TCP/IP
Прикладные протоколы

Протоколы ARP/RARP (RFC 826)

- Получение физического адреса по IP (ARP)
- Получение IP по физическому адресу (RARP) (RFC 903)
- Получение IP по локальному (ATM, FrameRelay) адресу (InARP) (RFC 2390)

ARP packet structure

bits	0-7	8-15	16-31
0	Hardware type (HTYPE)		Protocol type (PTYPE)
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)
64	Sender hardware address (SHA)		
??	Sender protocol address (SPA)		
??	Target hardware address (THA)		
??	Target protocol address (TPA)		

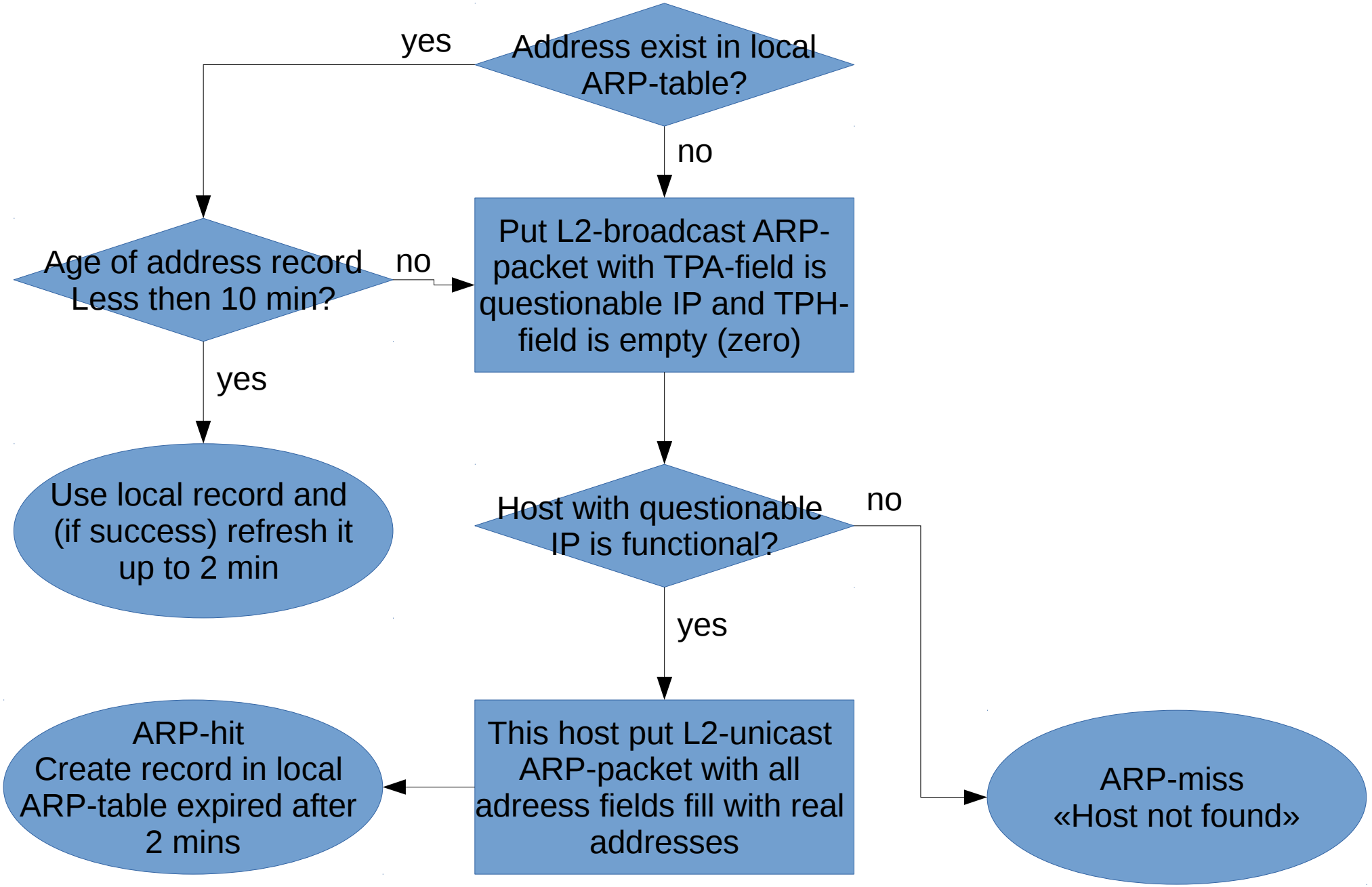
ARP request (sample)

bits	0-7	8-15	16-31
0	Hardware type = 0x0001		Protocol type = 0x0800
32	Hardware length = 6	Protocol length = 4	Operation = 0x0001
64	SHA (first 32 bits) = 0x000958D8		
96	SHA (last 16 bits) = 0x1122		SPA (first 16 bits) = 0x0A0A
128	SPA (last 16 bits) = 0x0A7B		THA (first 16 bits) = 0xFFFF
160	THA (last 32 bits) = 0xFFFFFFFF		
192	TPA = 0x0A0A0A8C		

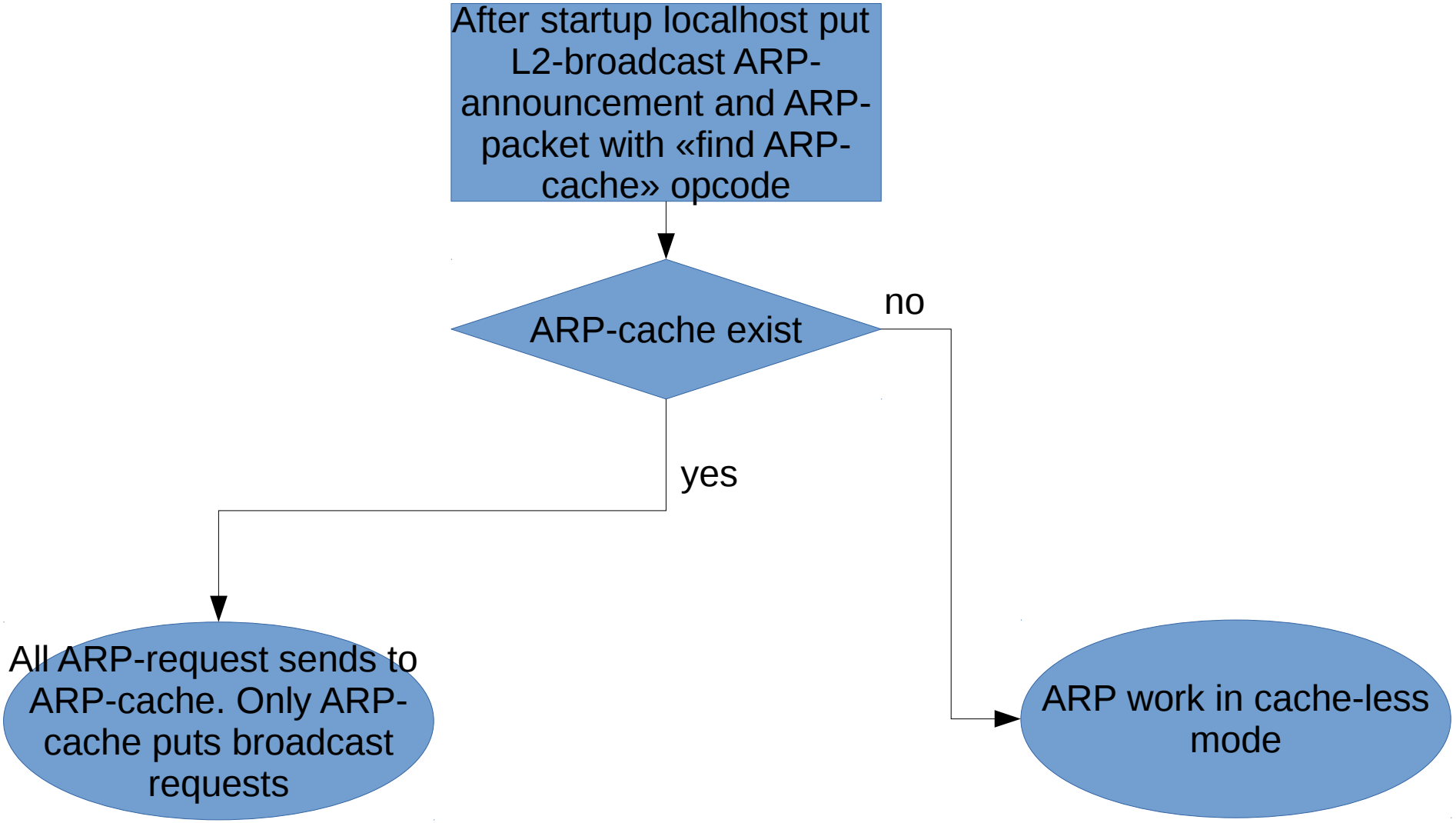
ARP answer (sample)

bits	0-7	8-15	16-31
0	Hardware type = 0x0001		Protocol type = 0x0800
32	Hardware length = 6	Protocol length = 4	Operation = 0x0002
64	SHA (first 32 bits) = 0x000958D8		
96	SHA (last 16 bits) = 0x33AA		SPA (first 16 bits) = 0x0A0A
128	SPA (last 16 bits) = 0x0A8C		THA (first 16 bits) = 0x0009
160	THA (last 32 bits) = 0x58D81122		
192	TPA = 0x0A0A0A7B		

Work ARP in cash-less mode



Work ARP in cash-enable mode



ARP-cache collect MAC-addresses from own broadcast investigations, from ARP-invites, optionally from router searches. Hence you must use local router or L3-switch as ARP-cache for perfomance hit.

RARP

Протокол применяется во время загрузки узла, когда он посылает групповое сообщение-запрос со своим физическим адресом. Сервер принимает это сообщение и просматривает свои таблицы в поисках соответствующего физическому, IP-адреса. После обнаружения найденный адрес отсылается обратно на запросивший его узел. Другие станции также могут «слышать» этот диалог и локально сохранить эту информацию в своих ARP-таблицах.

RARP позволяет разделять IP-адреса между не часто используемыми хост-узлами. После использования каким-либо узлом IP-адреса он может быть освобождён и выдан другому узлу.

Bootstrap Protocol (RFC 951)

Используется для автоматического получения IP-адресов во время первоначальной загрузки хоста (в т.ч. бездисковых станций) до загрузки ОС.

Поддержка протокола может содержаться в BIOS материнских плат.

Trivial File Transfer Protocol (КАС 1350)

- не содержит механизмов аутентификации
- работает «поверх» UDP
- простота реализации

Используется для загрузки бездисковых станций, конфигурирования (загрузка файлов конфигурации) активного сетевого оборудования, обновление firmware по сети.

Формат пакета WRQ, RRQ

	Packet type	File name	Term. byte	Op. mode	Term. byte	Options
Data type	0x01/0x02	ASCII string	0x00	ASCII string	0x00	
Lenght	2	variable	1	variable	1	

Packet types

- Read Request (RRQ, #1) — запрос на чтение файла.
- Write Request (WRQ, #2) — запрос на запись файла.
- Data (DATA, #3) — данные, передаваемые через TFTP.
- Acknowledgment (ACK, #4) — подтверждение пакета.
- Error (ERR, #5) — ошибка.
- Error2 (ERR2, #6) — ошибка2.

Options

Op. code	Term. byte	Op. Value	Term. byte
ASCII string	0x00	ASCII string	0x00

Op.code	Описание
netascii	файл перед передачей перекодируется в ASCII
octet	файл передается без изменений
blksize	Число, принимающее значение от 8 до 65464, обозначающее размер блока.
timeout	Число, принимающее значение от 1 до 255, обозначающее время ожидания перед повторной передачей блока в секундах
tsize	Число, обозначающее размер передаваемого файла в байтах

Сообщения об ошибках

	Packet type	Error Code	Error Description	Term. byte
Data type	0x05	binary	ASCII string	0x00
Lenght	2	2	variable	1

Error Code	Error Descriptions
0	Unknown Error, see additional info
1	File not found
2	Access Denied
3	Could not allocate space on filesystem #
4	Invalid TFTP operation
5	Invalid Transfer ID
6	File already exist
7	User not found
8	Invalid option

Direct Host Configuration Protocol (RFC 2131)

Предназначен для настройки сетевого окружения хоста (первоначально для автоматического распределения IP-адресов)

- локальный IP-адрес;
- маска подсети;
- IP-адрес маршрутизатора по умолчанию;
- адреса серверов DNS;
- имя домена DNS

Является наследником BOOTP и обратно совместим с ним.

Ресурсы DHCP:

- динамические (e.g. ip-адреса);
- статические (адреса серверов, параметры протоколов)

Способы предоставления динамических ресурсов:

- Ручное. При этом способе сетевой администратор сопоставляет MAC-адресу каждого хоста определённый IP-адрес. Данный способ распределения адресов отличается от ручной настройки тем, что сведения об адресах хранятся централизованно, и потому их проще изменять при необходимости.
- Автоматическое. Каждому хосту на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
- Динамическое. Адрес выдаётся хосту на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый.

Схема работы DHCP

- DHCPDISCOVER
- DHCPOFFER
- DHCPREQUEST
- DHCPACK(NOLEGEMENT)
- DHCPDECLINE

Протоколы маршрутизации

Протокол маршрутизации – сетевой протокол, используемый маршрутизаторами для построения топологии сети и возможных маршрутов следования данных в этой сети.

	Дистанционно-векторные протоколы (DVA)	Протоколы состояния каналов связи (LSA)
Interior Gateway Protocls	RIP RIPv2 IGRP	OSPF IS-IS level 1,2
Exterior Gateway Protocols	EGP BGP	IS-IS level 3

RIP, RIPv2

- Создан в 1969 для сети ARPANet
- Использован алгоритм Беллмана-Форда
- Работает поверх UDP
- Передаёт информацию об изменении топологии оперативно, полные таблицы маршрутизации 1 раз в 30 сек
- В версии 2 исправлены критические ошибки, в т.ч. те, которые приводили к зацикливанию пакетов
- Добавлены безклассовая адресация, аггрегирование сетей и поддержка аутентификации

OSPF (Open Shortest Path First)

- Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- Поддержка бесклассовой адресации и агрегирования сетей;
- Оптимальное использование пропускной способности путём построения дерева кратчайших путей по алгоритму Дейкстры;
- Поддерживаемые сети L2: широковещательные сети со множественным доступом (Ethernet, Token Ring); точка-точка (T1, E1, коммутируемый доступ); нешироковещательные сети со множественным доступом (Frame relay)

Алгоритм работы протокола:

1) Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определённых параметрах, указанных в их hello-пакетах.
2) На следующем этапе работы протокола маршрутизаторы будут пытаться перейти в состояние смежности со своими соседями. Переход в состояние смежности определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии смежности, синхронизирует между собой базу данных состояния каналов.
3) Каждый маршрутизатор посылает объявления о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности.
4) Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает передаваемую в нём информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим смежным с ним маршрутизаторам.
5) Рассылая объявления внутри одной OSPF-зоны, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.
6) Когда база данных построена, каждый маршрутизатор использует алгоритм «кратчайший путь первым» для вычисления графа без петель, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф — дерево кратчайших путей.
7) Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайших путей.

Internet Control Message Protocol (RFC 792)

- используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, (e.g. запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают)
- также на ICMP возлагаются некоторые сервисные функции
- работает непосредственно поверх протокола IP, вследствие чего подвержен уязвимости «man-in-the middle»

Формат пакета

bits	0-7	8-15	16-31
32	Type	Code	CRC16
...	Data (Depend of Type and Code)		

ICMP Types

1,2	Reserved
3	Адресат недоступен
4	Отключение источника при переполнении очереди
5	Перенаправление
6	Альтернативный адрес узла
7	Reserved
8	Эхо-запрос
9	Объявление маршрутизатора
10	Запрос маршрутизатора
11	Время жизни дейтаграммы истекло
12	Ошибка в IP-заголовке или отсутствует необходимая опция
13	Запрос метки времени
14	Ответ с меткой времени
15	Информационный запрос
16	Информационный ответ
17	Запрос адресной маски
18	Отклик на запрос адресной маски
19	Reserved (для обеспечения безопасности)
20-29	Reserved (для экспериментов на устойчивость к ошибкам)
30	Трассировка маршрута
31	Ошибка преобразования датаграммы
32	Перенаправление для мобильного узла
33	IPv6 Where-Are-You (где вы находитесь)
34	IPv6 I-Am-Here (я здесь)
35	Запрос перенаправления для мобильного узла
36	Отклик на запрос перенаправления для мобильного узла
37	Запрос доменного имени
38	Ответ на запрос доменного имени
39	SKIP
40	Объявления безопасности
41-255	Not used

Особенности проектирования ICMP с целью снижения трафика

- 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
- При повреждении фрагментированного IP-пакета ICMP-сообщение отправляется только после получения первого повреждённого фрагмента, поскольку отправитель всё равно повторит передачу всего IP-пакета целиком

Спасибо за внимание!