICMP

- Код уточняет функцию ICMP- сообщения
- Поля идентификатор и номер по порядку служат для того, чтобы отправитель мог связать в пары запросы и отклики

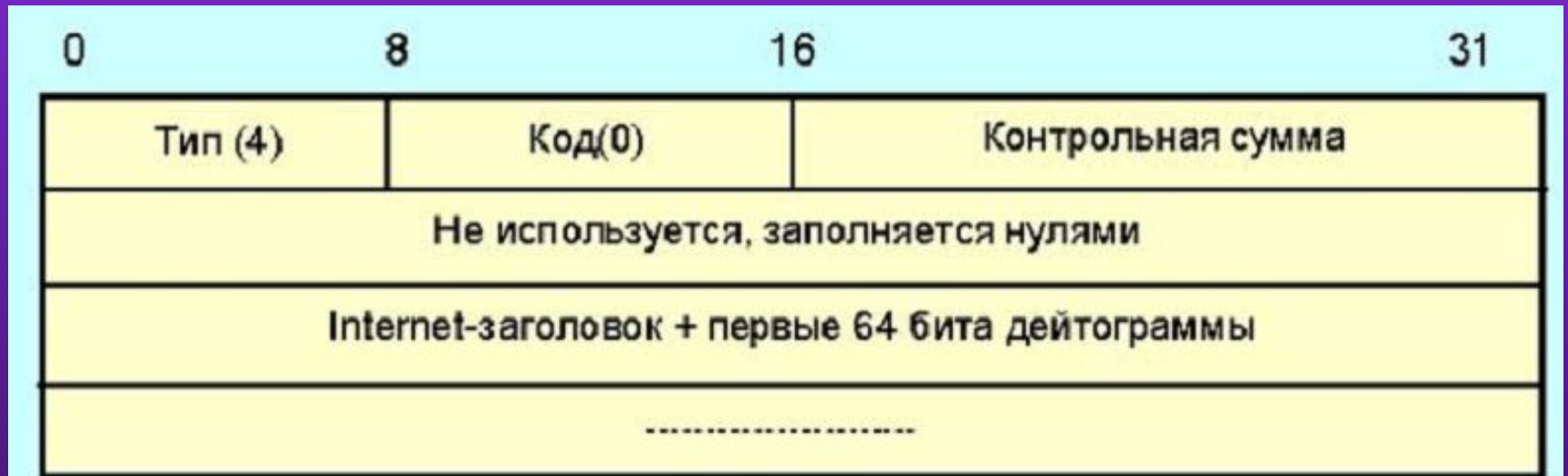


0		8	16	31
Тип (8 или 0)		Код(0)		Контрольная сумма
Идентификатор			Номер по порядку	
Данные				
.....				

Формат ICMP запроса переадресации



Формат ICMP запроса снижения нагрузки



Формат сообщения "время (ttl) истекло "

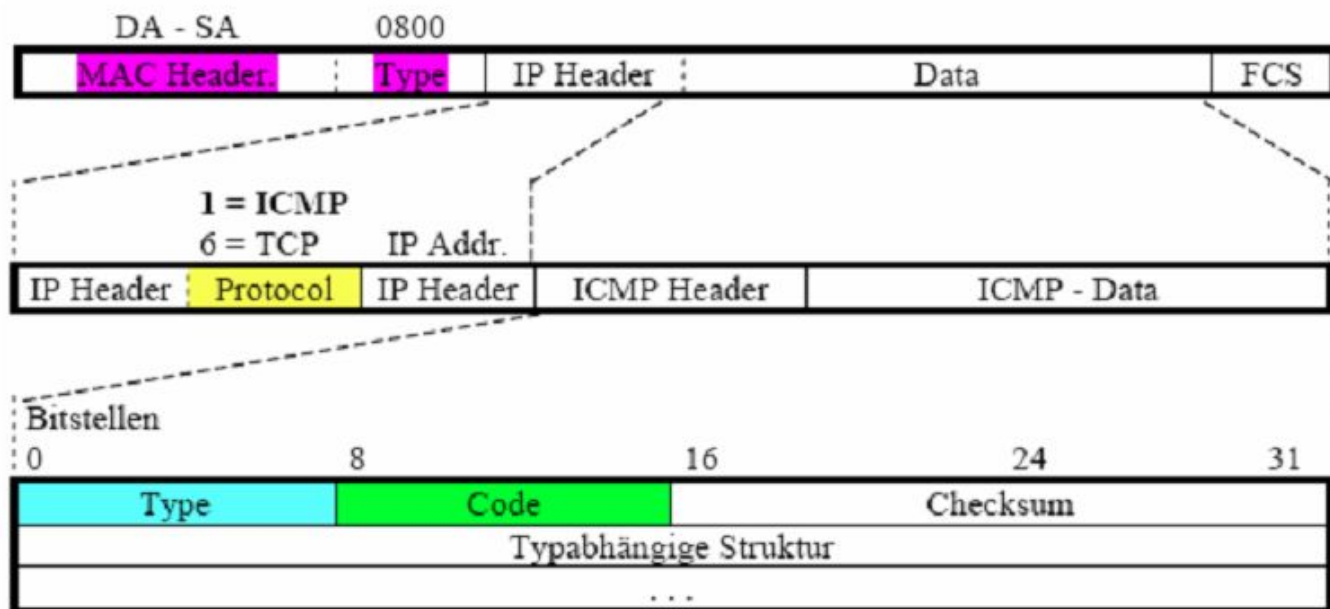
0	8	16	31
Тип (11)	Код(0 или 1)	Контрольная сумма	
Не используется, заполняется нулями			
Internet-заголовок + первые 64 бита дейтограммы			
.....			

Формат ICMP сообщений об имеющихся маршрутах

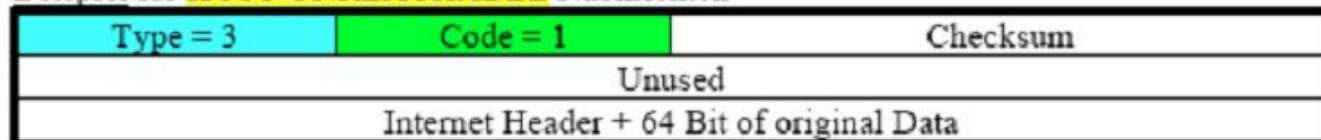
0 8 16 31

Тип (9)	Код(0)	Контрольная сумма
Число адресов	Длина адреса (2)	Время жизни
Адрес маршрутизатора [1]		
Уровень приоритета [1]		
Адрес маршрутизатора [2]		
Уровень приоритета [2]		
.....		

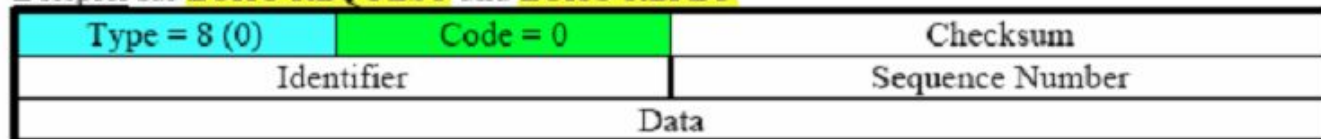
Протокол ICMP

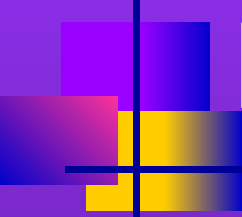


Beispiel für **HOST UNREACHABLE** Nachrichten



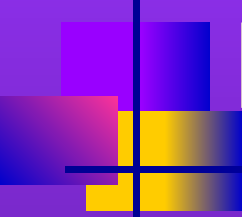
Beispiel für **ECHO REQUEST** und **ECHO REPLY**





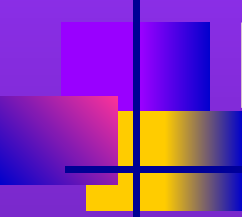
Команда ping

- С помощью отправки сообщений с эхо-запросом по протоколу ICMP проверяет соединение на уровне протокола IP с другим компьютером, поддерживающим TCP/IP. После каждой передачи выводится соответствующее сообщение с эхо-ответом.
- Ping - это основная TCP/IP-команда, используемая для устранения неполадки в соединении, проверки возможности доступа и разрешения имен. Команда **ping**, запущенная без параметров, выводит справку.
- **Синтаксис команды**
 - **ping** [-t] [-a] [-n *счетчик*] [-l *размер*] [-f] [-i *TTL*] [-v *тип*] [-r *счетчик*] [-s *счетчик*] [{-j *список_узлов* | -k *список_узлов*}] [-w *интервал*] [*имя_конечного_компьютера*]



Время жизни пакетов

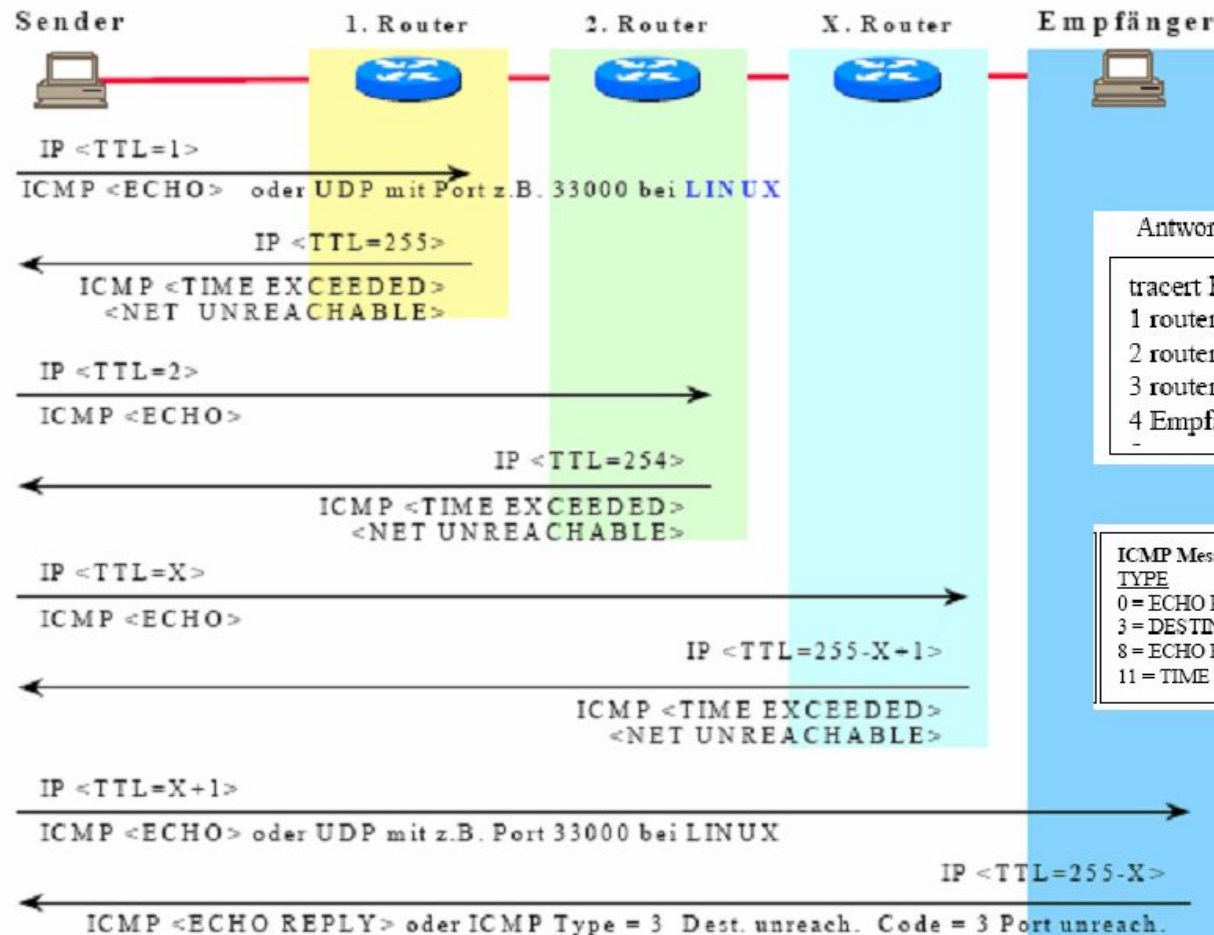
- Другое использование ICMP - это получение сообщения о "кончине" пакета на шлюзе. При этом используется время жизни пакета, которое определяет число шлюзов, через которые пакет может пройти.
- Программа, которая использует этот прием, называется traceroute (tracert в Windows). Она использует сообщение TIME EXCEEDED протокола ICMP.
- При посылке пакета через Internet traceroute устанавливает значение TTL (Time To Live) последовательно от 1 до 30 (значение по умолчанию).
- TTL определяет число шлюзов, через которые может пройти IP-пакет. Если это число превышено, то шлюз, на котором происходит обнуление TTL, высылает ICMP-пакет.
- Traceroute сначала устанавливает значение TTL равное единице - отвечает ближайший шлюз, затем значение TTL равно 2 - отвечает следующий шлюз и т. д.
- Если пакет достиг получателя, то в этом случае возвращается сообщение другого типа - **Detecting unreachable destination**, т.к. IP-пакет передается на транспортный уровень, а на нем нет обслуживания запросов.



Команда tracert

- Диагностическое средство, предназначенное для определения маршрута до точки назначения с помощью посылки в точку назначения эхо-запросов протокола ICMP с различными значениями срока жизни (TTL).
- Определяет путь до точки назначения с помощью посылки в точку назначения эхо-сообщений протокола ICMP с постоянным увеличением значений срока жизни (TTL).
- Выведенный путь — это список ближайших интерфейсов маршрутизаторов, находящихся на пути между узлом источника и точкой назначения.
- Ближний интерфейс представляют собой интерфейс маршрутизатора, который является ближайшим к узлу отправителя на пути. Запущенная без параметров, команда **tracert** выводит справку.
- **Синтаксис команды**
 - **tracert** [-d] [-h *максимальное_число_переходов*] [-j *список_узлов*] [-w *интервал*] [*имя_конечного_компьютера*]

Команда tracer



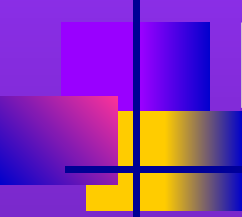
Antworten der Router im Netz:

tracert Empfänger

```
1 router1 (172.16.12.3) 10ms 8ms 4ms
2 router2 (188.88.1.4) 8ms 8ms 8ms
3 routerx (151.12.34.3) 8ms 8ms 8ms
4 Empfänger (122.45.67.5) 5ms 5ms
-
```

ICMP Message-TYPES und Codes

TYPE	CODE (bei TYPE=3)
0 = ECHO REPLY	0 = NET UNREACH.
3 = DESTINATION UNREACH.	1 = HOST "
8 = ECHO REQUEST	3 = Port "
11 = TIME EXCEEDED	

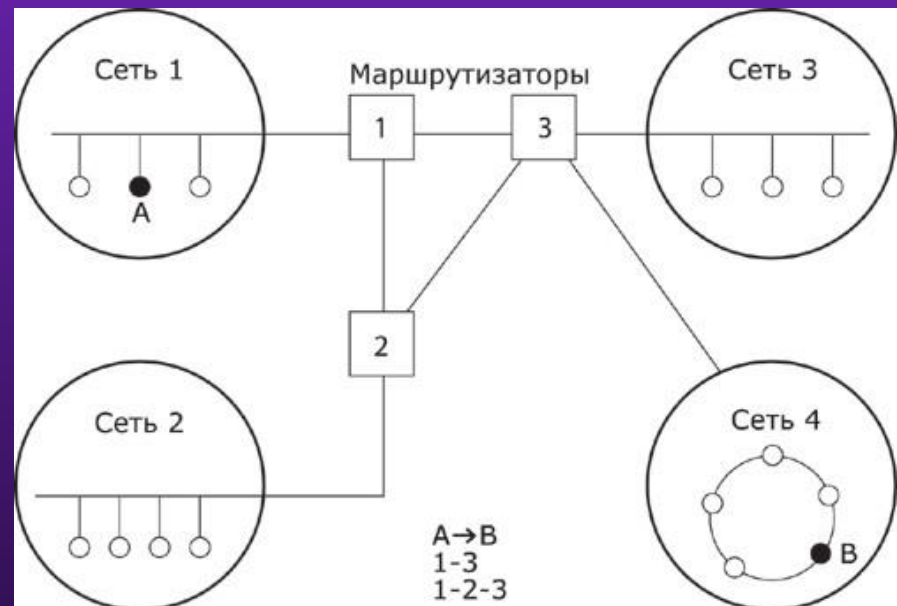


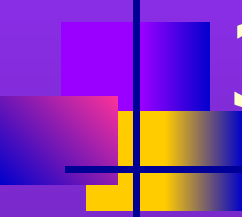
Маршрутизация

- Сети соединяются между собой специальными устройствами, называемыми *маршрутизаторами*.
- **Маршрутизатор** — это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает *пакеты сетевого уровня* в сеть назначения. Чтобы передать *сообщение* от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или **хопов** (от слова hop — прыжок), каждый раз выбирая подходящий *маршрут*. Таким образом, **маршрут** представляет собой последовательность *маршрутизаторов*, через которые проходит *пакет*.
- *Сетевой уровень* должен обеспечить доставку *пакета*:
 - между любыми двумя узлами сети с произвольной топологией;
 - между любыми двумя сетями в *составной сети*;
- **Сеть** — совокупность компьютеров, использующих для обмена данными единую сетевую технологию;
- **Маршрут** — последовательность прохождения *пакетом маршрутизаторов* в *составной сети*.

Маршруты движения пакетов

- На рисунке показаны четыре сети, связанные тремя маршрутизаторами. Между узлами A и B данной сети пролегает два маршрута:
 - первый — через маршрутизаторы 1 и 3,
 - второй — через маршрутизаторы 1, 2 и 3.

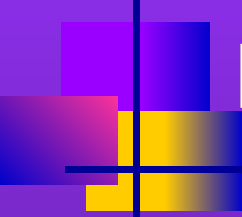




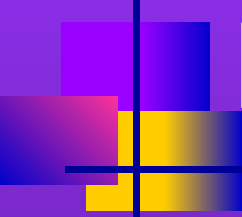
Задачи маршрутизации

- Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач *сетевого уровня*.
- Эта проблема осложняется тем, что самый короткий путь — не всегда самый лучший. Часто критерием при выборе *маршрута* является время передачи данных; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может с течением времени изменяться. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время.
- Выбор *маршрута* может осуществляться и по другим критериям, таким как *надежность* передачи.
- В общем случае функции *сетевого уровня* шире, чем функции передачи сообщений по связям с нестандартной структурой, которые мы рассмотрели на примере объединения нескольких локальных сетей.
- *Сетевой уровень* также решает задачи согласования разных технологий, упрощения *адресации* в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Маршрутизируемый протокол

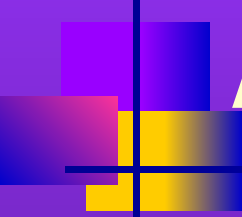


- Маршрутизируемый протокол – любой сетевой протокол, который обеспечивает в адресе сетевого уровня достаточно информации, чтобы передавать пакет от одной хост-машины к другой на основе принятой схемы адресации.
- Маршрутизируемый протокол определяет формат и назначение полей внутри пакета.
- В общем случае пакеты переносятся от одной станции к другой.
- Примеры маршрутизируемых протоколов – IP, IPX.



Протоколы маршрутизации

- Протокол маршрутизации – поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации.
- Сообщения протокола маршрутизации циркулируют между маршрутизаторами для обмена информацией и атуализации данных таблиц маршрутизации.
- Примеры протоколов маршрутизации:
 - RIP – протокол маршрутной информации;
 - IGRP – протокол внутренней маршрутизации между шлюзами;
 - EIGR – усовершенствованный протокол внутренней маршрутизации между шлюзами;
 - OSPF – протокол маршрутизации с выбором кратчайшего пути.

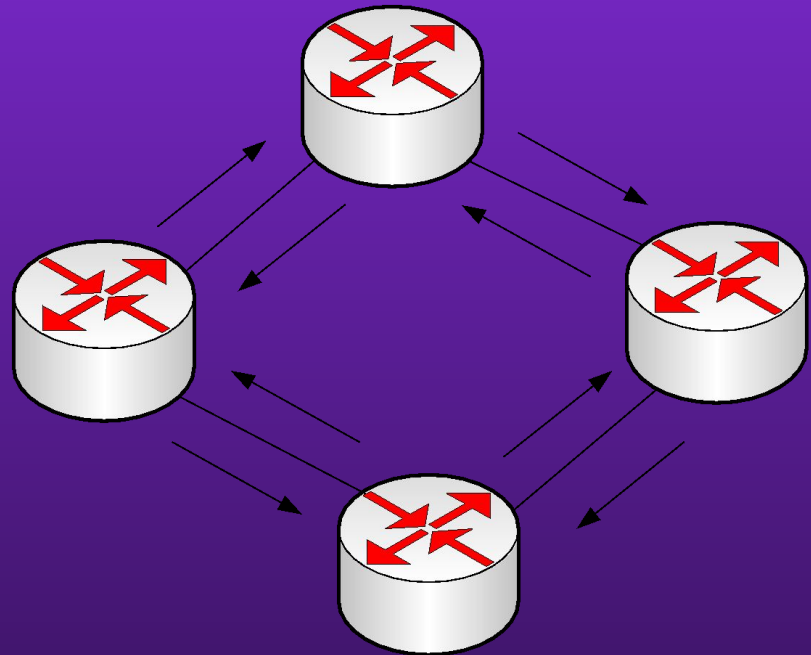


Алгоритмы маршрутизации

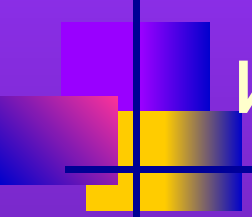
- Большинство алгоритмов маршрутизации можно свести к трем основным:
 - Маршрутизация на основе вектора расстояния – определяется направление (вектор) и расстояние до каждого канала в сети;
 - Маршрутизация на основе оценки состояния канала (выбор на основе кратчайшего пути), при которой воссоздается точная топология всей сети (по крайней мере, где размещается маршрутизатор);
 - Гибридный подход, объединяющий вышеуказанные алгоритмы.

Алгоритмы маршрутизации по вектору расстояния

- Алгоритмы маршрутизации на основе вектора расстояния (алгоритмы Беллмана-Форда) предусматривают периодическую передачу копий таблицы маршрутизации от одного маршрутизатора другому. Такие передачи позволяют актуализировать изменения в топологии сети.
- Каждый маршрутизатор получает информацию от соседнего маршрутизатора.
- При добавлении информации в таблицу маршрутизации добавляется величина, отражающая вектор расстояния (например, число переходов) и далее информация передается следующему маршрутизатору.

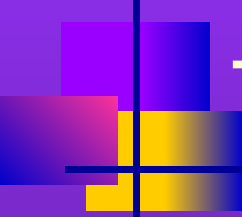


Алгоритм маршрутизации по вектору расстояния и исследованию сети



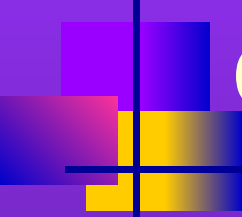
- В данных алгоритмах каждый маршрутизатор начинает с идентификации или исследования своих соседей. Порт к каждой непосредственно подключенной сети имеет расстояние 0.
- Продолжая процесс исследования векторов расстояния в сети, маршрутизаторы открывают наилучший путь до сети пункта назначения на основе информации от каждого соседа.
- Каждая запись в таблице маршрутизации имеет коммулятивное значение вектора расстояния, показывающая насколько далеко данная сеть находится в этом направлении.

Алгоритм маршрутизации по вектору расстояния и изменение топологии

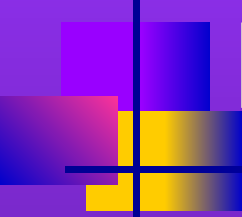


- При изменении топологии сети, использующей протокол на основе вектора расстояния, таблицы маршрутизации должны быть обновлены.
- Обновление содержания таблиц маршрутизации выполняется шаг за шагом от одного маршрутизатора к другому.
- Алгоритмы с вектором расстояния заставляют каждый маршрутизатор отправлять всю таблицу маршрутизации каждому своему непосредственному соседу.
- Таблицы маршрутизации, генерируемые в рамках метода вектора расстояния, содержат информацию об общей стоимости пути (метрика) и логический адрес маршрутизатора, стоящего на пути к каждой известной ему сети.

Маршрутизация с учетом состояния канала связи

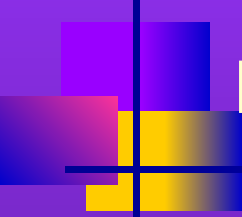


- Алгоритмы маршрутизации с учетом канала связи также называются *алгоритмы выбора первого кратчайшего пути (shortest path first, SPF)*.
- Данные алгоритмы поддерживают базу данных топологической информации.
- Для выполнения маршрутизации по данному алгоритму используются специальные сообщения объявлений о состоянии канала (link state advertisements, LSA), база данных топологии, SPF-алгоритм, результирующее SPS-дерево и таблица маршрутизации, содержащая пути и порты к каждой сети.



Режим исследования сети

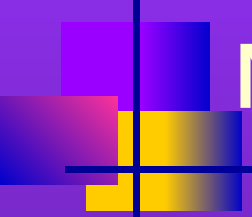
- В режиме исследования сети при маршрутизации с учетом состояния канала связи выполняются следующие процессы:
 - Маршрутизаторы обмениваются LSA-сообщениями, начиная с непосредственно подключенных маршрутизаторов;
 - Маршрутизаторы параллельно друг с другом топологическую базу данных, содержащую все LSA-сообщения;
 - SPF-алгоритм вычисляет достижимость сетей, определяя кратчайший путь до каждой сети комплекса. Маршрутизатор создает эту логическую топологию кратчайших путей в виде SPF-дерева, помещая себя в корень. Это дерево отображает пути от маршрутизатора до всех пунктов назначения.
 - Наилучшие пути и порты, имеющие выход на эти сети назначения, сводятся в таблицы маршрутизации. Также формируется базы данных с топологическими элементами и подробностями о статусе.



Обработка изменений топологии в протоколах маршрутизации

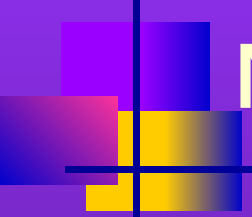
- Алгоритмы учета состояния канала связи полагаются на маршрутизаторы, имеющие общее представление о сети.
- Для достижения сходимости каждый маршрутизатор выполняет:
 - Отслеживает своих соседей: имя, рабочее состояние и стоимость линии связи;
 - Создает LSA-пакетов, в котором приводится перечень имен соседних маршрутизаторов и стоимость линий связи, а также данные о новых соседях и об изменениях в стоимости линий;
 - Посылает LSA-пакет на другие маршрутизаторы;
 - Получая LSA-пакет, записывает его в базу данных;
 - Используя накопленные данные LSA-пакетов для создания полной карты топологии сети, маршрутизатор запускает на исполнение SPF-алгоритм и рассчитывает оптимальные маршруты до каждой сети.

Сравнение методов маршрутизации



- Процесс маршрутизации по вектору расстояния получает топологические данные из таблиц маршрутизации соседних маршрутизаторов. Процесс маршрутизации SPF получает широкое представление обо всей топологии сетевого комплекса, собирая данные из всех LSA-пакетов;
- Процесс маршрутизации по вектору расстояния определяет лучший путь с помощью сложения метрик по мере того как таблица движется от одного маршрутизатора к другому. При использовании маршрутизации SPF каждый маршрутизатор работает отдельно, вычисляя свой собственный оптимальный путь;

Сравнение методов маршрутизации



- В большинстве протоколов маршрутизации по вектору расстояния пакеты актуализации, содержащие сведения об изменениях топологии, являются периодически посылаемыми пакетами актуализации таблиц. Эти таблицы передаются от одного маршрутизатора к другому, что приводит к медленной сходимости;
- В протоколах маршрутизации SPF пакеты актуализации генерируются и рассылаются по факту возникновения изменения топологии. Относительно небольшие LSA-пакеты передаются всем маршрутизаторам, что приводит к более быстрой сходимости при любом изменении топологии сети.