29

Стек TCP/IP

За основу этой главы был взят перевод соответствующей главы книги World of Protocols, © RADCOM Ltd., 1999. Перевод впоследствии был расширен и дополнен с использованием материалов из различных RFC

Агентство DARPA (Defense Advance Research Projects Agency) разработало протоколы TCP/IP (Transmission Control Protocol/Internet Protocol) для объединения в сеть компьютеров различных подразделений министерства обороны США. Международная распределенная сеть Internet использует стек протоколов TCP/IP для объединения компьютерных ресурсов всей планеты. Достаточно часто эти протоколы используются также в частных и коммерческих сетях. Стек TCP/IP включает следующие протоколы:

- IP/IPv6 - Internet Protocol.
- TCP - Transmission Control Protocol.
- UDP - User Datagram Protocol.

Канальный уровень

- ARP/RARP - Address Resolution Protocol/Reverse Address.

Протоколы туннелирования

- ATMP - Ascend Tunnel Management Protocol.
- L2F - Layer 2 Forwarding Protocol.

- L2TP - Layer 2 Tunneling Protocol.
- PPTP - Point-to-Point Tunneling Protocol.

Сетевой уровень

- DHCP/ DHCPv6 - Dynamic Host Configuration Protocol.
- DVMRP - Distance Vector Multicast Routing Protocol.
- ICMP/ICMPv6 - Internet Control Message Protocol.
- IGMP - Internet Group Management Protocol.
- MARS - Multicast Address Resolution Server.
- PIM - Protocol Independent Mulyicast.
- RIP - Routing Information Protocol.
- RIP2 - Routing Information Protocol II.
- RIPng for IPv6.
- RSVP - Resource ReSerVation setup Protocol.

Безопасность

- AH - Authentication Header.
- ESP - Encapsulating Security Payload.

Маршрутизация

- BGP-4 - Border Gateway Protocol.
- EGP - Exterior Gateway Protocol.
- EIGRP - Enhanced Interior Gateway Routing Protocol.
- GRE - Generic Routing Encapsulation.
- HSRP - Cisco Hot Standby Router Protocol.
- IGRP - Interior Gateway Routing.
- NARP - NBMA Address Resolution Protocol
- NHRP - Next Hop Resolution Protocol.
- OSPF - Open Shortest Path First.

Транспортный уровень

- Mobile IP.
- Van Jacobson - compressed TCP.
- XOT - X.25 over TCP.

VoIP

- MGCP - Media Gateway Control Protocol.
- SGCP - Simple Gateway Control Protocol.

Сеансовый уровень

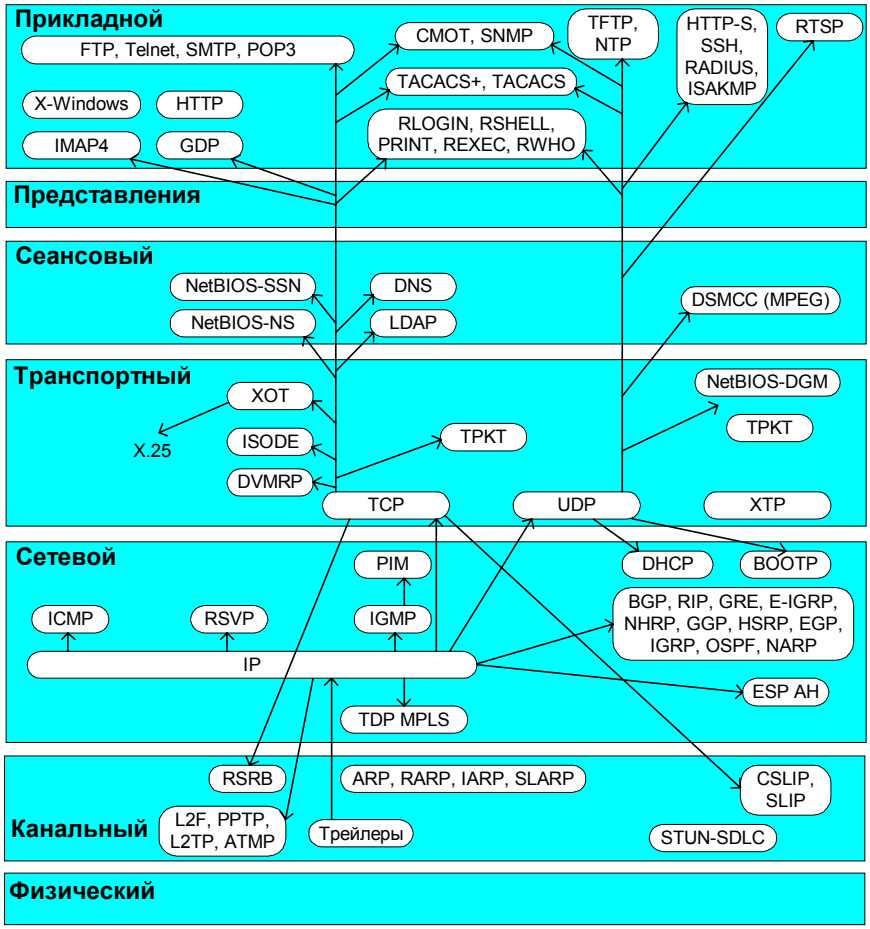
- DNS - Domain Name Service.
- NetBIOS/IP.

Прикладной уровень

- FTP - File Transfer Protocol.
- Finger User Information Protocol.
- TFTP - Trivial File Transfer Protocol.
- Gopher - Internet Gopher Protocol.

- HTTP - Hypertext Transfer Protocol.
- S-HTTP - Secure Hypertext Transfer Protocol.
- IMAP4 - Internet Message Access Protocol rev 4.
- IPDC - IP Device Control.
- ISAKMP - Internet Message Access Protocol version 4rev1.
- NTP - Network Time Protocol.
- POP3 - Post Office Protocol version 3.
- Radius.
- RLOGIN - Remote Login.
- RTSP - Real-time Streaming Protocol.
- SMTP - Simple Mail Transfer Protocol.
- SNMP - Simple Network Management Protocol.
- TACACS+ - Terminal Access Controller Access Control System.
- TELNET.
- X-Window.

Положение протоколов стека TCP/IP в модели OSI показано на рисунке.



Стек TCP/IP в эталонной модели OSI

IP

RFC 791 http://www.cis.ohio-state.edu/htbin/rfc/rfc791.html

RFC 1853 http://www.cis.ohio-state.edu/htbin/rfc/rfc1853.html

IP (Internet Protocol) представляет собой протокол уровня маршрутизируемых дейтаграмм в стеке TCP/IP. Все другие протоколы стека TCP/IP (кроме ARP и RARP) используют протокол IP для маршрутизации кадров между хостами. Заголовок кадров IP содержит маршрутную и управляющую информацию, связанную с доставкой дейтаграмм.

Структура заголовков IP показана на рисунке.

Структура заголовка IP.

Версия

Поле версии определяет формат заголовка Internet.

IHL

Internet Header Length - размер заголовка Internet указывает размер заголовка в 32-битовых словах, задавая смещение данных от начала пакета. Минимальный размер заголовка составляет 5 слов (160 битов).

Тип сервиса

Показывает желаемый уровень качества обслуживания. Сети могут обеспечивать различный уровень преимуществ при доставке, играющий важную роль при условиях высокой загрузки сети. Поддерживаются также три опции качества обслуживания - малая задержка, высокая надежность и высокая пропускная способность.

Биты 0 - 2 - преимущественная доставка

111 сетевое управление

110 межсетевое управление
101 CRITIC/ECP
100 Flash override
011 Flash
010 немедленная доставка
001 приоритетная доставка
000 Routine (нормальный режим)

Бит 3 - задержка

0 Нормальная
1 Малая

Бит 4 - пропускная способность

0 Нормальная
1 Высокая

Бит 5 - надежность доставки

0 Нормальная
1 Высокая

Биты 6 - 7 - зарезервированы для использования в будущем

Общий размер

Размер дейтаграммы в байтах с учетом заголовка и данных. Размер поля позволяет использовать дейтаграммы длиной до 65535 байтов, хотя такой размер нежелателен для многих сетей и хостов. Все хосты должны быть готовы к приему дейтаграмм размером до 576 байтов, независимо от того как они доставляются - целиком или фрагментами. Рекомендуется передавать дейтаграммы, размер которых превышает 576 байтов только в тех случаях, когда адресат готов принять такие дейтаграммы.

Идентификация

Значение идентификатора, которое отправитель задает для обеспечения корректного порядка сборки фрагментов дейтаграммы на приемной стороне.

Флаги

Трехбитовое поле флагов управления:

Бит 0 - зарезервирован и должен иметь нулевое значение

Бит 1 - возможность фрагментирования

0 Можно фрагментировать

1 Не фрагментировать

Бит 2 - наличие дополнительных фрагментов

0 Последний фрагмент

1 Есть последующие фрагменты

Смещение фрагмента

13-битовое значение, задающее смещение фрагмента от начала целой дейтаграммы. Смещение фрагмента измеряется в 8-байтовых (64 бита) словах. Первый фрагмент имеет нулевое смещение.

Время жизни

Показывает максимальное время существования дейтаграммы в сети Internet. При нулевом значении этого поля дейтаграмма должна быть уничтожена. Время жизни дейтаграмм измеряется в секундах. Однако, поскольку каждый модуль, работающий с дейтаграммой, должен уменьшать значение поля TTL (time-to-life) по крайней мере на 1 (даже в тех случаях, когда обработка дейтаграммы занимает меньше секунды), значение этого поля должно быть не меньше желаемого времени жизни дейтаграммы. Дейтаграммы с истекшим в процессе доставки временем жизни не попадают к получателю.

Протокол

Указывает протокол следующего уровня, содержащийся в поле данных дейтаграммы IP.

Контрольная сумма заголовка

Контрольная сумма, рассчитанная с учетом только полей заголовка дейтаграммы. Поскольку некоторые поля заголовка (например, время жизни) могут меняться в процессе доставки, значение контрольной суммы заново вычисляется и проверяется в каждой точке обработки заголовков.

Адрес отправителя/ получателя

32-битовые значения адресов отправителя и получателя дейтаграммы. Следует четко различать имена, адреса и маршруты. *Имя* показывает название объекта, *адрес* говорит о его местоположении в сети, а *маршрут* - показывает путь к объекту. Протокол IP имеет дело преимущественно с адресами. Связь между адресами и именами реализуется протоколами вышележащих уровней. Модуль Internet отображает адреса IP на локальные сетевые адреса. Связь локальных сетевых адресов с маршрутами обеспечивается протоколами нижележащих уровней.

Опции

Это поле содержит необязательные опции дейтаграммы. Используемые опции должны быть реализованы во всех модулях IP (хосты и шлюзы). В некоторых опции безопасности являются обязательными для всех дейтаграмм.

Поле опций имеет переменную длину и может содержать различное число опций. Существуют два формата опций:

- Однооктетные опции
- Многооктетные опции, содержащие поля типа опции (1 октет), ее размера (1 октет) и собственно опций.

Поле длины опции учитывает все субполя опции - тип, размер и сами опции.

Октет типа опции имеет три поля:

1 бит - флаг копирования показывает, что должна ли данная опция копироваться во все фрагменты дейтаграммы:

0 опция копируется
1 опция не копируется.

2 бита - класс опции:

0 управление
1 зарезервировано
2 отладка и измерение
3 зарезервировано

5 битов - номер опции

Данные

Данные IP или протоколов вышележащих уровней.

IPv6

RFC 1883 http://www.cis.ohio-state.edu/htbin/rfc/rfc1883.html

RFC 1826 http://www.cis.ohio-state.edu/htbin/rfc/rfc1826.html

RFC 1827 1995-12 http://www.cis.ohio-state.edu/htbin/rfc/rfc1827.html

IPv6 представляет собой обновленную версию протокола Internet, разработанную на основе IPv4. Оба протокола (IPv6 и IPv4) различаются на уровне среды. Например, пакеты IPv6 передаются через сеть Ethernet с использованием идентификатора типа 86DD вместо 0800 для IPv4.

IPv6 расширяет адресное пространство IP за счет использования 128-битовых адресов вместо принятых в IPv4 32-битовых. Такое расширение позволяет также увеличить число уровней сетевой иерархии, упростить процессы автоматической настройки адресов и во много раз увеличить число хостов в сети. В дополнение к этому вводится масштабируемость групповых (multicast) адресов и определяется новый тип адреса *anycast* (кому-нибудь) для передачи пакетов любому узлу из группы.

Расширенная поддержка опций - опции IPv6 помещаются в отдельный заголовок, располагающийся между заголовком IPv6 и заголовком транспортного уровня. Изменения в способе представления опций заголовка IP делают рассылку пакетов более эффективной, снижают уровень ограничений на размер опций, а также обеспечивают дополнительную гибкость при введении новых опций в будущем. В число расширений заголовка опций входят: Hop-by-Hop, Routing (Type 1), Fragment, Destination Option, Authentication, Encapsulation Payload.

Возможность маркирования потоков добавлена для того, чтобы помечать пакеты, требующие специальной обработки (например, нестандартных условий QoS или обработки в реальном масштабе времени).

Структура заголовков IPv6 показана на рисунке.

Структура заголовка IPv6.

Версия

Номер версии протокола Internet (6).

Приоритет

Это поле позволяет отправителю указать желаемый уровень приоритета доставки пакета. Значения уровней приоритета делятся на две группы - с контролем насыщения, обеспечиваемым отправителем, и без контроля насыщения.

Метка потока

Метки используются отправителем для пакетов, которым требуются специальные условия обработки в маршрутизаторах IPv6. Для уникальной идентификации потока используется комбинация адреса отправителя и ненулевого значения метки потока.

Размер содержимого

Размер поля содержимого пакета (в октетах).

Следующий заголовок

Указывает тип заголовка, следующего непосредственно после заголовка IPv6.

Число интервалов

8-битовое целое число, уменьшаемое на 1 каждым узлом, который пересылает пакет. При обнулении этого поля пакет отбрасывается.

Адрес отправителя

128-битовый адрес отправителя пакета.

Адрес получателя

128-битовый адрес получателя пакета.

TCP

RFC 793 http://www.cis.ohio-state.edu/htbin/rfc/rfc793.html

RFC 1072 http://www.cis.ohio-state.edu/htbin/rfc/rfc1072.html

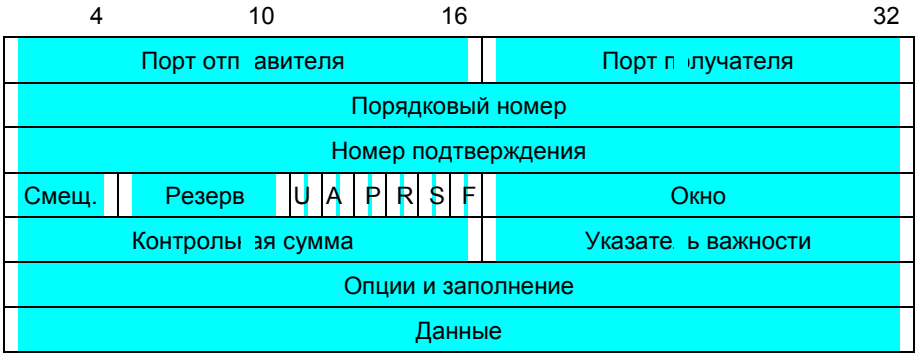
RFC 1693 http://www.cis.ohio-state.edu/htbin/rfc/rfc1693.html

RFC 1146 http://www.cis.ohio-state.edu/htbin/rfc/rfc1146.html

RFC 1323 http://www.cis.ohio-state.edu/htbin/rfc/rfc1323.html

Протокол TCP обеспечивает надежную доставку потоков и сервис поддержки виртуальных соединений за счет использования подтверждений и повторной передачи пакетов при возникновении необходимости.

Структура заголовка TCP показана на рисунке.



Структура заголовка TCP

Порт отправителя

Номер порта-отправителя.

Порт получателя

Номер порта-получателя.

Порядковый номер

Порядковый номер первого октета в данном сегменте (за исключением присутствия SYN). При наличии SYN поле порядкового номера содержит изначальный порядковый номер (Initial Sequence Number - ISN) и первый октет имеет номер ISN+1.

Номер подтверждения

Если бит управления ACK установлен (1), это поле содержит значение следующего порядкового номера, который отправитель сегмента ожидает

получить. После организации соединения значение этого поля устанавливается во всех случаях.

Смещение данных

4-битовое поле, указывающее число 32-битовых слов в заголовке TCP. После заголовка размещаются данные, поэтому поле указывает на начало данных в пакете. Заголовок пакетов TCP всегда имеет размер, кратный 32 битам.

Резерв

Зарезервированное поле размером 6 битов.

Биты управления

6 битовое поле, содержащее флаги управления:

U (URG) - значимое поле указателя важности;

A (ACK) - значимое поле подтверждения;

P (PSH) - функция push;

R (RST) - сброс соединения;

S (SYN) - синхронизация порядковых номеров;

F (FIN) - нет данных от отправителя.

Окно

16-битовое поле, содержащее число октетов данных, которые отправитель данного сегмента будет воспринимать, начиная с октета, указанного в поле подтверждения.

Контрольная сумма

16-битовое значение контрольной суммы, вычисляемой для 16-битовых слов заголовка и текста. Если сегмент содержит нечетное число октетов в заголовке /или тексте, последние октеты дополняются справа 8 нулями для выравнивания по 16-битовой границе. Биты заполнения (0) не передаются в сегменте и служат только для расчета контрольной суммы. При расчете контрольной суммы значение самого поля контрольной суммы принимается равным 0.

Указатель важности

16-битовое значение положительного смещения от порядкового номера в данном сегменте. Это поле указывает порядковый номер октета, с которого начинаются важные (urgent) данные. Поле принимается во внимание только для пакетов с установленным флагом U.

Опции

Опции передаются в конце заголовка TCP и всегда имеют размер, кратный 8 битам. При расчете контрольной суммы пакета значения опций принимаются во внимание. Опции могут начинаться на любой границе октета.

Существуют два формата опций:

- Однооктетные опции
- Многооктетные опции, содержащие поля типа опции (1 октет), ее размера (1 октет) и собственно опций.

Поле длины опций учитывает все субполя опций - тип, размер и сами опции.

Список опций может закончиться раньше, нежели указывает поле смещения данный, поэтому значения битов после поля End-of-Option должны быть заполнены нулями.

Протокол TCP Должен реализовать все опции.

Данные

Поле данных TCP или протоколов вышележащих уровней.

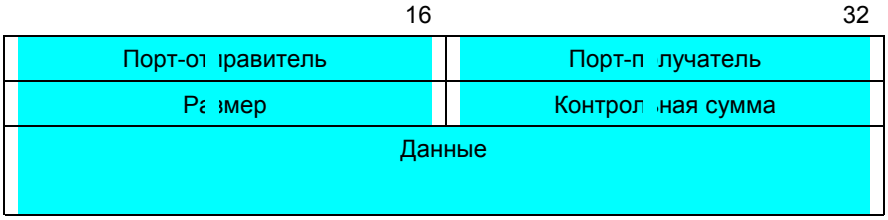
Пример декодирования TCP over ATM

UDP

RFC768 http://www.cis.ohio-state.edu/htbin/rfc/rfc768.html

Протокол UDP (User Datagram Protocol - протокол пользовательских дейтаграмм) обеспечивает простой сервис передачи сообщений без гарантии доставки для ориентированных на транзакции услуг. Каждый заголовок UDP содержит идентификаторы портов отправителя и получателя, которые позволяют протоколам вышележащих уровней связать указанные приложения и услуги с хостами.

Структура заголовков UDP показана на рисунке.



Структура заголовков UDP

Порт-отправитель

Необязательное поле, указывающее порт процесса-отправителя. По номеру указанного в этом поле порта адресуются ответы, если явно не указан другой порт. При отсутствии номера порта-отправителя это поле заполняется нулями.

Порт-получатель

Номер порта-получателя, рассматриваемый в контексте указанного IP-адреса получателя.

Размер

Размер данной пользовательской дейтаграммы в октетах с учетом заголовка и данных. Минимальная длина дейтаграммы составляет 8 октетов.

Контрольная сумма

16-битовое значение контрольной суммы псевдозаголовка, содержащего информацию из заголовков IP и UDP, а также данных с дополнением (при необходимости) нулей для выравнивания по двухоктетной границе.

Данные

Поле данных UDP.

ARP/RARP

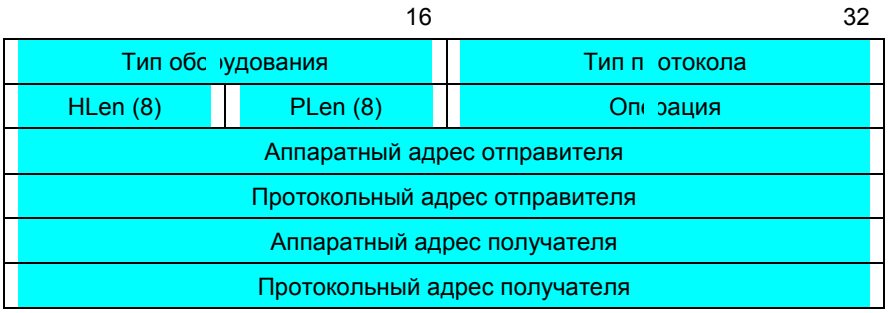
RFC826 1982-11 http://www.cis.ohio-state.edu/htbin/rfc/rfc826.html

RFC1293 1992-01 http://www.cis.ohio-state.edu/htbin/rfc/rfc1293.html

RFC1390 1993-01 http://www.cis.ohio-state.edu/htbin/rfc/rfc1390.html

TCP/IP использует протоколы ARP (Address Resolution Protocol - протокол преобразования адресов) и RARP (Reverse Address Resolution Protocol - протокол обратного преобразования адресов) для инициализации использования адресов Internet в сетях Ethernet и сетях иных типов, использующих метод MAC (media access control) для управления доступом к среде передачи. Протокол ARP позволяет хостам обмениваться информацией с другими хостами в тех случаях, когда известен только IP-адрес ближайшего соседа. Перед тем, как использовать IP хост передает широковещательный запрос ARP, содержащий IP-адрес желаемой системы-получателя.

Структура заголовков ARP/RARP показана на рисунке.



Структура заголовков ARP/RARP

Тип оборудования

Указывает тип интерфейса, для которого отправителю нужен отклик.

Тип протокола

Задает тип адреса вышележащего протокола, который представляет отправитель.

HLen

Размер аппаратного адреса.

PLen

Размер протокольного адреса.

Операция

Поддерживаются следующие типы операций:

1 запрос ARP.
2 отклик ARP.
3 запрос RARP.
4 отклик RARP.
5 запрос Dynamic RARP.
6 отклик Dynamic RARP.
7 ошибка Dynamic RARP.
8 запрос InARP.
9 отклик InARP.

Аппаратный адрес отправителя

Аппаратный адрес отправителя размером HLen.

Протокольный адрес отправителя

Протокольный адрес отправителя размером PLen.

Аппаратный адрес получателя

Аппаратный адрес получателя размером HLen.

Протокольный адрес получателя

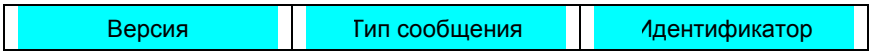
Протокольный адрес получателя размером PLen.

ATMP

RFC 2107 http://www.cis.ohio-state.edu/htbin/rfc/rfc2107.html

ATMP (Ascend Tunnel Management Protocol - протокол управления туннелями компании Ascend) представляет собой протокол, используемый в настоящее время компанией Ascend Communications для организации виртуального присутствия программ доступа по коммутируемым линиям в удаленной сети. Пользователь соединяется по телефонной линии с сервером удаленного доступа в сеть (NAS), но вместо использования адреса, непосредственно входящего в сеть, где установлен сервер NAS, клиентские программы используют адрес, относящийся к "домашней сети" пользователя. Этот адрес может предоставлять клиентская программа или он выделяется из пула адресов "домашних сетей". В любом случае этот адрес связывается с "домашней сетью" и для маршрутизации пакетов от клиента и к нему требуется использовать специальные соглашения. Для обмена данными используется туннель между сервером NAS и специальным "домашним агентом" (Home Agent - HA) в "домашней сети.

Формат заголовка ATMP показан на рисунке.



Формат заголовка ATMP

Версия

Текущий номер версии протокола ATMP (1).

Тип сообщения

Протокол ATMP определяет набор сообщений для запросов и откликов, передаваемых с использованием протокола UDP. Используемые для сообщений коды приведены ниже.

Тип сообщения	***Код***
Registration Request	1
Challenge Request	2
Challenge Reply	3
Registration Reply	4
Deregister Request	5
Deregister Reply	6
Error Notification	7

Идентификатор

16-битовое значение, служащее для сопоставления откликов с запросами. Для каждого нового запроса должен использоваться новый идентификатор. При повторной передаче запроса используется прежний идентификатор.

L2F

RFC 2341 http://www.cis.ohio-state.edu/htbin/rfc/rfc2341.html

Протокол рассылки канального уровня L2F (layer 2 Forwarding Protocol) позволяет организовать туннелирование канального уровня протоколами вышележащих уровней. Использование таких туннелей позволяет избавиться от связи местоположения изначального сервера dial-up с местом завершения коммутируемого соединения и обеспечения доступа в сеть.

Формат пакетов L2F показан на рисунке.

Формат пакетов L2F

Версия

Старшая часть номера версии программы L2F, создавшей пакет.

Протокол

Указывает протокол, передаваемый в пакетах L2F.

Номер

Порядковый номер пакета присутствует в заголовке, если флаг S установлен.

Идентификатор мультиплексирования

Идентификатор мультиплексирования служит для обозначения отдельных соединений в туннеле.

Идентификатор клиента

Идентификатор клиента (CLID) помогает демультиплексировать туннели в конечных точках.

Размер

Размер (в октетах) целого пакета с учетом заголовка, всех полей и содержимого.

Смещение содержимого

Указывает смещение начала содержимого пакета от конца заголовка L2F (в байтах). Это поле присутствует в пакетах с установленным флагом F.

Ключ пакета

Поле ключа используется в пакетах с установленным флагом K и используется в процессе аутентификации.

Контрольная сумма

Контрольная сумма пакета, используемая при установке флага C.

Опции

После организации соединения конечные точки проверяют наличие L2F на удаленной стороне и выполняют аутентификацию. Поле протокола для таких сообщений всегда имеет значение 1 (управляющие сообщения L2F). Сами сообщения структурированы как последовательность октетов, содержащих значения опций. Когда поле протокола указывает на L2F-управление, тело пакета содержит опции (возможно, их число равно 0). Каждая опция представляет собой однооктетное сообщение, за которым могут следовать субопции. Каждая субопция представляет собой однобайтовое значение, за которым могут следовать дополнительные субопции.

Список поддерживаемых опций приведен ниже:

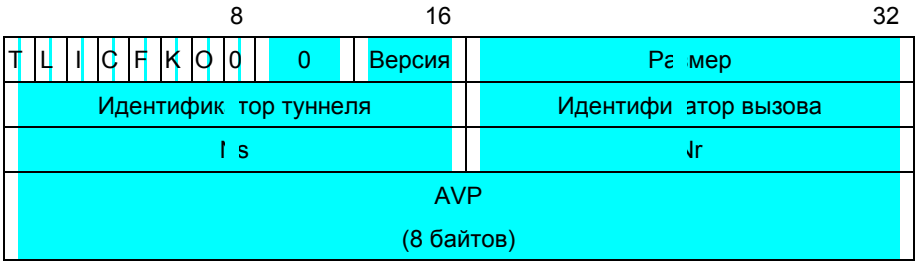
0x00	Invalid	некорректное сообщение
0x01	L2F_CONF	конфигурация запроса
0x02	L2F_CONF_NAME	имя партнера (peer), передающего L2F_CONF
0x03	L2F_CONF_CHAL	случайный номер связанный с peer
0x04	L2F_CONF_CLID	Assigned_CLID для используемого peer
0x02	L2F_OPEN	конфигурация восприятия (Accept)
0x01	L2F_OPEN_NAME	имя, принятое от клиента
0x02	L2F_OPEN_CHAL	запрос клиента получен
0x03	L2F_OPEN_RESP	отклик от клиента
0x04	L2F_ACK_LCP1	от клиента принято сообщение LCP CONFACK
0x05	L2F_ACK_LCP2	клиенту передано сообщение LCP CONFACK
0x06	L2F_OPEN_TYPE	тип используемой аутентификации
0x07	L2F_OPEN_ID	идентификатор, связанный с аутентификацией
0x08	L2F_REQ_LCP0	первое сообщение LCP CONFREQ от клиента
0x03	L2F_CLOSE	запрос разрыва соединения
0x01	L2F_CLOSE_WHY	код причины разрыва соединение
0x02	L2F_CLOSE_STR	описание причины в виде строки ASCII
0x04	L2F_ECHO	проверка присутствия партнера
0x05	L2F_ECHO_RESP	отклик на L2F_ECHO

L2TP

RFC 2661 http://www.cis.ohio-state.edu/htbin/rfc/rfc2661.html

Протокол L2TP используется для интеграции мультипротокольного сервиса по коммутируемым линиям в существующие точки доступа (Point of Presence - POP) сервис-провайдеров Internet. Этот протокол можно использовать и для решения проблемы расщепления групп "multilink hunt-group". Протокол Multilink PPP, часто используемый для объединения каналов ISDN BRI, требует, чтобы все каналы мультиканального потока попадали на один сервер доступа NAS. Поскольку протокол L2TP ведет к появлению сеанса PPP в месте, отличающемся от физической точки завершения канала, этот протокол можно использовать для представления всех каналов на одном сервере NAS, даже в тех случаях, когда физические каналы организуются через различные NAS-серверы.

Формат пакетов L2TP показан на рисунке.



Формат пакетов L2TP

T

Флаг T имеет значение для управляющих сообщений и 0 - для информационных (payload). В управляющих сообщениях следующие за этим флагом 7 битов имеют значения 1001000, используемые для обеспечения совместимости по кодированию с информационными сообщениями.

L

Флаг L устанавливается для пакетов, содержащих поле размера, показывающее общую длину принятого пакета. Этот флаг должен устанавливаться для управляющих сообщений.

I и C

Поля I и C зарезервированы и должны иметь нулевые значения. Поля использовались для опций, более не поддерживаемых протоколом L2TP.

F

Флаг F устанавливается для пакетов, в которых присутствуют поля Ns и Nr. Данный флаг должен устанавливаться для управляющих сообщений.

K

Поле K зарезервировано и должно иметь нулевое значение.

O

Этот флаг говорит о присутствии поля Размер смещения (Offset Size) в информационных сообщениях.

Версия

Это трехбитовое поле указывает номер версии протокола L2TP и для версии 1 должно иметь значение 2.

Размер

Общий размер сообщения с учетом заголовка, AVP типа сообщения и всех дополнительных AVP, связанных с данным типом управляющих сообщений.

Идентификатор туннеля

Указывает туннель, к которому относится управляющее сообщение. Если от партнера еще не получено сообщение Assigned Tunnel ID (присвоенный идентификатор туннеля), это поле должно иметь нулевое значение. После получения от партнера идентификатора туннеля во все пакеты должно помещаться это значение.

Идентификатор вызова

Указывает на пользовательскую сессию в туннеле, к которой имеет отношение данное управляющее сообщение. Если сообщение не связано с отдельной сессией в туннеле (например, сообщение Stop-Control-Connection-Notification), это поле должно иметь нулевое значение.

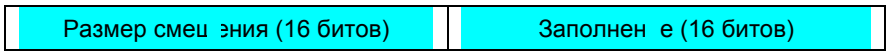
Ns

Передаваемый в настоящее время пакет.

Nr

Последний принятый пакет.

Информационные сообщения L2TP используют два дополнительных поля перед полем AVP. Эти поля показаны на рисунке.



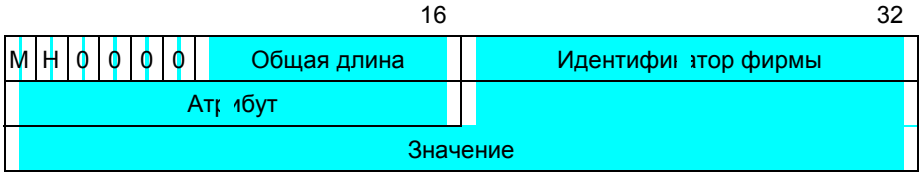
Дополнительные поля информационных сообщений L2TP

Размер смещения

Это поле указывает число байтов от конца заголовка L2TP до начала информационной части сообщения (payload). Если размер смещения равен 0 или флаг O не установлен, информационная часть сообщения начинается сразу после заголовка L2TP.

AVP

Пары AVP (Attribute-Value Pair - атрибут-значение) используются для кодирования типа сообщений L2TP. Формат поля AVP показан на рисунке.



Структура поля AVP

M

Первые 6 битов образуют битовую маску, которая описывает общие атрибуты AVP. Обязательный бит M используется для контроля за обработкой нераспознанных AVP.

H

Этот флаг служит для управления спрятанными (hidden) данными в поле значения AVP. Сокрытие данных можно использовать для передачи конфиденциальной информации (например, паролей) в AVP.

Общая длина

Число октетов (с учетом самого поля длины), содержащихся в AVP. Поле длины занимает 10 битов, позволяя передавать AVP размером до 1024 октетов.

Идентификатор фирмы

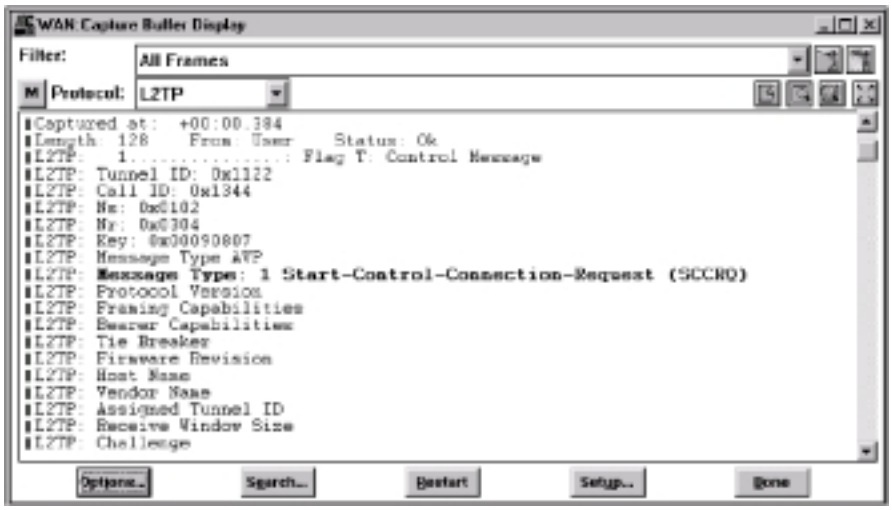
Выделенные IANA идентификаторы SMI Network Management Private Enterprise Code.

Атрибут

16-битовое значение атрибута, значение которого определяется с учетом идентификатора фирмы-производителя.

Значение

Поле значения размещается сразу же после атрибута и занимает оставшиеся октеты пакета (общий размер пакета за вычетом шести октетов заголовка).



Пример декодирования L2TP

PPTP

RFC2637 http://www.cis.ohio-state.edu/htbin/rfc/rfc2637.html

Протокол PPTP (Point to Point Tunneling Protocol) позволяет передавать пакеты PPP через сети IP. Протокол использует архитектуру клиент-сервер для разделения функций, существующих в современных серверах сетевого доступа NAS и поддержки виртуальных частных сетей VPN (Virtual Private Network). PPTP включает спецификации протоколов контроля вызовов и управления, позволяющих серверу контролировать доступ по коммутируемым каналам телефонных сетей ТсОП и ISDN или организовывать исходящие коммутируемые соединения. Протокол PPTP использует GRE-подобный (Generic Routing Encapsulation) механизм для управления сервисом инкапсуляции дейтаграмм по потокам и насыщению при передаче пакетов PPP.

Формат заголовков PPTP показан на рисунке.

Формат заголовков PPTP

Размер

Общая длина сообщения PPTP (с учетом заголовка) в октетах.

Тип сообщения PPTP

Один из двух идентификаторов типа сообщения:

1 контроль
2 управление

Магическое число

Это поле всегда содержит значение 0x1A2B3C4D, служащее для того, чтобы приемник мог корректно синхронизироваться с потоком данных TCP.

Тип сообщений контроля

1 Start-Control-Connection-Request
2 Start-Control-Connection-Reply
3 Stop-Control-Connection-Request
4 Stop-Control-Connection-Reply
5 Echo-Request

6 Echo-Reply

Управление вызовами

7 Outgoing-Call-Request
8 Outgoing-Call-Reply
9 Incoming-Call-Request
10 Incoming-Call-Reply
11 Incoming-Call-Connected
12 Call-Clear-Request
13 Call-Disconnect-Notify

Отчеты об ошибках

14 WAN-Error-Notify

Управление сеансами PPP

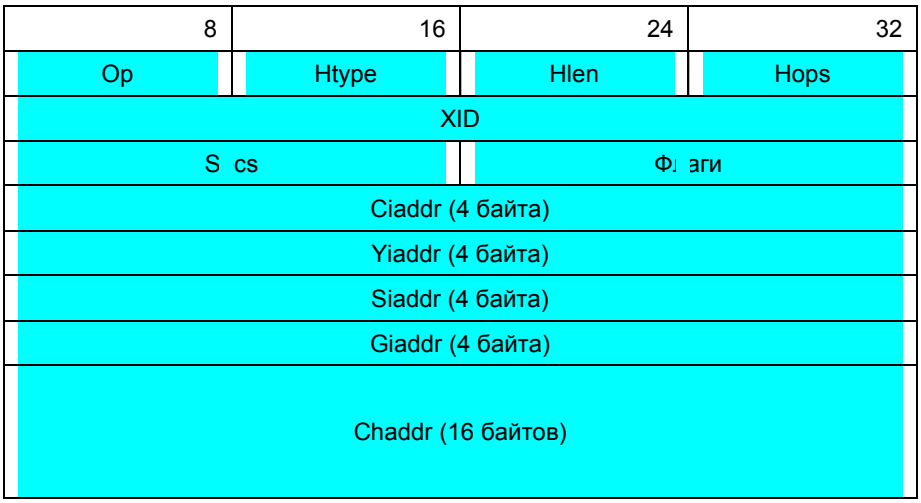
15 Set-Link-Info

DHCP

RFC1531 http://www.cis.ohio-state.edu/htbin/rfc/rfc1531.html

Протокол DHCP (Dynamic Host Configuration Protocol - протокол динамической настройки хостов) обеспечивает конфигурационные параметры для хостов Internet. DHCP представляет собой расширение протокла BOOTP и состоит из двух компонент - протокол доставки параметров хоста от сервера DHCP и механизм предоставления сетевых адресов хостам.

Формат заголовка DHCP показан на рисунке.



Формат заголовка DHCP

Op

Код операции, связанной с сообщением - BOOTREQUEST (запрос) или BOOTREPLY (отклик).

Htype

Тип аппаратного адреса.

Hlen

Размер аппаратного адреса.

Hops

Клиент устанавливает для этого поля нулевое значение. Поле может использоваться relay-агентами при загрузке с использованием таких агентов.

XID

Идентификатор транзакции.

Secs

Число секунд, прошедших с того момента, как клиент инициировал процесс получения адреса или процесс обновления.

Флаги

2 байта флагов DHCP.

Ciaddr

IP-адрес клиента.

Yiaddr

Ваш (клиента) IP-адрес.

Siaddr

IP-адрес следующего сервера, который можно использовать для загрузки.

Giaddr

IP-адрес, используемый для загрузки с помощью relay-агента.

Chaddr

Аппаратный адрес клиента.

DHCPv6

http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-14.txt

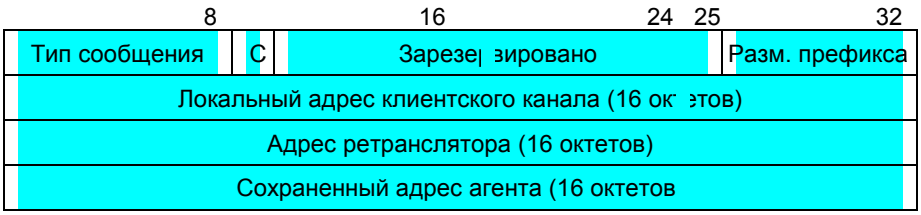
Протокол динамической настройки хостов версии 6 (DHCPv6) позволяет серверам DHCP передавать информацию узлам IPv6 с использованием расширений. Протокол обеспечивает возможность автоматического распределения сетевых адресов и предоставляет дополнительную гибкость настройки по сравнению со своими предшественниками. Протокол DHCPv6 является важной частью протокола SAA (Stateless Address Autoconfiguration) и может использоваться совместно с ним или отдельно для получения конфигурационной информации.

DHCPv6 поддерживает 6 различных типов сообщений - Solicit, Advertise, Request, Reply, Release и Reconfigure.

Сообщения DHCP Solicit

Клиенты передают сообщения DHCP Solicit через настраиваемый интерфейс для получения адреса одного или нескольких конфигурационных серверов. Значения полей устанавливаются клиентом, если явно не указано иное.

Формат сообщений DHCP Solicit показан на рисунке.



Формат сообщений DHCP Solicit

Тип сообщения

Значение 1 в этом поле говорит о сообщении DHCP Solicit.

C

Этот флаг показывает, что клиент запрашивает у всех серверов, получивших сообщение, освободить (deallocate) связанные с клиентом ресурсы. При установке этого флага клиент должен обеспечить сохраненный адрес агента для поиска клиентский связей сервером.

Зарезервировано

Зарезервированное поле, которое должно иметь нулевое значение.

Размер префикса

Отличное от нуля значение префикса указывает число битов в левой части адреса IPv6 агента, которые служат префиксом маршрутизации. Поле размера префикса устанавливается ретранслятором DHCP (DHCP relay) при получении запроса и его пересылке одному или нескольким серверам DHCP.

Локальный адрес клиентского канала

Локальный адрес канала IP клиентского интерфейса, с которого клиент передал запрос DHCP Request.

Адрес ретранслятора

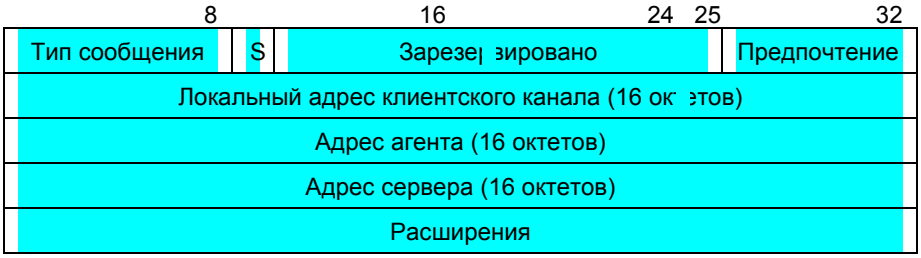
Клиент устанавливает для этого поля нулевое значение. При получении пакета ретранслятор (relay) DHCP устанавливает в этом поле значение IP-адреса интерфейса, через который получен клиентский запрос DHCP Solicit.

Сохраненный адрес агента

Это поле, будучи установленным, показывает IP-адрес агентского интерфейса, который был сохранен клиентом от предыдущей транзакции DHCP.

Сообщения DHCP Advertise

Агент DHCP посылает сообщения DHCP Advertise для того, чтобы информировать потенциальных клиентов об IP-адресе сервера, которому можно посылать запросы DHCP Request. Когда клиент и сервер находятся на различных каналах (link), сервер посылает анонсы обратно через ретранслятор, который переслал запрос. Значения всех полей сообщения DHCP Advertise заполняются сервером DHCP и не изменяются при ретрансляции.



Формат сообщений DHCP Advertise

Тип сообщения

Значение 2 в этом поле говорит о сообщении DHCP Advertise.

S

Этот флаг говорит о присутствии адреса сервера.

Предпочтение

Показывает готовность сервера к обслуживанию клиентов.

Локальный адрес клиентского канала

Локальный адрес канала IP клиентского интерфейса, с которого клиент передал запрос DHCP Request.

Адрес агента

IP-адрес агентского интерфейса DHCP, находящегося на одном канале с клиентом.

Адрес сервера

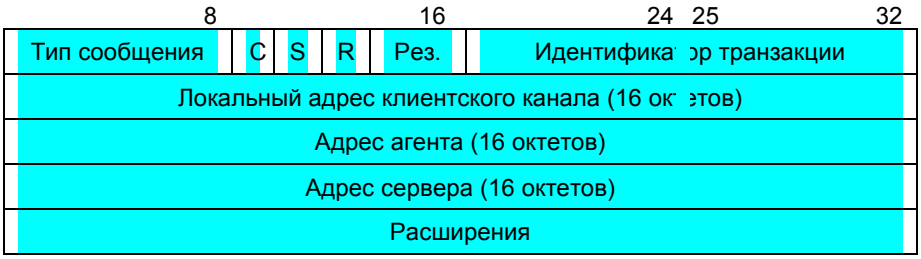
Это поле, будучи установленным, показывает IP-адрес сервера DHCP.

Расширения

Это поле находится в стадии разработки. См. C. Perkins. Extensions for the Dynamic Host Configuration Protocol for IPv6 http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6ext-11.txt.

Сообщения DHCP Request

Для получения конфигурационных параметров от сервера клиент посылает сообщение DHCP Request, к которому могут быть добавлены произвольные расширения. Если клиенту неизвестен адрес хотя бы одного сервера, он должен сначала выяснить такой адрес, передав для этого запрос DHCP Solicit с групповым адресом. Обычно при перезагрузке клиента последний не имеет корректного адреса IP, требуемого для взаимодействия между сервером и клиентом. В таких случаях клиент не может передать сообщение напрямую серверу, поскольку сервер не может вернуть клиенту ответ, не зная адреса клиента. В таких случаях клиент должен послать запрос локальному ретранслятору, указав адрес ретранслятора в заголовке сообщения как адрес агента.



Формат сообщений DHCP Request

Тип сообщения

Значение 3 в этом поле говорит о сообщении DHCP Request.

R

Этот флаг говорит о перезагрузке клиента и запросе удаления всех идентификаторов предыдущих транзакций.

Идентификатор транзакции

Беззнаковое целое число, служащее для обозначения запроса.

Остальные поля были описаны выше при рассмотрении сообщений DHCP Solicit и DHCP Advertise.

Сообщения DHCP Reply

Сервер посылает сообщения DHCP Reply в ответ на каждый запрос DHCP Request и DHCP Release. Если запрос получен с флагом S, это говорит о том, что клиент не может передавать запросы серверу напрямую и использует расположенный по соседству ретранслятор. В таких случаях сервер передает сообщения DHCP Reply с установленным битом L, адресуя их агенту, указанному в запросе. Все поля сообщений DHCP Reply устанавливает сервер DHCP.

Формат сообщений DHCP Reply

Тип сообщения

Значение 4 в этом поле говорит о сообщении DHCP Reply.

L

Установка этого флага говорит о присутствии в сообщении локального адреса клиентского канала.

Состояние

0	Успешное выполнение запроса
16	Отказ, причина не указана
17	Отказ при аутентификации
18	Некорректно сформированный запрос Request или Release
19	Ресурсы недоступны
20	Клиентская запись недоступна

21 Некорректный IP-адрес клиента в запросе Release

23 Ретранслятор не может найти адрес сервера

64 Сервер недоступен (ошибка ICMP)

Идентификатор транзакции

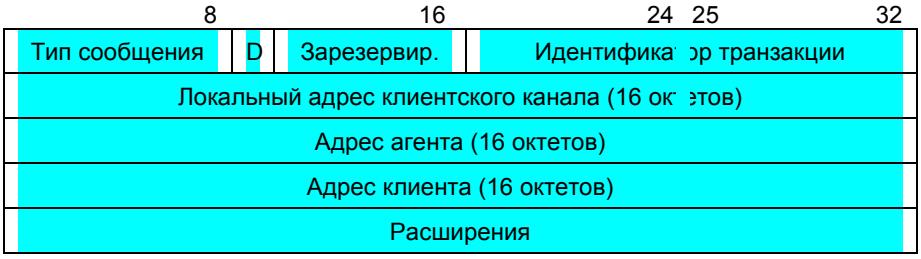
Беззнаковое целое число, служащее для обозначения отклика. Значение этого поля копируется из одноименного поля пакета Request.

Локальный адрес клиентского канала

Если это поле используется, оно содержит локальный адрес канала IP клиентского интерфейса, с которого клиент передал запрос DHCP Request. При установленном флаге L локальный адрес клиентского канала присутствует в пакете Reply. Тогда сообщение Reply посылается сервером по адресу ретранслятора, который использует локальный адрес клиентского канала для доставки сообщения клиенту. Поле идентификатора транзакции сообщений DHCP Reply копируется сервером из клиентского запроса DHCP Request.

Сообщения DHCP Release

Сообщения DHCP Release передаются без использования ретрансляторов DHCP. Когда клиент посылает сообщение Release, предполагается, что этот клиент имеет корректный IP-адрес, позволяющий передать сообщение серверу. Если в поле расширения указаны параметры, освобождаются только эти параметры. Значения всех полей сообщений DHCP Release задаются клиентом. Сервер DHCP подтверждает сообщения DHCP Release путем передачи DHCP Reply.



Формат сообщений DHCP Release

Тип сообщения

Значение 5 в этом поле говорит о сообщении DHCP Release.

D

Установка этого флага говорит серверу о том, что отклик DHCP Reply следует передавать непосредственно клиенту вместо использования адресов агента и локального адреса канала для ретрансляции сообщения Reply.

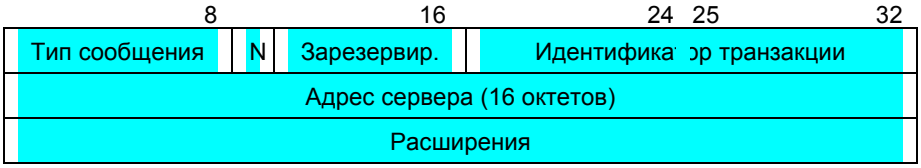
Идентификатор транзакции

Беззнаковое целое число, служащее для обозначения запроса DHCP Release. Значение этого поля копируется в одноименное поле пакета Reply.

Остальные поля сообщений описаны выше.

Сообщения DHCP Reconfigure

Сообщения DHCP Reconfigure могут посылаться только клиентам, имеющим IP-адрес, который маршрутизируется в канал, обеспечивающий доступ к клиенту. Следовательно, сообщения DHCP Reconfigure передаются без использования ретрансляторов DHCP. Когда сервер посылает сообщение DHCP Reconfigure, он предполагает, что получатель имеет корректный адрес IP в доступной для сервера области. В ответ на сообщение DHCP Reconfigure клиент должен снова запросить те (и только те) параметры, которые указаны в поле расширения. Сервер может передавать сообщения DHCP Reconfigure, используя индивидуальные или групповые адреса получателей. Получив сообщение, клиент должен разобрать поле расширения и послать серверу запрос для получения значений указанных в расширении параметров.



Формат сообщений DHCP Reconfigure

Тип сообщения

Значение 6 в этом поле говорит о сообщении DHCP Reconfigure.

N

Установка этого флага говорит о том, что клиент не должен ожидать сообщения DHCP Reply в ответ на запрос DHCP Request, переданный в результате получения пакета DHCP Reconfigure.

Остальные поля сообщений описаны выше.

DVMRP

RFC 1075 http://www.cis.ohio-state.edu/htbin/rfc/rfc1075.html

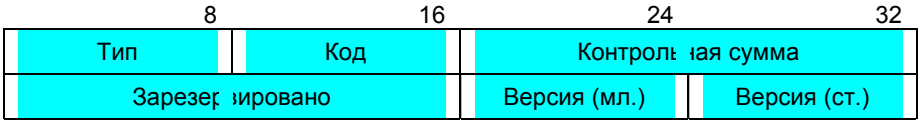
IETF draft: http://www.ietf.org/internet-drafts/draft-ietf-idmr-dvmrp-v3-08.txt

Протокол DVMRP (Distance Vector Multicast Routing Protocol) представляет собой протокол маршрутизации Internet, обеспечивающий эффективный механизм доставки дейтаграмм группам хостов в интерсети без организации соединений (connectionless). Это распределенный протокол, который динамически генерирует деревья групповой доставки пакетов IP на основе метода RPM (Reverse Path Multicasting).

Протокол DVMRP поддерживает многие функции RIP с алгоритмом TRBP (Truncated Reverse Path Broadcasting). DVMRP разработан на основе протокола RIP, поскольку эта реализация была доступна и алгоритм дистантных векторов достаточно прост, по сравнению с алгоритмами на основе состояния каналов. В дополнение к этому был разработан механизм *туннелирования* для проведения экспериментов по передаче пакетов через сети, не поддерживающие групповой адресации.

Между протоколами RIP и DVMRP есть важное различие - RIP маршрутизирует и рассылает дейтаграммы конкретным адресатам, а DVMRP может работать с групповыми адресами. Одной из задач протокола является сохранение информации о пути возврата к отправителю дейтаграмм с групповой адресацией. Чтобы сделать описание протокола DVMRP более близким к описанию RIP используется термин *получатель* (destination) взамен более корректного термина *отправитель* (source), однако дейтаграммы не рассылаются *получателям*, а происходят от них.

Пакеты DVMRP инкапсулируются в дейтаграммы IP с полем протокола, имеющим значение 2 (IGMP). Пакеты DVMRP используют общий заголовок протокола, который указывает тип пакетов IGMP как DVMRP. При передаче пакетов DVMRP флаги преимущественной доставки (Precedence) в поле типа сервиса должны указывать на межсетевое управлений (Internetwork Control - 0xC0). Общий заголовок протокола показан на рисунке.



Структура DVMRP

Тип

Тип пакета. Значение 0x13 говорит о пакете DVMRP.

Код

Определяет тип пакета DVMRP. В настоящее время поддерживаются коды для протокола DVMRP, а также для протоколов анализа и поиска неисправностей.

Probe	поиск соседа
Report	обмен маршрутами
Prune	уничтожение деревьев групповой доставки
Graft	создание деревьев групповой доставки
Graft ack	подтверждение сообщение о создании деревьев.

Контрольная сумма

Контрольная сумма пакета DVMRP, рассчитываемая до передачи пакета и проверяемая при его получении. При расчете контрольной суммы это поле принимается равным нулю.

Зарезервировано

Зарезервировано для использования в будущем.

Младшие цифры версии

Младшие цифры номера версии протокола DVMRP - для текущей версии - 0xFF.

Старшие цифры версии

Старшие цифры номера версии протокола DVMRP - для текущей версии - 3.

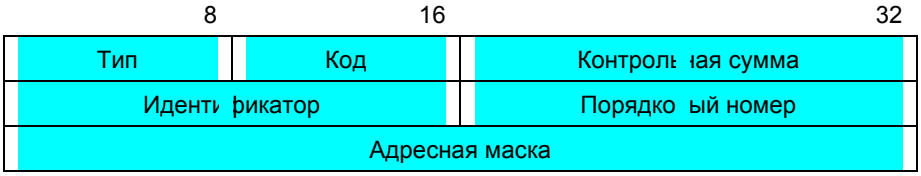
ICMP

RFC792 http://www.cis.ohio-state.edu/htbin/rfc/rfc792.html

RFC1970 http://www.cis.ohio-state.edu/htbin/rfc/rfc1970.html

Протокол ICMP (Internet Control Message Protocol - протокол управляющих сообщений Internet) в общем случае используется для передачи сведений о трудностях маршрутизации дейтаграмм IP или простого обмена временными метками и эхо-транзакциями (ping).

Структура заголовка пакетов ICMP показана на рисунке.



Структура заголовка ICMP

Тип и код

Тип	*Код*	*Описание*
0		эхо-отклик
	0	нет кода
1		не используется
2		не используется
3		адресат недоступен
3	0	нет доступа
3	1	хост недоступен
	2	протокол недоступен
	3	порт недоступен
	4	требуется фрагментация, но установлен флаг DF (не фрагментировать)
	5	отказ при маршрутизации Source route
	6	неизвестна сеть адресата
	7	неизвестен хост-адресат
	8	хост-отправитель изолирован
	9	связь с сетью адресата запрещена административными мерами
	10	связь с хостом-адресатом запрещена административными мерами
	11	сеть адресата недоступна для заданного типа обслуживания (TOS)
	12	хост-адресат недоступен для заданного типа обслуживания (TOS)
4		Source quench
4	0	нет кода

5		перенаправление
5	0	перенаправление дейтаграмм для сети или подсети
5	1	перенаправление дейтаграмм для хоста
5	2	перенаправление дейтаграмм для указанного типа сервиса (TOS) и сети
5	3	перенаправление дейтаграмм для указанного типа сервиса (TOS) и хоста
6		альтернативный адрес хоста
6	0	альтернативный адрес для хоста
7		не используется
8		эхо
8	0	нет кода
9		анонсирование маршрутизатора (RFC-1256)
9	0	нет кода
10		выбор маршрутизатора (RFC-1256)
10	0	нет кода
11		время истекло
11	0	время жизни (TTL) истекло во время передачи
11	1	истекло время сборки фрагментов
12		проблемы с параметрами
12	0	указатель говорит об ошибке
12	1	отсутствует требуемая опция
12	2	некорректная длина
13		временная метка
13	0	нет кода
14		ответ на временную метку
14	0	нет кода
15		запрос информации
15	0	нет кода
16		отклик на запрос информации
16	0	нет кода
17		запрос маски адреса (RFC-950)
17	0	нет кода
18		отклик на запрос маски (RFC-950)
18	0	нет кода
19		зарезервирован (обеспечение безопасности)
20-29		зарезервированы (для экспериментов на устойчивость к ошибкам)
30		трассировка маршрута (traceroute) – RFC-1393
31		ошибка преобразования дейтаграммы (RFC-1475)
32		перенаправление для мобильного хоста
33		IPv6 Where-Are-You (где вы находитесь)
34		IPv6 I-Am-Here (я здесь)
35		запрос перенаправления для мобильного хоста
36		отклик на запрос перенаправления для мобильного хоста

Контрольная сумма

Контрольная сумма пакета ICMP, рассчитанная начиная с поля типа ICMP. При расчете контрольной суммы значение поля контрольной суммы предполагается равным нулю.

Идентификатор

Идентификатор используется для обозначения соответствия запросов и откликов. Это поле должно иметь нулевое значение.

Порядковый номер

Порядковый номер используется для обозначения соответствия запросов и откликов. Это поле должно иметь нулевое значение.

Адресная маска

32-битовая маска.

ICMPv6

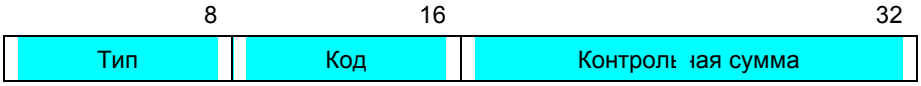
RFC1885 http://www.cis.ohio-state.edu/htbin/rfc/rfc1885.html

RFC1970 http://www.cis.ohio-state.edu/htbin/rfc/rfc1970.html

При подготовке протокола IPv6 был пересмотрен протокол управляющих сообщений ICMP и в новый вариант протокола ICMPv6 были добавлены функции управления групповой рассылкой IGMP (IPv4 Group Membership

Protocol).

Структура заголовков ICMPv6 показана на рисунке.



Структура заголовка ICMPv6

Тип

Сообщения ICMPv6 могут быть различных типов - сообщения об ошибках и информационные сообщения. К числу сообщений об ошибках относятся сообщения о недостижимости адресата (Destination unreachable), слишком больших пакетах (Packet too big), истечении времени (Time exceed) и проблемах с параметрами (Parameter problem). В число информационных сообщений входят Echo Request (эхо-запрос), Echo Reply (эхо-отклик), Group Membership Query (запрос на включение в группу), Group Membership Report (отчет о включении в группу), Group Membership Reduction (исключение из группы).

Код

Для каждого типа сообщений определено несколько значений кодов. Примером может служить сообщение Destination Unreachable, для которого определены коды отсутствия маршрута к адресату, административного запрета связи с адресатом, not a neighbor (не является соседом), недостижимости адреса и порта.

Дополнительную информацию о кодах вы сможете найти в тексте стандарта.

Контрольная сумма

Это поле служит для обнаружения ошибок при передаче пакетов ICMPv6.

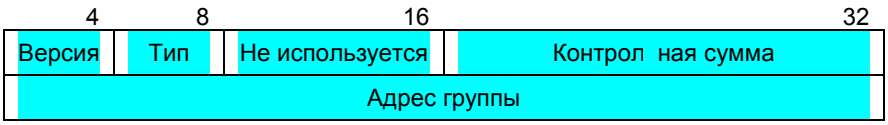
IGMP

RFC1112 http://www.cis.ohio-state.edu/htbin/rfc/rfc1112.html

Протокол IGMP (Internet Group Management Protocol - протокол управления группами Internet) используется хостами IP для передачи информации об их принадлежности к группам любым маршрутизаторам из числа ближайших соседей.

Протокол IGMP интегрирован в стек IP и должен быть реализован на всех хостах, соответствующих спецификации групповой адресации IP для канального уровня. Сообщения IGMP инкапсулируются в дейтаграммы IP с полем протокола, имеющим значение 2. (в соответствии с IETF RFC1112, август 1989).

Формат пакетов IGMP показан на рисунке.



Формат пакетов IGMP

Версия

Номер версии протокола.

Тип

Тип сообщения:

1 Host Membership Query (запрос включения в группу).

2 Host Membership Report (сообщение о принадлежности к группе).

Контрольная сумма

Контрольная сумма пакета.

Адрес группы

В сообщениях Host Membership Report это поле содержит IP для группы.

MARS

RFC2022 http://www.cis.ohio-state.edu/htbin/rfc/rfc2022.html

Групповая рассылка (Multicasting) представляет собой процесс, при котором отправитель (хост или протокол) посылает пакет одновременно группе получателей, используя одну локальную операцию передачи. Технология

ATM используется как новая технология канального уровня для поддержки множества протоколов, включая IP. Протокол MARS имеет два основных назначения - регистрация принадлежности к группам и распространение этой информации. Такие возможности позволяют сетям на базе UNI 3.0/3.1 поддерживать групповой сервис для протоколов типа IP и определять специфическое поведение оконечных точек для поддержки виртуальных каналов "один со многими", используемых при групповой рассылке пакетов сетевого уровня. Сервер MARS (Multicast Address Resolution Server) является, по сути, расширением сервера ATM ARP (сервер преобразования адресов). Этот сервер регистрирует идентификаторы multicast-групп сетевого уровня, связывая их с интерфейсами ATM, представляющими членов группы. Сообщения MARS используются для распространения информации о принадлежности к группам между сервером MARS и оконечными точками (хосты и маршрутизаторы). Объекты системы преобразования адресов оконечных точек запрашивают сервис MARS при возникновении необходимости преобразования адресов сетевого уровня в адреса оконечных точек ATM, входящих в группу. Оконечные точки обеспечивают MARS актуальной информацией, когда им требуется вступление в группу сетевого уровня или выход из такой группы. Для обеспечения своевременной информации об изменениях в группах сервер MARS поддерживает виртуальные каналы со всеми оконечными точками, требующими поддержки групповой рассылки. Каждый сервер MARS обслуживает кластер оконечных точек ATM.

Формат заголовков MARS показан на рисунке.

Семейство адресов	1-2
Идентификация протокола	3-9
Зарезервировано	10-12
Контрольная сумма	13-14
Смещение расширения	15-16
Код операции	17-18
Тип и размер ATM-номера отпра ителя	19
Тип и размер ATM-субрадреса отп авителя	20

Структура заголовка MARS

Семейство адресов

Определяет тип передаваемых адресов канального уровня.

Идентификация протокола

Идентификатор протокола состоит из двух субполей - тип протокола (16 битов) и необязательное расширение SNAP (40 битов)

Зарезервировано

Это поле зарезервировано и может использоваться по частям другими протоколами управления, указанными номером версии.

Контрольная сумма

Стандартная контрольная сумма IP, рассчитанная для всего пакета.

Смещение расширения

Это поле указывает на существование и расположение дополнительного списка параметров.

Код операции

Код операции состоит из двух субполей - версия и тип. Версия показывает выполняемую операцию в контексте версии протокола управления, указанного mar$op.version.

Тип и размер ATM-номера отправителя

Информация об аппаратном адресе отправителя.

Тип и размер ATM-субрадреса отправителя

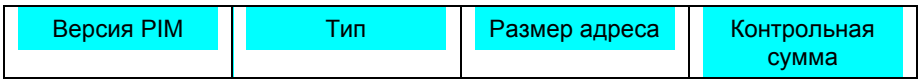
Информация об аппаратном субадресе отправителя.

PIM

RFC 2117 *http://www.cis.ohio-state.edu/htbin/rfc/rfc2117.html*

Протокол PIM-SM (Protocol Independent Multicast - Sparse Mode) служит для эффективной маршрутизации Multicast-групп, которые могут быть распределены по разным местам интерсети (в разных доменах). Этот протокол не связан с каким-либо из протоколов маршрутизации и разработан для поддержки разбросанных (sparse) групп.

Формат пакетов PIM показан на рисунке.



Формат пакетов PIM

Версия PIM

Номер версии протокола (текущее значение - 2).

Тип

Тип сообщения PIM.

Размер адреса

Размер адреса в байтах.

Контрольная сумма

Контрольная сумма всего сообщения PIM. При расчете контрольной суммы значение этого поля принимается нулевым.

RIP

RFC1058 http://www.cis.ohio-state.edu/htbin/rfc/rfc1058.html

RFC1528 http://www.cis.ohio-state.edu/htbin/rfc/rfc1528.html

RFC1723 http://www.cis.ohio-state.edu/htbin/rfc/rfc1723.html

Протокол RIP (Routing Information Protocol) используется операционной системой Berkeley 4BSD UNIX для обмена маршрутной информацией. Реализованный как программа UNIX, протокол RIP2 базируется на своем одноименном предшественнике, разработанном компанией Xerox.

RIP2 является расширением протокола RIP, обеспечивающим передачу дополнительной маршрутной информации в сообщениях RIP и повышающим уровень безопасности.

Протокол RIP2 основан на передача дейтаграмм UDP. Каждый хост, использующий RIP2 имеет процесс маршрутизации, принимающий и передающий дейтаграммы UDP через порт 520. Формат пакетов RIP показан на рисунке.

Формат пакетов RIP

Часть дейтаграммы (от адреса до метрики, включительно) может повторяться до 25 раз.

Команда

Поле команды показывает назначение дейтаграммы:

1. Request - запрос на передачу всей таблицы маршрутизации или ее части.
2. Response - сообщение, содержащее полную таблицу маршрутизации или ее часть. Эти сообщения могут передаваться в ответ на запрос или сканирование, а при отсутствии изменений в таблице маршрутизации отправитель может генерировать такие сообщения по своей инициативе.
3. Traceon - (устаревшая команда) такие сообщения игнорируются.

4 Traceoff - (устаревшая команда) такие сообщения игнорируются.

5 Reserved - зарезервированное поле, используемое компанией Sun Microsystems для своих целей.

Версия

Номер версии протокола RIP. Обработка дейтаграмм зависит от указанного номера версии:

0 дейтаграммы с нулевым номером версии игнорируются.

1 дейтаграммы протокола версии 1. Проверяются все поля, которые должны иметь нулевые значения. При обнаружении в таком поле отличного от нуля значения дейтаграмма игнорируется.

2 указывает сообщения RIP, использующие аутентификацию, или содержащие информацию в недавно определенных полях.

>2 дейтаграммы протокола версии выше 1. Игнорируются все поля с нулевыми значениями.

Идентификатор семейства адресов

Показывает тип адреса, указанного в данной записи. Это поле требуется потому, что протокол RIP2 может передавать информацию для различных протоколов. Идентификатор семейства адресов IP равен 2.

При использовании аутентификации это поле имеет значение 0xFFFF, а поле тега маршрута указывает тип аутентификации и пароль.

Тег маршрута

Это поле используется только для RIP2 и в сообщениях RIP должно иметь нулевое значение.

Атрибут, присвоенный маршруту. Этот атрибут должен сохраняться и использоваться при повторном анонсировании маршрута. Тег маршрута обеспечивает метод разделения внутренних (сетей внутри домена маршрутизации RIP) и внешних маршрутов RIP, которые могут импортироваться из EGP или других IGP.

IP-адрес

IP-адрес получателя.

Маска подсети

Это поле используется только для RIP2 и в сообщениях RIP должно иметь нулевое значение.

Сетевая часть адреса (байты, задающие номера хостов, имеют нулевые значение, остальные байты - 1). Нулевое значение маски говорит о ее отсутствии.

Следующий маршрутизатор

Это поле используется только для RIP2 и в сообщениях RIP должно иметь нулевое значение.

IP-адрес следующего устройства (маршрутизатора), которому передаются пакеты, предназначенные для данного маршрута.

Метрика

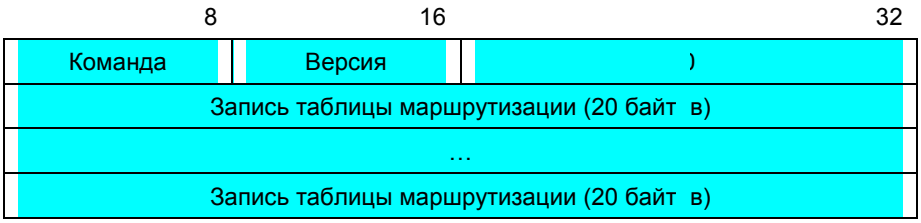
Определяет общую "стоимость" маршрута к получателю. Метрика представляет собой сумму стоимостей, связанных с сетями, через которые передается информация.

RIPng для IPv6

RFC 2080 1997-01 http://www.cis.ohio-state.edu/htbin/rfc/rfc2080.html

RIPng for IPv6 представляет собой протокол маршрутизации для версии IPv6, являющейся расширением протокола IPv4.

Формат заголовков RIPng для IPv6 показан на рисунке.



Формат заголовков RIPng

Команда

Поле команды говорит о назначении сообщения. Поддерживаются два варианта команд:

Request	запрос таблицы маршрутизации или ее части.
Response	отклик - сообщение, содержащее таблицу маршрутизации или ее часть.

Версия

Номер версии протокола (текущее значение - 1).

Запись таблицы маршрутизации

Каждая запись таблицы маршрутизации содержит префикс получателя, число значимых битов префикса и стоимость пути к получателю.

RSVP

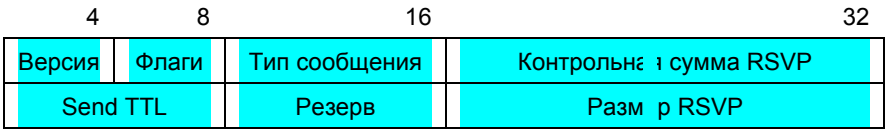
RFC 2205 http://www.cis.ohio-state.edu/htbin/rfc/rfc2205.html

RFC 2208 http://www.cis.ohio-state.edu/htbin/rfc/rfc2208.html

RFC 2209 http://www.cis.ohio-state.edu/htbin/rfc/rfc2209.html

RSVP является протоколом резервирования ресурсов (Resource ReSerVation setup Protocol) предназначенным для интегрированного сервиса Internet. Протокол используется хостами для поддержки потоков данных от приложений, требующих заданного качества обслуживания от сети для отдельных потоков данных. Протокол также используется маршрутизаторами для доставки управляющих запросов QoS всем узлам.

Формат заголовков RSVP показан на рисунке.



Формат заголовков RSVP

Версия

Номер версии протокола (текущее значение - 1).

Флаги

Поле флагов в настоящее время не используется.

Тип сообщения

Поддерживаются следующие типы сообщений:

1 Path.
2 Resv.
3 PathErr.
4 ResvErr.
5 PathTear.
6 ResvTear.
7 ResvConf.

Контрольная сумма RSVP

Контрольная сумма сообщения.

Send TTL

Значение времени жизни IP, с которым передается пакет.

Размер RSVP

Общая длина сообщения RSVP в байтах с учетом общего заголовка и следующих за ним полей переменной длины.

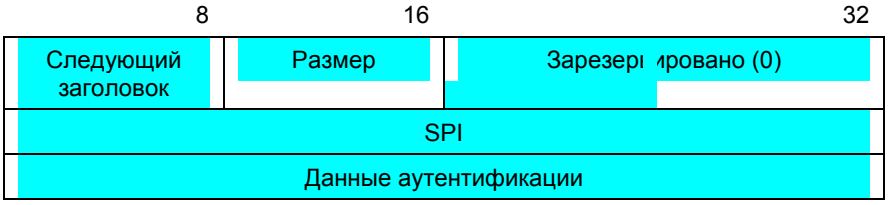
AH

RFC1826 *http://www.cis.ohio-state.edu/htbin/rfc/rfc1826.html*

RFC1827 *http://www.cis.ohio-state.edu/htbin/rfc/rfc1827.html*

Протокол IP AH (Authentication Header - заголовок аутентификации) обеспечивает дополнительный уровень безопасности за счет добавления полей аутентификации в дейтаграммы IP. Параметры аутентификации рассчитываются с использованием всех полей дейтаграммы IP (включая не только заголовок IP, но и заголовки других протоколов, а также пользовательские данные), которые не могут изменяться в процессе доставки. Поля или опции, которые при доставке изменяются (например, счетчик интервалов, время жизни, идентификаторы, смещения фрагмента или указатели маршрутов) при расчете не принимаются во внимание (предполагается, что они имеют нулевые значения). Использование этого метода позволяет существенно повысить уровень безопасности по сравнению с протоколом IPv4 и этого уровня достаточно для большинства пользователей. При использовании с протоколом IPv6 заголовок AH обычно появляется после заголовка IPv6 Hop-by-Hop, но перед опциями получателя IPv6. При использовании с протоколом IPv4 заголовок AH обычно размещается после заголовка IPv4.

Формат заголовка AH показан на рисунке.



Формат заголовка AH

Следующий заголовок

Следующий заголовок после поля данных аутентификации.

Размер

Размер поля данных аутентификации.

SPI

Security Parameters Index - указывает параметры безопасности для дейтаграммы.

Данные аутентификации

Данные аутентификации в виде переменного числа 32-битовых слов.

ESP

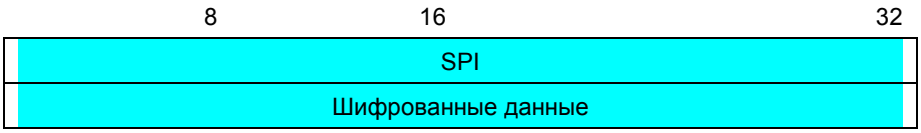
RFC1826 http://www.cis.ohio-state.edu/htbin/rfc/rfc1826.html

RFC1827 http://www.cis.ohio-state.edu/htbin/rfc/rfc2406.html

ESP (IP Encapsulating Security Payload) служит для обеспечения целостности и конфиденциальности данных за счет их шифрования. В зависимости от пользовательских требований к безопасности этот механизм может применяться для шифрования сегментов транспортного уровня (например, TCP, UDP, ICMP, IGMP) или дейтаграмм IP целиком. Чтобы обеспечить конфиденциальность всей исходной дейтаграммы требуется использовать инкапсуляцию.

ESP может содержаться в любом месте между заголовком IP и конечным протоколом транспортного уровня. Для протокола ESP используется идентификатор IANA 50. Заголовок, расположенный непосредственно перед заголовком ESP, всегда будет содержать значение 50 в поле Next Header (следующий заголовок) для IPv6) или Protocol (протокол) для IPv4. ESP состоит из нешифрованного заголовка, за которым следуют зашифрованные данные. Шифруемые данные включают в себя защищенные поля заголовка ESP и защищаемые пользовательские данные, которые представляют собой целую дейтаграмму IP или кадр протокола вышележащего уровня (например, TCP или UDP).

Формат заголовка ESP показан на рисунке.



Формат заголовка ESP

SPI

Security association identifier - 32-битовое псевдослучайное значение, идентифицирующее ассоциации безопасности дейтаграммы. Если ассоциаций не создано, поле SPI содержит значение 0x00000000. Поле SPI подобно параметру SAID, используемому другими протоколами безопасности.

Шифрованные данные

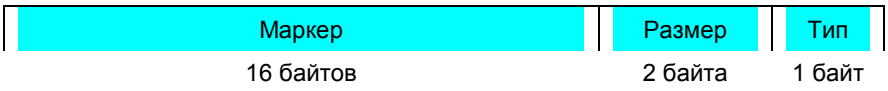
Поле данных переменной длины.

BGP-4

RFC 1654 http://www.cis.ohio-state.edu/htbin/rfc/rfc1654.html

BGP (Border Gateway Protocol - протокол граничного шлюза) представляет собой протокол маршрутизации между автономными системами (inter-Autonomous System). Основной функцией протокола BGP является обмен информацией о доступности сетей с другими системами BGP. Протокол BGP-4 обеспечивает расширенный набор механизмов для поддерживаемых классов междоменной маршрутизации.

Формат заголовка BGP-4 показан на рисунке.



Формат заголовка BGP-4

Маркер

16-байтовое сообщение, содержащее значение, которое предсказано получателем.

Размер

Размер сообщения в байтах с учетом заголовка.

Тип

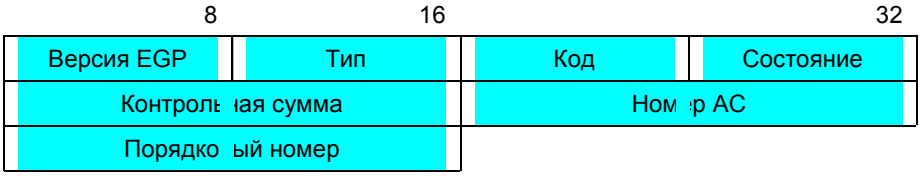
Тип сообщения - Open (открыть), Update (обновить), Notification (уведомление), KeepAlive (поддержать, сохранить).

EGP

RFC 904 http://www.cis.ohio-state.edu/htbin/rfc/rfc904.html

Протокол EGP (Exterior Gateway Protocol - протокол внешнего шлюза) служит для обмена сведениями о доступности сетей между соседними шлюзами (возможно из разных автономных систем). Протокол включает механизм приобретения (acquire) соседей, средства мониторинга доступности соседей и обмена информацией о доступности сетей в форме сообщений Update (обновление). Работа протокола основана на периодическом сканировании (polling) с использованием обмена сообщениями Hello/I-Heard-You (I-H-U) для мониторинга доступности соседей и передаче команд Poll для запроса сообщений Update.

Формат заголовка EGP показан на рисунке.



Формат заголовка EGP

Версия EGP

Номер версии протокола EGP (текущее значение - 2).

Тип

Идентифицирует тип сообщения:

1 Отклик/индикация обновления
2 Команда опроса (Poll)
3 Сообщение о приобретении соседа
5 Сообщение о доступности соседа
8 Отклик/индикация ошибки.

Код

Идентифицирует код сообщения.

Состояние

Информация о состоянии, зависящая от типа сообщения.

Контрольная сумма

Контрольная сумма всех полей сообщения EGP. При расчете контрольной суммы значение этого поля предполагается нулевым.

Номер АС

Номер автономной системы.

Порядковый номер

Переменная состояния передачи (команды) или приема (отклики и индикаторы).

EIGRP

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol - расширенный протокол внутреннего шлюза) представляет собой расширенный вариант протокола IGRP. Протокол IGRP является протоколом внутреннего шлюза компании Cisco, используемым в сетях TCP/IP и OSI. Протокол относится к числу внутренних шлюзов (interior gateway protocol - IGP), но может также использоваться в качестве протокола внешнего шлюза для междоменной маршрутизации. Протокол IGRP использует технологию маршрутизации на основе дистантного вектора. Такая же технология дистантного вектора применяется и для протокола EIGRP с сохранением информации о дистанциях нижележащего уровня. Возможности конвергенции (сближения) и эффективность работы этого протокола существенно повысились по сравнению с IGRP.

Формат заголовков EIGRP показан на рисунке.

Формат заголовка EIGRP

Версия

Номер версии протокола.

Код операции

1 Update (обновление).
2 Reserved (зарезервировано).
3 Query (запрос).
4 Hello (приветствие).
5 IPX-SAP.

Тип

1 Параметры EIGRP.
2 Зарезервировано.
3 Sequence (последовательность).
4 Версия программ.

5 Next Multicast

Размер

Размер кадра.

GRE

RFC 1701: *http://www.cis.ohio-state.edu/htbin/rfc/rfc1701.html*

RFC 1702: *http://www.cis.ohio-state.edu/htbin/rfc/rfc1702.html*

Протокол GRE (Generic Routing Encapsulation) обеспечивает механизм инкапсуляции произвольных пакетов в произвольный транспортный протокол. В наиболее общем случае система имеет пакеты, которые нужно инкапсулировать и маршрутизировать (информационные пакеты). Информация (payload) сначала инкапсулируется в пакет GRE, который может также содержать маршрут. Полученный в результате пакет GRE инкапсулируется в пакет другого протокола (протокол доставки).

Протокол GRE может с IP в качестве протокола доставки или информационного (payload) протокола. Заголовок GRE, используемый протоколом PPTP, незначительно отличается от заголовка, описанного в текущей спецификации протокола GRE.

Формат заголовка показан на рисунке.

Формат заголовка GRE

Флаги

Первые два октета заголовка содержат флаги GRE. Бит 0 является младшим, бит 12 - старшим. Используются следующие флаги:

Контрольная сумма присутствует (бит 0) и содержит корректное значение.

Маршрутизация присутствует (бит 1) - поля смещения и маршрутизации содержат корректные значения.

Ключ присутствует (бит 2) в заголовке GRE.

Порядковый номер присутствует (бит 3).

Strict Source Route (бит 4) - рекомендуется устанавливать этот флаг только поле маршрутной информации содержит только маршруты Strict Source.

Контроль рекурсии (биты 5-7) 3-битовое беззнаковое целое, указывающее допустимое число дополнительных инкапсуляций.

Номер версии (биты 13-15) - 0.

Тип протокола

Тип протокола в поле содержимого (payload) пакета. В общем случае это поле указывает тип протокола Ethernet для данного пакета.

Контрольная сумма

Необязательное поле. Контрольная сумма IP (дополнение до 1) для заголовка GRE и содержимого пакета.

Смещение

Необязательное поле. Показывает смещение в октетах от начала поля маршрутизации до первого октета проверяемой записи Source Route.

Ключ

Необязательное поле. 4-октетное число, которое было вставлено при инкапсуляции. Это значение может использоваться получателем для аутентификации отправителя пакета.

Порядковый номер

Необязательное поле. 32-битовое целое число, вставляемое при инкапсуляции. Это значение может использоваться получателем для поддержки порядка передачи пакетов.

Маршрутизация

Необязательное поле. Содержит данные, которые могут использоваться при маршрутизации данного пакета.

Расширенный заголовок GRE использует показанный на рисунке формат.

Формат расширенного заголовка GRE

Флаги

Поле флагов может принимать следующие значения:

C (бит 0) - контрольная сумма присутствует.

R (бит 1) - маршрутизация присутствует.

K (бит 2) - ключ присутствует.

S (бит 3) - порядковый номер присутствует.

s (бит 4) - присутствует Strict source route.

Recur (биты 5-7) - управление рекурсией.

A (бит 8) - порядковый номер подтверждения присутствует.

Flags (биты 9-12) - 0.

Ver (биты 13-15) - 1 (расширение GRE).

Тип протокола

880B.

Ключ

Необязательное поле. Использование этого поля определяется конкретной реализацией.

Порядковый номер

Необязательное поле. Порядковый номер содержимого.

Номер подтверждения

Необязательное поле. Порядковый номер пакета GRE с максимальным номером, принятого передающей стороной в данной пользовательской сессии.

HSRP

RFC2281 http://www.cis.ohio-state.edu/htbin/rfc/rfc2281.html

Протокол HSRP (Hot Standby Router Protocol) компании Cisco обеспечивает механизм поддержки неразрушающего восстановления трафика IP в некоторых ситуациях. В частности, этот протокол обеспечивает защиту от сбоев в маршрутизаторе первого интервала, когда хост-отправитель не может узнать IP-адрес маршрутизатора первого хопа динамически. Протокол предназначен для использования в локальных сетях с множественным доступом, групповой или широковещательной адресацией (например, Ethernet). Широкий класс традиционных реализаций хостов не поддерживает возможность динамического обнаружения принятого по умолчанию шлюза и соответствующей настройки своих параметров. Протокол HSRP обеспечивает для таких хостов требуемый сервис.

Протокол HSRP работает поверх UDP и использует порт 1985. Пакеты передаются по групповому адресу 224.0.0.2 с временем жизни TTL=1. Маршрутизаторы используют свои реальные адреса IP (а не виртуальные адреса IP) в качестве адреса отправителя для протокольных пакетов, поскольку маршрутизаторы HSRP могут идентифицировать друг друга.

Формат содержащей данные части дейтаграммы UDP для протокола HSRP показан на рисунке.

Формат заголовка HSRP

Версия

Номер версии HSRP (0 для текущей версии).

Код операции

Тип сообщения, содержащегося в пакете:

0 Приветствие (Hello), передаваемое для индикации работы маршрутизатора и его способности работать в активном или резервном (standby) режиме.

1 Coup (переворот) передается в тех случаях, когда маршрутизатор хочет стать активным.

2 Resign передается в тех случаях, когда маршрутизатор больше не хочет быть активным.

Состояние

Каждый маршрутизатор в резервной (standby) реализует машину состояний. Поле состояния описывает текущее состояние маршрутизатора, передающего сообщение. Поле состояния может принимать следующие значения:

0 Initial (изначальное состояние)

1 Learn (обучение)

2 Listen (прослушивание)

4 Speak (разговор)

8 Standby (резерв)

16 Active (активен)

Время приветствия (Hellotime)

Приблизительный период (в секундах) повторения сообщений приветствия (hello), которые передает маршрутизатор. Если для маршрутизатора не настроено время приветствия, он может узнать его из сообщения Hello активного маршрутизатора. Маршрутизатор, передающий сообщение Hello должен установить значение периода приветствия в поле Hellotime. Если поле Hellotime не удается прочитать из сообщения активного маршрутизатора и оно не задано явно, рекомендуется использовать принятый по умолчанию период в 3 секунды.

Время удержания (Holdtime)

Время (в секундах), в течение которого сохраняется корректность текущего приветствия Hello. Это поле применяется только для сообщений Hello.

Приоритет

Поле приоритета используется для выбора активных и резервных маршрутизаторов. При сравнении приоритетов двух различных маршрутизаторов активным назначается тот, у которого значение приоритета выше. При равных приоритетах выбирается маршрутизатор с большим адресом IP.

Группа

Идентифицирует резервную (standby) группу. Для сетей Token Ring корректны значения 0, 1 и 2, для остальных сетей - значения от 0 до 255.

Данные аутентификации

8-байтовое поле, содержащее пароль в явном виде (Clear-text) Если аутентификация не настроена, рекомендуется использовать принятое по умолчанию значение 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.

Виртуальный адрес IP

4-байтовое поле виртуального адреса IP, используемого данной группой. Если виртуальный адрес не задан для маршрутизатора, он может быть получен из сообщения Hello от активного маршрутизатора. Адрес должен определяться таким способом только при его отсутствии в поле и наличии аутентификации для сообщения Hello.

IGRP

Протокол IGRP (Interior Gateway Routing Protocol - протокол внутреннего шлюза) был разработан компанией Cisco. Этот протокол используется для передачи маршрутной информации между маршрутизаторами.

Пакеты IGRP передаются с использованием дейтаграмм IP с полем протокола 9 (IGP). Пакеты начинаются с заголовка IGRP, за которым сразу же следует заголовок IP.

Версия
Код операции
Редактирование
ASystem
NInterior
NSystem
NExterior
Контрольная сумма

Структура заголовка IGRP

Версия

Номер версии протокола (текущее значение - 1).

Код операции

Код операции, связанной с сообщением:

1 Update (обновление).

2 Request (запрос).

Редактирование

Порядковый номер, значение которого уменьшается при каждом внесении изменений в таблицу маршрутизации. Номер редактирования позволяет шлюзам избежать обработки обновлений таблиц маршрутизации, которые уже были учтены.

ASystem

Номер автономной системы. Шлюз может входить в несколько автономных систем, в каждой из которых используется свой протокол IGRP. Для каждой автономной системы используются свои таблицы маршрутизации. Это поле позволяет шлюзу выбрать набор используемых таблиц маршрутизации.

NInterior, NSystem, NExterior

Эти поля показывают номера записей в каждой из трех секций сообщений об обновлении таблиц. Первый элемент (NInterior) является внутренним, следующий (NSystem) - системным и последний (NExterior) - внешним.

Контрольная сумма

Контрольная сумма IP, рассчитанная по тому же алгоритму, который используется для дейтаграмм UDP. При вычислении контрольной суммы принимается во внимание заголовок IGRP и маршрутная информация, которая следует после заголовка. При расчете поле контрольной суммы предполагается нулевым (не учитывается). Контрольная сумма не включает заголовок IP и не использует виртуальных заголовков как в UDP и TCP.

Запрос IGRP требует от получателя передать таблицу маршрутизации. Для запросов используются только поля версии, кода операции и ASystem, остальные поля имеют нулевые значения.

Сообщения об обновлении таблиц содержат заголовок, сразу за которым располагается таблица маршрутизации. Количество записей в таблице ограничено размером дейтаграммы (1500 байтов с учетом заголовка IP). При используемой в настоящее время структуре записей таблица может содержать до 104 элементов. Если таблица маршрутизации содержит большее число записей, нужно использовать несколько сообщений.

NARP

RFC1735 http://www.cis.ohio-state.edu/htbin/rfc/rfc1735.html

Протокол преобразования адресов NARP (NBMA Address Resolution Protocol) позволяет отправителю пакетов (хост или маршрутизатор), желающему связаться с другим узлом через сеть, не поддерживающую широковещательных адресов, с множественным доступом (Non-Broadcast Multi-Access или NBMA) на канальном уровне, найти NBMA-адрес получателя, если последний подключен к той же сети NBMA.

Общий формат заголовков показан на рисунке. Конфигурация заголовка несколько отличается для запросов и откликов NARP.

Структура заголовка NARP

Версия

Номер версии NARP (текущее значение - 1).

Счетчик хопов

Показывает максимальное число NAS, которые может пройти запрос или отклик до его отбрасывания.

Контрольная сумма

Стандартная контрольная сумма IP для всего пакета NARP (начиная с фиксированного заголовка).

Тип

Тип пакета NARP - NARP Request (запрос) имеет тип 1, NARP Reply (отклик) - тип 2.

Код

Отклик на запрос NARP может содержать кэшируемую информацию. Если желательно получить аутентичные (некэшированные) данные, следует использовать код 2 (NARP Request for Authoritative Information). В остальных

случаях используется код 1 (NARP Request). Отклики NARP мошут быть позитивными и негативными. Позитивный, не аутентичный (non-authoritative) отклик передается с кодом 1, позитивный аутентичный - с кодом 2. Для негативных и неаутентичных откликов используется код 3, а для негативных аутентичных - 4.

IP-адрес получателя

Адрес запрашивающего узла.

IP-адрес отправителя

Адрес искомого узла NBMA.

Размер NBMA

Размер (в байтах) поля адреса NBMA отправителя пакета.

Адрес NBMA

Адрес NBMA, дополненный нулями для выравнивания по 32-битовой границе.

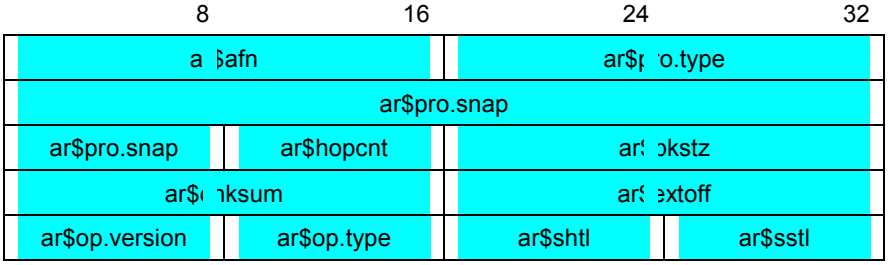
NHRP

RFC2332 http://www.cis.ohio-state.edu/htbin/rfc/rfc2332.html

draft http://info.internet.isi.edu:80/in-drafts/files/draft-ietf-rolc-nhrp-15.txt

Протокол NHRP (NBMA Next Hop Resolution Protocol) позволяет станции-отправителю (хост или маршрутизатор), желающему связаться с другим узлом через сеть, не поддерживающую широковещательных адресов, с множественным доступом (Non-Broadcast Multi-Access или NBMA) на канальном уровне, определять адреса межсетевого уровня и адреса NBMA следующего подходящего маршрутизатора (next hop) NBMA в направлении станции-получателя.

Формат заголовков NHRP показан на рисунке.



Формат заголовков NHRP

ar$afn

Определяет тип адреса канального уровня, который будет передаваться.

ar$pro.type

16-битовое беззнаковое целое.

ar$pro.snap

Когда поле ar$pro.type имеет значение 0x0080, для кодирования типа протокола будет использоваться расширение snap, помещаемое в поле ar$pro.snap. В остальных случаях это поле имеет нулевое значение.

ar$hopcnt

Счетчик интервалов, показывающий максимальное число NHS, через которые может пройти пакет NHRP до его отбрасывания.

ar$pktsz

Общий размер пакета NHRP в октетах.

ar$chksum

Стандартная контрольная сумма IP для всего пакета NHRP.

ar$extoff

Это поле говорит о существовании и местоположении расширений NHRP.

ar$op.version

Это поле показывает версию базового протокола отображения адресов и протокола управления, представленных в данном сообщении.

ar$op.type

Если ar$op.version = 1, данное поле представляет тип пакета NHRP. Поддерживаются следующие типы пакетов:

1 NHRP Resolution Request (запрос преобразования адреса).
2 NHRP Resolution Reply (отклик на запрос преобразования адреса).
3 NHRP Registration Request (запрос регистрации).
4 NHRP Registration Reply (отклик на запрос регистрации).
5 NHRP Purge Request (запрос удаления).
6 NHRP Purge Reply (отклик на запрос удаления).
7 NHRP Error Indication (индикация ошибки).

ar$shtl

Тип и размер NBMA-адреса отправителя в контексте семейства адресов.

ar$sstl

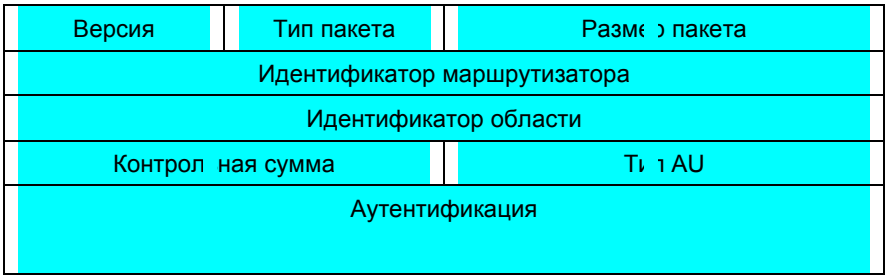
Тип и размер субадреса NBMA для отправителя в контексте семейства адресов (address family number).

OSPF

RFC1583 *http://www.cis.ohio-state.edu/htbin/rfc/rfc1583.html*

OSPF (Open Shortest Path First - открывать сначала кратчайший путь) представляет собой протокол маршрутизации IP на основе информации о состоянии каналов. OSPF является протоколом внутреннего шлюза, используемым для маршрутизации внутри группы маршрутизаторов. Протокол использует технологию оценки состояния каналов, при которой маршрутизаторы передают друг другу информацию о прямых соединениях между ними и каналах связи с другими маршрутизаторами.

Структура заголовков OSPF показана на рисунке.



Структура заголовка OSPF

Версия

Номер версии протокола (текущее значение - 1).

Тип пакета

Используются пакеты следующих типов:

1 Hello
2 Database Description
3 Link State Request
4 Link State Update
5 Link State Acknowledgment.

Размер пакета

Размер пакета в байтах с учетом стандартного заголовка OSPF.

Идентификатор маршрутизатора

Идентификатор маршрутизатора отправителя пакетов. В протоколе OSPF отправителем и получателем пакетов являются два маршрутизатора, расположенные на разных сторонах канала.

Идентификатор области

32-битовое число, идентифицирующее область, к которой относится данный пакет. Все пакеты OSPF ассоциируются с одной областью. Большинство пакетов передаются только через один интервал между маршрутизаторами (хоп). Пакеты, передаваемые через виртуальный канал, маркируются идентификатором магистрали (0.0.0.0).

Контрольная сумма

Стандартная контрольная сумма IP для всего пакета, начиная с заголовка OSPF, но без учета 64-битового поля аутентификации. При расчете контрольной суммы используются 16-битовые слова пакета, за исключением поля аутентификации. Если длина пакета не кратна 16, пакет дополняется 8 нулями до расчета контрольной суммы.

Тип AU

Указывает схему аутентификации, используемую для пакета.

Аутентификация

64-битовое поле, используемое для аутентификации пакета.

Mobile IP

RFC2002 http://www.cis.ohio-state.edu/htbin/rfc/rfc2002.html

RFC2290 http://www.cis.ohio-state.edu/htbin/rfc/rfc2290.html

RFC2344 http://www.cis.ohio-state.edu/htbin/rfc/rfc2344.html

Протокол Mobile IP позволяет перемещать узлы IP из одной подсети в другую. Для идентификации каждого мобильного узла используется его "домашний адрес", независимо от текущего положения этого узла в сети Internet. При обращении из другого места с мобильным узлом также связывается адрес care-of, который обеспечивает информацию о текущем месте подключения узла к Internet. Протокол позволяет регистрировать адреса care-of с "домашним агентом". Агент передает дейтаграммы, адресованные мобильному узлу через туннель, используя адрес care-of. После доставки на удаленный конец туннеля каждая дейтаграмма передается мобильному узлу. Протокол Mobile IP можно использовать в однородных и гетерогенных сетях. Mobile IP определяет группу новых управляющих сообщений, передаваемых с использованием UDP, Registration Request (запрос регистрации) и Registration Reply (отклик на запрос регистрации).

Пакеты IP содержат IP-адреса отправителя и получателя, после которых указывается номер порта UDP для отправителя и получателя, а за ними следуют поля протокола Mobile IP. Пакеты Mobile IP могут являться запросами регистрации (Registration Request) или откликами на такие запросы (Registration Reply).

Формат запросов регистрации Mobile IP показан на рисунке.

Структура запросов регистрации Mobile IP

Тип

Значение 1 говорит о запросе регистрации.

S

Установленный флаг S говорит о том, что мобильный узел запрашивает регистрацию с прежними привязками (prior mobility bindings).

B

Широковещательная дейтаграмма. Установка этого флага говорит о том, что мобильный узел запрашивает туннель для любых широковещательных дейтаграмм, принятых для его домашней сети.

D

Флаг D говорит о том, что мобильный узел будет самостоятельно декапсулировать (извлекать) дейтаграммы, переданные по адресу care-of.

M

Минимальная инкапсуляция. Флаг M говорит о том, что домашний агента мобильного узла использует минимальную инкапсуляцию дейтаграмм, туннелируемых мобильному узлу.

G

GRE-инкапсуляция. Флаг G говорит о том, что домашний агента мобильного узла использует инкапсуляцию GRE для дейтаграмм, туннелируемых мобильному узлу.

V

Van Jacobson. Этот флаг говорит о том, что агент мобильного узла использует компрессию заголовков Van Jacobson для канала связи с мобильным узлом.

T

Этот флаг устанавливается в тех случаях, когда мобильный узел просит своего домашнего агента воспринимать обратный туннель со своего адреса care-of. Мобильные узлы, использующие чужие (foreign) care-of-адреса агентов запрашивают у чужого агента обратное туннелирование для своих пакетов.

R

Зарезервированное поле (0).

Время жизни

Число секунд, остающееся до окончания срока регистрации.

Домашний адрес

IP-адрес мобильного узла.

Домашний агент

IP-адрес домашнего агента мобильного узла.

Адрес Care-of

IP-адрес конца туннеля.

Идентификация

64-битовое число, создаваемое мобильным узлом, для обеспечения соответствия между регистрационными запросами и откликами, а также для защиты от атак путем ответа на регистрационные запросы.

Расширение

После фиксированной части регистрационного запроса может размещаться одно или несколько расширений (Extension). Во все запросы регистрации должно включаться расширение Mobile-Home Authentication Extension.

Формат откликов на регистрационные запросы Mobile IP показан на рисунке.

Структура регистрационных откликов Mobile IP

Тип

Значение 3 говорит об отклике на регистрационный запрос.

Код

Значение, показывающее результат регистрационного запроса:

Успешная регистрация:

0 регистрация принята

1 регистрация принята, но одновременное связывание не поддерживается.

Регистрация отвергнута чужим (foreign) агентом:

64 причина не указана

65 административный отказ

66 нехватка ресурсов

67 отказ при аутентификации мобильного узла
68 отказ при аутентификации домашнего агента
69 время жизни слишком велико для регистрации
70 некорректно сформированный запрос
71 некорректно сформированный отклик
72 запрошенная инкапсуляция недоступна
73 запрошенная компрессия Van Jacobson недоступна

Сервис не поддерживается чужим агентом:

74 запрошенный туннель недоступен
75 обратный туннель является обязательным, а флаг T не установлен
76 мобильный узел слишком удален

Регистрация отвергнута домашним агентом:

80 домашняя сеть недоступна (получена ошибка ICMP)
81 недоступен хост домашнего агента (ошибка ICMP)
82 недоступен порт домашнего агента (ошибка ICMP)
88 недоступен домашний агент (ошибка ICMP)

Сервис не поддерживается домашним агентом:

137 запрошенный обратный туннель недоступен
138 обратный туннель является обязательным, а флаг T не установлен
139 запрошенная инкапсуляция недоступна.

Время жизни

Если поле кода говорит о том, что запрос регистрации принят, время жизни показывает число секунд, остающихся до истечения времени регистрации. Нулевое значение этого поля говорит об отмене регистрации мобильного узла. Значение 0xffff показывает бесконечное время жизни. Если поле кода содержит код отказа в регистрации, значение поля времени жизни не имеет смысла и должно игнорироваться.

Van Jacobson

RFC1144 http://www.cis.ohio-state.edu/htbin/rfc/rfc1144.html

Протокол Van Jacobson обеспечивает механизм компрессии TCP, существенно повышающий эффективность работы систем TCP/IP на низкоскоростных (300 - 19200 бит/с) последовательных каналах.

Формат сжатых пакетов TCP показан на рисунке.

Структура сжатых пакетов TCP

C, I, P, S, A, W, U

Маски изменений, показывающие, какие поля пакета могут быть изменены.

Номер соединения

Используется для указания местоположения копии последнего пакета для данного соединения TCP.

Контрольная сумма TCP

Служит для сквозной проверки целостности передачи данных.

Указатель важности

Это поле используется при установке флага U.

Дельта-значения для каждого поля

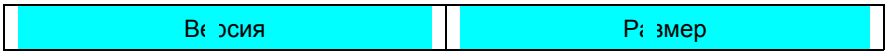
Показывает изменения соответствующих полей по сравнению с исходным пакетом TCP (для каждого поля, указанного в маске изменений).

XOT

RFC1613 *http://www.cis.ohio-state.edu/htbin/rfc/rfc1613.html*

Протокол XOT является реализацией X.25 over TCP компании Cisco Systems.

Формат заголовков XOT показан на рисунке.



Формат заголовков XOT

Версия

Номер версии протокола.

Размер

Общая длина пакета.

MGCP

IETF draft: *http://www.ietf.org/internet-drafts/draft-huitema-mgcp-test1-00.txt*

Протокол MGCP (Media Gateway Control Protocol - протокол управления шлюзом между средами) используется для управления телефонными шлюзами с помощью внешних элементов управления вызовами, называемых контроллерами шлюза сред (media gateway controller) или агентами вызовов (call agent). Телефонный шлюз является элементом сети, обеспечивающим преобразование звуковых сигналов, переносимых по телефонным каналам, в пакеты данных, передаваемые через Internet, и обратное преобразование.

MGCP использует архитектуру управления, в которой интеллектуальные элементы управления вызовами располагаются за пределами шлюза и обслуживаются внешними элементами управления вызовами. MGCP предполагает, что все элементы управления вызовами или агенты вызовов (Call Agent) синхронизированы между собой для передачи согласованных (coherent) команд шлюзам, находящимся под их управлением. Важно отметить, что протокол MGCP использует отношения ведущий-ведомый (master/slave) - шлюзы выполняют команды, передаваемые агентами вызовов.

Протокол MGCP реализует интерфейс управления шлюзом между средами как набор транзакций. Транзакции состоят из команд и обязательных (mandatory) откликов. Существует восемь типов команд:

- CreateConnection (организовать соединение)
- ModifyConnection (изменить соединение)
- DeleteConnection (удалить соединение)
- NotificationRequest (запрос уведомления)
- Notify (уведомление)
- AuditEndpoint (аудит оконечной точки)
- AuditConnection (аудит соединения)
- RestartInProgress (едет процесс перезапуска).

Первые четыре команды передаются шлюзу агентом вызовов. Команда Notify передается шлюзом агенту. Шлюз может также передавать команды удаления соединений (DeleteConnection). Call Agent может передавать шлюзу команды аудита (Audit). Шлюз может передавать команды RestartInProgress агенту вызовов.

Все команды содержат заголовок, за которым может следовать описание сессии. Все отклики содержат заголовок, за которым также может следовать описание сессии. Заголовки и описания сессий представляются наборами текстовых строк, разделенными символами возврата каретки и перевода строки или одним символом перевода строки. Между заголовком и описанием сессии помещается пустая строка.

MGCP использует идентификаторы транзакций для того, чтобы можно было связать запрос с откликом на него. Значения идентификаторов транзакций могут находиться в диапазоне от 1 до 999999999. Объект MGCP не может

повторно использовать идентификатор транзакции раньше, чем через три минуты после завершения предыдущей транзакции с таким же номером.

Заголовок команды содержит:

- Командную строку, идентифицирующую запрашиваемую операцию, идентификатор транзакции, имя оконечной точки, для которой должна выполняться запрошенная операция, и номер версии протокола MGCP.
- Набор строк параметров, содержащих имя и значение параметра.

Командная строка содержит:

- Имя запрашиваемой команды.
- Идентификатор транзакции (1 и 999999999), используемый для сопоставления команд и откликов. Объект MGCP не может повторно использовать идентификатор транзакции раньше, чем через три минуты после завершения предыдущей транзакции с таким же номером.
- Имя оконечной точки, для которой должна выполняться запрошенная операция (в уведомлениях - имя оконечной точки, для которой передается уведомление).
- Номер версии протокола.

Все четыре элемента команд передаются в виде текстовых строк ASCII с разделением слов пробелами (ASCII - 0x20) или символами табуляции (0x09). Предпочтительно использовать в качестве разделителя символ пробела.

SGCP

IETF draft: *http://www.ietf.org/internet-drafts/draft-huitema-sgcp-v1-02.txt*

Протокол SGCP (Simple Gateway Control Protocol - простой протокол управления шлюзом) используется для управления телефонными шлюзами с помощью внешних элементов управления вызовами. Телефонный шлюз является элементом сети, обеспечивающим преобразование звуковых сигналов, переносимых по телефонным каналам, в пакеты данных, передаваемые через Internet, и обратное преобразование.

SGCP использует архитектуру управления, в которой интеллектуальные элементы управления вызовами располагаются за пределами шлюза и обслуживаются внешними элементами управления вызовами. SGCP предполагает, что все элементы управления вызовами или агенты вызовов (Call Agent) синхронизированы между собой для передачи согласованных (coherent) команд шлюзам, находящимся под их управлением.

Протокол SGCP реализует простой интерфейс управления шлюзом между средами как набор транзакций. Транзакции состоят из команд и обязательных (mandatory) откликов. Существует пять типов команд:

- CreateConnection (организовать соединение)
- ModifyConnection (изменить соединение)
- DeleteConnection (удалить соединение)
- NotificationRequest (запрос уведомления)
- Notify (уведомление)

Первые четыре команды передаются шлюзу агентом вызовов. Команда Notify передается шлюзом агенту. Шлюз может также передавать команды удаления соединений (DeleteConnection).

Все команды содержат заголовок, за которым может следовать описание сессии. Все отклики содержат заголовок, за которым также может следовать описание сессии. Заголовки и описания сессий представляются наборами текстовых строк, разделенными символами возврата каретки и перевода строки или одним символом перевода строки. Между заголовком и описанием сессии помещается пустая строка.

Заголовок команды содержит:

- Командную строку.
- Набор строк параметров, содержащих имя и значение параметра.

Командная строка содержит:

- Имя запрашиваемой команды.
- Идентификатор транзакции (1 и 999999999), используемый для сопоставления команд и откликов. Объект MGCP не может повторно использовать идентификатор транзакции раньше, чем через три минуты после завершения предыдущей транзакции с таким же номером.
- Имя оконечной точки, для которой должна выполняться запрошенная операция (в уведомлениях - имя оконечной точки, для которой передается уведомление).

- Номер версии протокола.

Все четыре элемента команд передаются в виде текстовых строк ASCII с разделением слов пробелами (ASCII - 0x20) или символами табуляции (0x09). Предпочтительно использовать в качестве разделителя символ пробела.

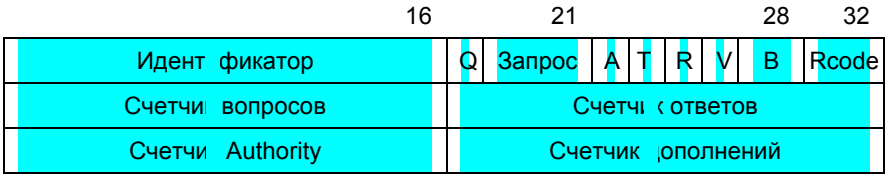
DNS

RFC1035 http://www.cis.ohio-state.edu/htbin/rfc/rfc1035.html

RFC1706 http://www.cis.ohio-state.edu/htbin/rfc/rfc1706.html

Протокол DNS (Domain Name Service - служба доменных имен) обеспечивает поиск имен хостов, используя распределенную по сетевым серверам имен базу данных.

Формат сообщений DNS показан на рисунке.



Формат сообщений DNS

Идентификатор

16-битовое поле для обозначения соответствия между запросами и откликами.

Q

1-битовый флаг запроса (query).

Запрос

4-битовое описание типа сообщения:

0 стандартный запрос (адрес по имени).

1 обратный запрос (имя по адресу).

2 запрос состояния сервера.

A

Authoritative Answer - 1-битовый флаг, показывающий отклик от уполномоченного (authoritative) сервера имен.

T

Truncation - отбрасывание. 1-битовый флаг, говорящий об отбрасывании сообщения.

R

1-битовый флаг, устанавливаемый устанавливаемый для разрешения запроса рекурсивным путем.

V

1-битовый флаг поддержки рекурсивного сервиса.

B

3-битовое поле, зарезервированное для использования в будущем (0).

RCode

Код отклика - 4-битовое поле, устанавливаемое сервером имен для обозначения состояния запроса:

0 нет ошибок.

1 невозможно интерпретировать запрос из-за формальной ошибки.

2 обработка невозможна из-за сбоя на сервере.

3 запрошенное имя не существует.

4 неподдерживаемый тип запроса.

5 отказ от выполнения запроса.

Счетчик вопросов

16-битовое поле, содержащее число записей в разделе вопросов.

Счетчик ответов

16-битовое поле, содержащее число записей о ресурсах в разделе ответов.

Счетчик Authority

16-битовое поле, определяющее число записей о ресурсах сервера имен в разделе authority (полномочия).

Счетчик дополнений

16-битовое поле, определяющее число записей о ресурсах сервера имен в дополнительном разделе.

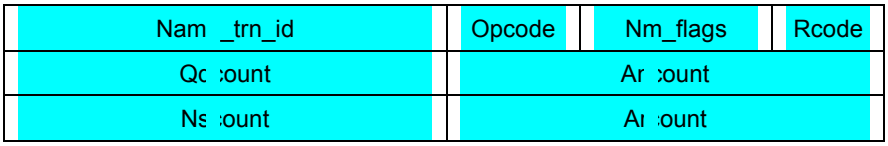
NetBIOS/IP

RFC1002 *http://www.cis.ohio-state.edu/htbin/rfc/rfc1002.html*

NetBIOS/IP является стандартным протоколом поддержки сервиса NetBIOS в средах TCP/IP как для локальных сетей, так и для Internet. Определены различные типы узлов для поддержки разных топологий ЛВС и Internet, а также для обеспечения возможности использования широковещательных пакетов IP или запрета широковещания.

Для протокола NetBIOS поддерживаются типы Name Service, Session или Datagram.

Формат заголовков NetBIOS/IP показан на рисунке.



Структура заголовка NetBIOS/IP

Name_trn_id

Идентификатор транзакции для службы имен (Name Service Transaction).

Opcode

Код операции, задающий тип пакета:

0 Query (запрос).

5 Registration (регистрация).

6 Release (освобождение).

7 WACK.

8 Refresh (обновление).

Nm_flags

Флаги операции.

Rcode

Код результата запроса.

Qdcount

16-битовое беззнаковое целое, показывающее число записей в разделе вопросов пакета службы имен.

Ancount

16-битовое беззнаковое целое, показывающее число записей в разделе ответов пакета службы имен.

Nscount

16-битовое беззнаковое целое, показывающее число записей в разделе authority (полномочия) пакета службы имен.

Arcount

16-битовое беззнаковое целое, показывающее число записей в дополнительном разделе пакета службы имен.

FTP

RFC959 http://www.cis.ohio-state.edu/htbin/rfc/rfc959.html

Протокол FTP (File Transfer Protocol - протокол переноса файлов) обеспечивает базовые элементы системы совместного использования файлов хостами сети. Протокол FTP использует TCP для создания виртуальных соединений, обеспечивающих поддержку управления. Для операций переноса файлов организуется отдельное соединение TCP. Управляющие соединения используют образ протокола TELNET для обмена командами и сообщениями между хостами сети.

Команды

Кадры управления FTP используют обмен TELNET и могут содержать команды TELNET или опции согласования параметров. Однако, большинство управляющих кадров FTP является просто текстовыми строками ASCII и может классифицироваться как команды или сообщения FTP. Ниже приведен список стандартных команд FTP:

Команда	***Описание***
ABOR	прервать соединение, используемое для передачи данных.
ACCT <account>	Учетная запись для системных привилегий.
ALLO <bytes>	Выделение пространства для записи фалов на сервер.
APPE <filename>	Добавление (Append) файла к файлу с таким же именем на сервере.
CDUP <dir path>	Переход в родительский каталог на сервере.
CWD <dir path>	Смена рабочего каталога на сервере.
DELE <filename>	Удаление файла на сервере.
HELP <command>	Получение справки об указанной команде.
LIST <name>	Получение информации о связи имени с файлом или каталогом.
MODE <mode>	Режим передачи (S=поток, B=блок, C=компрессия).
MKD <directory>	Создание каталога на сервере.
NLST <directory>	Список содержимого каталога.
NOOP	Отсутствие операций, кроме подтверждений от сервера.
PASS <password>	Пароль для входа в систему.
PASV	Запрос к серверу на соединение, для передачи данных.
PORT <address>	IP-адрес и 2-байтовый номер порта.
PWD	Выводит имя текущего каталога.
QUIT	Отключение от сервера FTP.
REIN	Повторный вход в систему.
REST <offset>	Восстановление передачи файла с заданной позиции.

RETR <filename>	Найти (скопировать) файл на сервере.
RMD <directory>	Удалить каталог на сервере.
RNFR <old path>	Переименовать путь (со старого).
RNTO <new path>	Переименовать путь (на новый).
SITE <params>	Получить параметры сайта от сервера.
SMNT <pathname>	Смонтировать указанную структуру файлов.
STAT <directory>	Получить информацию о текущем каталоге или процессе.
STOR <filename>	Записать (скопировать) файл на сервер.
STOU <filename>	Сохранить файл с именем сервера.
STRU <type>	Структура данных (F=файл, R=запись, P=страница).
SYST	Получить информацию об операционной системе сервера.
TYPE <data type>	Тип данных (A=ASCII, E=EBCDIC, I=бинарные).
USER <username>	Имя пользователя для входа в систему.

Сообщения

Сообщения FTP являются откликами на команды FTP и содержат код отклика, за которым следует пояснительный текст. Стандартные сообщения FTP и пояснительные тексты к ним перечисленыв ниже:

Код	***Пояснительный текст***
110	Restart marker at MARK yyyy=mmmm (new file pointers).
120	Service ready in nnn minutes.
125	Data connection open, transfer starting.
150	Open connection.
200	OK.
202	Command not implemented.
211	(System status reply).
212	(Directory status reply).
213	(File status reply).
214	(Help message reply).
215	(System type reply).
220	Service ready.
221	Log off network.
225	Data connection open.
226	Close data connection.
227	Enter passive mode (IP address, port ID).
230	Log on network.
250	File action completed.
257	Path name created.

331	Password required.
332	Account name required.
350	File action pending.
421	Service shutting down.
425	Cannot open data connection.
426	Connection closed.
450	File unavailable.
451	Local error encountered.
452	Insufficient disk space.
500	Invalid command.
501	Bad parameter.
502	Command not implemented.
503	Bad command sequence.
504	Parameter invalid for command.
530	Not logged onto network.
532	Need account for storing files.
550	File unavailable.
551	Page type unknown.
552	Storage allocation exceeded.
553	File name not allowed.

TFTP

RFC783 http://www.cis.ohio-state.edu/htbin/rfc/rfc783.html

RFC1350 http://www.cis.ohio-state.edu/htbin/rfc/rfc1350.html

Протокол TFTP (Trivial File Transfer Protocol - тривиальный протокол переноса файлов) использует дейтаграммы UDP. TFTP поддерживает операции записи и чтения файлов, но не поддерживает служб каталогов и проверки полномочий (авторизации) пользователей.

Команды

Список команд TFTP приведен ниже:

Команда	***Описание***
Read Request	Запрос на чтение файла.
Write Request	Запрос на запись в файл.
File Data	Копирование файла.
Data Acknowledge	Подтверждение.
Error	Индикация ошибки.

Параметры

Запросы чтения и записи протокола TFTP используют следующие параметры:

Параметр	Описание
Filename	Имя файла (в кавычках), который будет использоваться для чтения или записи.
Mode	Режим передачи данных - формат файла для копирования:
	NetASCII — файл ASCII.
	Octet — 8-битовые бинарные данные.
	Mail — стандартный формат ASCII с именем пользователя вместо имени файла.

Команды данных и подтверждения TFTP используют следующие параметры:

Команда	***Описание***
Block	Номер блока или порядковый номер текущего кадра данных.
Data	Первая часть файла данных для кадров данных TFTP.
TFTP Errors	Кадр ошибки TFTP, содержащий код ошибки в круглых скобках, сопровождаемое сообщением об ошибке:
	(0000) — неизвестная ошибка.
	(0001) — файл не найден.
	(0002) — нарушение прав доступа.
	(0003) — нехватка места на диске.
	(0004) — некорректная операция TFTP.

(0005) неизвестный идентификатор транзакции.
(0006) файл с таким именем уже существует.
(07) неизвестный пользователь.

Finger

RFC1288 http://www.cis.ohio-state.edu/htbin/rfc/rfc1288.html

Протокол Finger обеспечивает простой интерфейс с удаленными программами, обеспечивающими информацию о пользователях. Это протокол обмена информацией о пользователях на базе протокола TCP с использованием порта 79 (восьмеричный номер - 117). Локальный хост открывает TCP-соединение с удаленным хостом через порт Finger. После этого удаленная сторона получает доступ к RUIP для обработки запросов о пользователях. Локальный хост посылает RUIP одну строку запроса на основе спецификации запросов Finger и ожидает отклика RUIP. После получения и обработки запроса RUIP возвращает ответ, инициируя завершение сеанса и разрыв соединения. Локальный хост получает ответ и сигнал закрытия сеанса, после чего разрывает соединение.

Протокол Finger отображает данные и вся передаваемая информация должна быть представлена в формате ASCII без бита контроля четности и с завершением строк символами перевода строки и возврата каретки (ASCII 13, ASCII 10). Такое требование исключает использование других форматов типа EBCDIC. Кроме того, любой символ с кодом ASCII от 128 до 255 должны трактоваться как символы других языков. Отметим, что последовательность символов ASCII 13, ASCII 10 не отображается на экране, поскольку она означает лишь переход в начало новой строки.

Gopher

RFC 1436 http://www.ietf.org/rfc/rfc1436.txt

Протокол Internet Gopher и одноименная программа используют модель клиент-сервер. Этот протокол предполагает использование надежного протокола доставки TCP. Серверы Gopher прослушивают порт 70 (этот номер порта выделен для протокола Gopher комитетом IANA). Документы Gopher могут располагаться на множестве хостов Internet. Пользователи запускают клинетскую программу на своем компьютере, подключаются к серверу Gopher и посылают ему селектор (строка текста, которая может быть пустой) через соединение TCP с использованием пердопределенного порта. Сервер отвечает на запрос текстовым блоком, завершающимся точкой в пустой строке и разрывает соединение.

Первый символ каждой строки говорит о том, что описывает строка - документ, каталог или поисковый сервис. Следующие символы (до знака табуляции) формируют строку вывода на пользовательский экран, служащую для выбора данного документа (или каталога). Первый символ строки реально определяет тип элемента, отображаемого этой строкой. Почти во всех случаях клиент Gopher предоставляет пользователю некоторое представление о том, чему соответствует данный элемент (выводится пиктограмма, короткий текст или несто подобное).

Символы после знака табуляции (до следующего символа табуляции) формируют строку селектора, которую клиентская программа должна передать серверу для получения документа (или списка содержимого каталога). Клиент никогда не меняет строку селектора, которая зачастую является маршрутом доступа или другим селектором, используемым сервером для доступа к желаемому элементу. Следующие два символа табуляции обозначают имя домена для хоста и номер порта. При наличии других символов табуляции клиент Gopher должен игнорировать их. Символы CR LF обозначают переход на новую строку.

Символы типа элементов

Клиент Gopher решает вопрос доступности объекта для просмотра по первому символу каждой строки в списке содержимого каталога. Увеличение этого списка может расширять протокол. Ниже приведен список определенных в настоящее время элементов:

0	Файл
1	Каталог
2	Сервер телефонного справочника CSO
3	Ошибка
4	Файл BinHexed Macintosh
5	Некоторые типы бинарных архивов DOS (клиент должен читать архив до завершения сеанса TCP).
6	UU-кодированный файл UNIX

7	Сервер Index-Search
8	Указатель на текстовую сессию Telnet.
9	Бинарный файл (клиент должен читать архив до завершения сеанса TCP).
+	Резервный сервер
T	Указатель на текстовый сеанс tn3270
g	Графический файл в формате GIF
I	Некоторые файлы образов (клиент должен сам выбрать способ отображения).

Символы от 0 до Z зарезервированы. Для локальных экспериментов следует использовать другие символы. Связанные с отдельными типами оборудования расширения не приветствуются. Отметим, что для типов 5 и 9 клиент должен клиент должен быть готов к чтению до завершения сеанса TCP. В конце таких файлов отсутствует завершающая точка в пустой строке, сеанс для этих файлов имеет бинарный тип и клиент должен самостоятельно выбирать способ отображения.

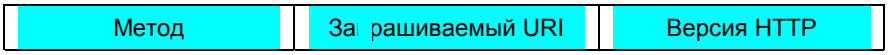
HTTP

RFC1945 http://www.cis.ohio-state.edu/htbin/rfc/rfc1945.html

HTTP (Hypertext Transfer Protocol - протокол передачи гипертекста) представляет собой протокол уровня приложений, обеспечивающий простой и быстрый способ организации распределенных гиперсред для совместного использования в сети. Сообщения передаются в формате, похожем на форматы Internet Mail и MIME (Multipurpose Internet Mail Extensions).

Пакет запроса

Формат запросов показан на рисунке.



Структура заголовка HTTP

Метод

Метод, который нужно выполнить для ресурса.

Запрашиваемый URI

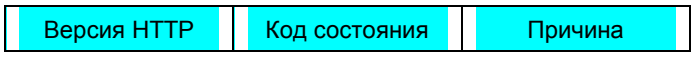
Универсальный идентификатор ресурса (Uniform Resource Identifier URI), к которому адресуется запрос, т.е. сетевого ресурса.

Версия HTTP

Используемая версия протокола HTTP.

Пакеты откликов

Формат откликов HTTP показан на рисунке.



Структура отклика HTTP

Версия HTTP

Используемая версия протокола HTTP.

Код состояния

3-значное целое число, указывающее код результата.

Причина

Текстовое описание результата запроса.

S-HTTP

draft-ietf-wts-shttp-06

Протокол S-HTTP (Secure HTTP) обеспечивает механизм защищенной связи между парами клиент-сервер HTTP для того, чтобы можно было выполнять коммерческие транзакции с помощью широкого класса приложений. S-HTTP обеспечивает гибкое решение для поддержки множества ортогональных режимов работы, механизмов управления ключами, моделей доверия, криптографических алгоритмов и форматов инкапсуляции путем согласования опций между участниками каждой транзакции. Сообщения Secure HTTP синтаксически совпадают с сообщениями HTTP и состоят из строк запроса или состояния, за которыми следует заголовок и текст сообщения. Однако заголовки S-HTTP отличаются от заголовков HTTP, а тело сообщений обычно зашифровано.

IMAP4

RFC2060 http://www.cis.ohio-state.edu/htbin/rfc/rfc2060.html

Протокол IMAP4 (Internet Message Access Protocol, Version 4rev1) обеспечивает клиентам доступ и возможность манипуляций с почтовыми сообщениями на сервере. IMAP4 поддерживает операции с удаленными папками сообщений, называемыми почтовыми ящиками (mailbox) как при работе с локальными почтовыми ящиками. Протокол IMAP4 обеспечивает также поддержку offline-клиентов для ресинхронизации с сервером.

IMAP4 включает операции создания, удаления и переименования почтовых ящиков, просмотра новых сообщений, удаления сообщений навсегда, установки и снятия флагов, грамматического разбора (parsing), поиска и выборки атрибутов сообщений, текстов и их частей. Сообщения в IMAP4 допускают использование номеров, являющихся порядковыми номерами или уникальными идентификаторами сообщений.

IMAP4 состоит из последовательности текстовых сообщений, содержащих команды, текстовые строки и т.п. Каждое сообщение завершается последовательностью символов CRLF (перевод строки, возврат каретки). Пример сообщения приведен ниже:

```
Server Message: "a002 OK [READ-WRITE] SELECT completed<crlf>"
```

```
Client Message: "a001 login mrc secret<crlf>"
```

Предопределенных полей в протколе IMAP4 не используется.

IPDC

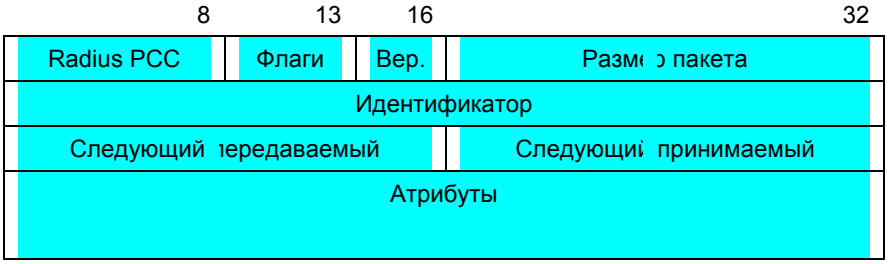
Internet Drafts http://www.ietf.org/internet-drafts/draft-draft-taylor-ipdc-00.txt

Internet Drafts http://www.ietf.org/internet-drafts/draft-calhoun-diameter-07.txt

IPDC (IP Device Control - управление устройствами IP) представляет собой семейство протоколов, компоненты которого можно использовать совместно ил по отдельности для управления соединениями, средой и передачей сигнализации. Этот протокол решает задачи одного или нескольких протоколов управления шлюзами, расположенными на границе между коммутируемой телефонной сетью и сетью internet, а также завершающих коммутируемые транки. Примерами таких устройств могут служить серверы доступа и шлюзы VoIP (голос через IP). Необходимость разделения протоколов управления от системы сигнализации возникает в тех случаях, когда требуется, чтобы логика управления сервисом для обработки соединений полностью или частично была реализована за пределами шлюзов. Протокол IPDC был построен на базе структуры, обеспечиваемой протоколом DIAMETER, который был специально разработан для аутентификации, авторизации и ведения учета.

Существуют два типа сообщений IPDC/DIAMETER - сообщения, содержащие только заголовок, и сообщения с парами атрибут-значение AVP в дополнение к заголовку. Сообщения, состоящие только из заголовка, используются в качестве подтверждений для партнера.

Формат заголовков IPDC показан на рисунке.



Формат заголовков IPDC

Radius PCC

Поле PCC (Packet Compatibility Code - код совместимости пакета) используется для обратной совместимости с протоколом RADIUS. Для того, чтобы отличать сообщения DIAMETER/IPDC от сообщений RADIUS используются специально зарезервированные значения, позволяющие одновременно поддерживать оба протокола, используя первый октет заголовка. Поле RADIUS PCC в сообщениях DIAMETER/IPDC должно иметь значение 254.

Флаги пакета

Флаги пакета используются для идентификации всех опций.

Версия

Номер версии, связанной с принимаемым пакетом. Значение 1 показывает протокол IPDC версии 1.

Размер пакета

Показывает размер пакета с учетом полей заголовка.

Идентификатор

Используется для обозначения соответствия между запросами и откликами.

Следующий передаваемый (Ns)

Это поле присутствует в пакетах при установке флага Window-Present в заголовке пакета. Поле Next Send (Ns) копируется из переменной состояния порядкового номера передачи (Ss) во время передачи сообщения.

Следующий принимаемый (Nr)

Это поле присутствует в пакетах при установке флага Window-Present в заголовке пакета. Поле Nr Поле Next Send (Ns) копируется из переменной состояния порядкового номера приема (Sr) и показывает порядковый номер (Ns) +1 (модуль 2^16) принятого пакета с наибольшим номером.

Атрибуты

Атрибуты IPDC содержат специфические команды и параметры, которые должны передаваться между оконечными точками IPDC для выполнения задач связанных с управлением шлюзом сред (Media Gateway).

ISAKMP

RFC2408 *http://www.cis.ohio-state.edu/htbin/rfc/rfc2408.html*

Протокол ISAKMP (Internet Message Access Protocol, version 4rev1) определяет процедуры и форматы пакетов для организации, согласования, обновления и удаления ассоциаций безопасности SA (Security Associations). SA содержат все сведения, требуемые для выполнения различных типов сервиса обеспечения безопасности сети (услуги IP-уровня типа аутентификации заголовков и инкапсуляции содержимого, услуги транспортного и прикладного уровней, самообеспечение безопасности трафика согласования параметров). ISAKMP определяет содержимое (payload) обмена при генерации ключей и данных аутентификации. Эти форматы обеспечивают надежный способ обмена ключами и сведениями аутентификации независимо от метода генерации ключей, алгоритма шифрования и механизма аутентификации.

Формат заголовков ISAKMP показан на рисунке.

Структура ISAKMP

Initiator cookie

Cookie объекта, инициировавшего организацию SA, уведомление SA или удаление SA.

Responder cookie

Cookie объекта, отвечающего на сообщение от организации SA, уведомлении SA или удалении SA.

Следующий элемент

Показывает тип первого элемента содержимого (payload) в данном сообщении. Поддерживаются следующие типы:

0 нет

1	Security Association (SA)
2	Proposal (P) - предложение
3	Transform (T) -0 преобразовать
4	Key Exchange (KE) - обмен ключами
5	Identification (ID) - идентификация
6	Certificate (CERT) - сертификат
7	Certificate Request (CR) - запрос сертификата
8	Hash (HASH) - смешать
9	Signature (SIG) - сигнатура, подпись
10	Nonce (NONCE)
11	Notification (N) - уведомление
12	Delete (D) - удалить
13	Vendor ID (VID) - идентификатор производителя
14-127	Reserved - зарезервированы
128-255	Private use - частное использование

MjVer

Показывает старшую часть номера версии используемого протокола ISAKMP. Реализации на основе RFC2408 должны использовать значение 1, а реализации на основе предварительных версий ISAKMP (Internet-Drafts) - 0. Никакая из реализаций не будет воспринимать пакеты с номером версии, превышающий номер версии данной реализации.

MnVer

Показывает младшую часть номера версии используемого протокола ISAKMP. Реализации на основе RFC2408 должны использовать значение 0, а реализации на основе предварительных версий ISAKMP (Internet-Drafts) - 1. Никакая из реализаций не будет воспринимать пакеты с номером версии, превышающий номер версии данной реализации.

Тип обмена

Показывает тип используемого обмена. Это поле диктует тип сообщений и содержимого при обмене ISAKMP. Поддерживаются следующие типы:

0	None
1	Base
2	Identity Protection
3	Authentication Only
4	Aggressive
5	Informational
6-31	ISAKMP Future Use
32-239	DOI Specific Use
240-255	Private Use

Флаги

Задает опции, установленные для обмена ISAKMP.

E(ncryption) - бит 0 - указывает, что содержимое после заголовка зашифровано с использованием алгоритма, указанного в ISAKMP SA.

C(ommit) - бит 1 - сигнализирует о синхронизации обмена ключами. Этот флаг используется для того, чтобы зашифрованная информация не была получена до завершения процесса организации SA.

A(uthentication Only) - бит 2 - предназначен для использования в Informational Exchange с содержимым Notify и будет позволять передачу информации с проверкой целостности, но без шифрования.

Все остальные биты устанавливаются в нулевые значения до передачи.

Идентификатор сообщения

Уникальный идентификатор протокола используется для идентификации состояния протокола в процессе согласования Phase 2 (фаза 2). Это число генерируется случайным образом инициатором согласования фазы 2. В случае одновременной организации SA (коллизия), значения этого поля будут явно отличаться, поскольку они генерируются независимо и, таким образом, две ассоциации безопасности будут находиться в процессе создания. Однако, ниоткуда не следует, что эти ассоциации будут завершены одновременно. В течение согласования фазы Phase 1 это поле должно иметь нулевое значение 0.

Размер

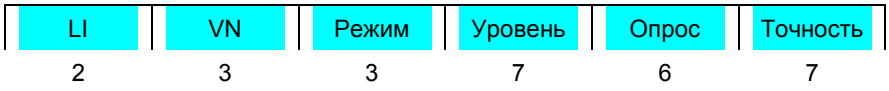
Размер сообщения (заголовок и содержимое) в октетах. Шифрование может расширять размер сообщения ISAKMP.

NTP

RFC1305 http://www.cis.ohio-state.edu/htbin/rfc/rfc1305.html

NTP (Network Time Protocol) представляет собой систему синхронизации компьютерных часов через сеть Internet, обеспечивающую механизм синхронизации и координацию распространения информации в больших сетях, использующих каналы с различными скоростями. Протокол использует структуру распространения информации между серверами точного времени, образующими самоорганизующуюся иерархическую структуру "ведущий-ведомый" (master-slave) для синхронизации локальных часов подсети с национальными стандартными часами по проводам или радиоканалу.

Формат заголовков NTP показан на рисунке.



Структура заголовка NTP

LI (Leap Indicator)

2-битовый код предупреждения о приближении секунд, добавляемых в конце последнего дня текущего месяца. Используются следующие варианты кодов предупреждения:

00 нет предупреждения.
01 +1 секунда (следующая минута содержит 61 секунду).
10 -1 секунда (следующая минута содержит 59 секунд).
11 условия тревоги (часы не синхронизированы).

VN

3-битовый код, показывающий номер версии.

Режим

Поле режима может содержать следующие значения:

0 зарезервировано.
1 Symmetric active (симметричный).
3 Client (клиент).
4 Server (сервер).
5 Broadcast (широковещательный).
6 NTP control message (управляющее сообщение NTP).

Уровень эталона

Целое число, показывающее уровень эталона для локальных часов:

0 не указана.

1 первичный эталон (например, радио-часы).

2...n вторичный эталон (через NTP).

Опрос

Целое число со знаком, показывающее максимальный интервал между последовательными сообщениями в степенях числа 2.

Точность

Целое число со знаком, показывающее точность локальных часов в виде степени числа 2.

POP3

RFC1939 http://www.cis.ohio-state.edu/htbin/rfc/rfc1939.html

Протокол POP3 (Post Office Protocol version 3) позволяет рабочим станциям динамически забирать почту с сервера. Этот протокол обычно используется рабочими станциями для получения почты с обслуживающих их почтовых серверов..

Сообщения POP3 являются командами или откликами.

RADIUS

RFC2138 http://www.cis.ohio-state.edu/htbin/rfc/rfc2138.html

RFC2139 http://www.cis.ohio-state.edu/htbin/rfc/rfc2139.html

RADIUS представляет собой протокол, управляющий распределенными последовательными линиями для большого числа пользователей.

Формат заголовков RADIUS показан на рисунке.

Структура заголовка RADIUS

Код

Идентификатор типа сообщения.

Идентификатор

Значение, используемое для сопоставления запросов и откликов.

Размер

Размер сообщения с учетом заголовка.

Authenticator

Поле, используемое для аутентификации откликов от сервера RADIUS и в алгоритмах сокрытия пароля.

RLOGIN

Протокол RLOGIN (Remote LOGIN - удаленный вход в систему) позволяет пользователям UNIX подключаться к системам UNIX на других машинах через сеть Internet и работать так же, как при прямом подключении терминала к машине. Этот протокол обеспечивает такой же сервис, как протокол TELNET.

RTSP

RFC2326 http://www.cis.ohio-state.edu/htbin/rfc/rfc2326.html

RTSP (Real-Time Streaming Protocol - протокол потоков в реальном масштабе времени) представляет собой протокол прикладного уровня, обеспечивающий контроль доставки данных для приложений реального времени. RTSP обеспечивает возможность эффективной, управляемой доставки по запросам данных в реальном масштабе времени для таких приложений, как видео или аудио. Источниками данных могут являться как системы сбора информации (например, видеокамеры), так и системы хранения данных (воспроизведение клипов). Этот протокол предназначен для управления множеством сеансов доставки данных за счет организации каналов доставки (таких, как UDP, multicast UDP и TCP) и обеспечения выбора механизма доставки на основе RTP.

Потоки, управляемые протоколом RTSP могут использовать RTP, но работа протокола RTSP не зависит от механизма транспортировки, используемого для передачи непрерывного потока данных. Протокол по синтаксису сделан подобным протоколу HTTP/1.1 что позволяет в большинстве случаев добавлять механизмы расширения HTTP в протокол RTSP.

Однако, RTSP в нескольких аспектах значительно отличается от протокола HTTP:

- RTSP добавляет множество новых методов и использует другой идентификатор протокола.
- Сервер RTSP должен по умолчанию поддерживать состояние почти во всех случаях в отличии от stateless-природы протокола HTTP.
- Как серверы, так и клиенты RTSP могут передавать запросы.
- Данные передаются по отдельному каналу (out-of-band) с использованием другого протокола.
- Для протокола RTSP определено использование набора символов ISO 10646 (UTF-8) взамен ISO 8859-1, используемого в текущей версии HTML.
- Request-URI всегда содержать абсолютные указатели URI. В силу обратной совместимости с историческими глупостями HTTP/1.1 передает в запросах только абсолютные пути, помещая имя хоста в отдельное поле заголовка.

Использование протокола RTSP упрощает создание и поддержку виртуальных серверов, где один хост с одним адресом IP обслуживает несколько структур (деревьев) документов.

SMTP

RFC821 http://www.cis.ohio-state.edu/htbin/rfc/rfc821.html

SMTP (Simple Mail Transfer Protocol - простой почтовый протокол) представляет собой почтовый сервис, смоделированный на основе файлового сервиса FTP. SMTP обеспечивает передачу почтовых сообщений между системами и уведомления о входящей почте.

Команды

Команды SMTP представляют собой сообщения ASCII, передаваемые между хостами SMTP. Ниже приведен список поддерживаемых команд:

Команда	***Описание***
DATA	Начинает сборку (composition) сообщения.
EXPN <string>	Возвращает имена из указанного списка рассылок.
HELO <domain>	Возвращает идентификацию почтового сервера.
HELP <command>	Возвращает информацию об указанной команду.
MAIL FROM <host>	Инициирует почтовый сеанс с хоста.
NOOP	Нет операций кроме подтверждений от сервера.
QUIT	Прерывает почтовую сессию.
RCPT TO <user>	Обозначает получателя почты.
RSET	Сбрасывает (Reset) почтовое соединение.
SAML FROM <host>	Передает почту на терминал пользователя и в почтовый ящик.
SEND FROM <host>	Передает почту на терминал пользователя.
SOML FROM <host>	Передает почту на терминал пользователя или в почтовый ящик.
TURN	Меняет ролями отправителя и получателя.
VRFY <user>	Проверяет идентификацию пользователя.

Сообщения

Отклики SMTP содержат код сообщения и текстовое пояснение к нему:

Код отклика	***Пояснение***
211	(Response to system status or help request) - отклик на запрос состояния системы или справки.
214	(Response to help request) - отклик на запрос справки.
220	Mail service ready - готовность почтового сервиса.
221	Mail service closing connection - почтовый сервис закрыл соединение.
250	Mail transfer completed - передача почты завершена.

251	User not local, forward to <path> - нелокальный пользователь, использовать маршрут.
354	Start mail message, end with <CRLF><CRLF> - начало почтового сообщения, завершаемого символами <CRLF><CRLF>.
421	Mail service unavailable - почтовый сервис недоступен.
450	Mailbox unavailable - почтовый ящик недоступен.
451	Local error in processing command - локальная ошибка при обработке команды.
452	Insufficient system storage - недостаточно свободного пространства на диске.
500	Unknown command - неизвестная команда.
501	Bad parameter - некорреткный параметр.
502	Command not implemented - команда не реализована.
503	Bad command sequence - некорректная последовательность команд.
504	Parameter not implemented - параметр не реализован.
550	Mailbox not found - не найден почтовый ящик.
551	User not local, try <path> - нелокальный пользователь, нужно попробовать маршрут.
552	Storage allocation exceeded - невозможно выделить больше пространства на диске.
553	Mailbox name not allowed недопустимое имя почтового ящика.
554	Mail transaction failed - сбой при почтовой транзакции.

SNMP

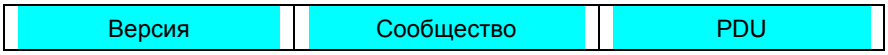
RFC1157 http://www.cis.ohio-state.edu/htbin/rfc/rfc1157.html

Обзор протокола SNMP: http://service.baltnet.ru/info/CIE/Topics/108.htm

Сообщество Internet разработало протокол SNMP для того, чтобы различные объекты сетей могли участвовать в глобальной архитектуре управления сетью. Системы сетевого управления могут опрашивать (сканировать) сетевые объекты, реализующие протокол SNMP для получения информации, имеющей отношение к частной реализации системы управления сетью. Система управления сетью узнает о проблемах, получая прерывания (trap) или уведомления об изменениях от сетевых устройств, реализующих SNMP.

Формат сообщений SNMP

SNMP является сеансовым протоколом, инкапсулируемым в дейтаграммы UDP. Формат сообщений SNMP показан на рисунке.



Формат сообщений SNMP

Версия

Номер версии протокола SNMP. Менеджер и агент должны использовать одну версию протокола. Сообщения, содержащие идентификаторы других версий отбрасываются без обработки.

Сообщество

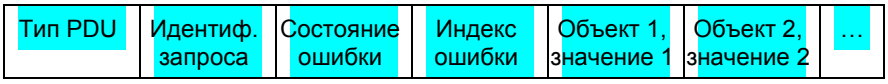
Имя сообщества (Community), используемое для аутентификации перед разрешением доступа к агенту.

PDU

Поддерживаются пять различных типов PDU: GetRequest, GetNextRequest, GetResponse, SetRequest и Trap. Общее описание всех типов пакетов приведено ниже.

Формат PDU

Формат пакетов GetRequest, GetNext Request, GetResponse и SetRequest показан на рисунке.



Формат SNMP PDU

Тип PDU

Задает тип PDU:

0 GetRequest.
1 GetNextRequest.
2 GetResponse.
3 SetRequest.

Идентификатор запроса

Целое число, позволяющее установить корреляцию между запросами менеджера и откликами агента.

Состояние ошибки

Целое число, показывающее результат выполнения операции. Возможные коды результатов перечислены ниже:

0 noError: нет ошибок, корректная работа менеджера или агента.
1 tooBig: размер требуемого пакета GetResponse превышает локальные ограничения.
2 noSuchName: имя запрошенного объекта не соответствует ни одному из доступных имен MIB View.
3 badValue: запрос SetRequest имеет некорректный тип, размер или значение переменной.
4 readOnly: не определено в RFC1157.
5 genErr: прочие ошибки, не включенные в список.

Индекс ошибки

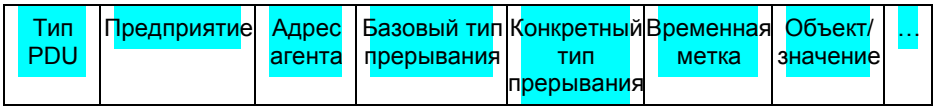
Указывает запись в переменной, с которой связана причина ошибки.

Объект/значение

Связанная пара имени и значения переменной.

Формат прерываний

Формат пакетов прерываний (Trap) показан на рисунке.



Формат Trap PDU

Тип PDU

Показывает тип пакета (4=Trap).

Предприятие

Идентифицирует компанию-производителя, для которой определено данное прерывание.

Адрес агента

IP-адрес агента, используемый для дальнейшей идентификации.

Базовый тип прерывания

Поле описания события:

0 coldStart: передающий элемент протокола был реинициализирован с изменением конфигурации агента или реализации объекта.

1 warmStart: передающий элемент протокола был реинициализирован без изменения конфигурации агента или реализации объекта.

2 linkDown: сбой в коммуникационном канале.

3 linkUp: коммуникационный канал восстановлен.

4 authenticationFailure: агент получил от менеджера сообщение SNMP с некорректной аутентификацией (неверное имя сообщества).

5 egpNeighborLoss: Сосердний партнер EGP не работает (down).

6 enterpriseSpecific: произошло отличное от базового прерывание, идентифицированное полями Specific Trap Type (Конкретный тип прерывания) и Enterprise (Предприятие).

Конкретный тип прерывания

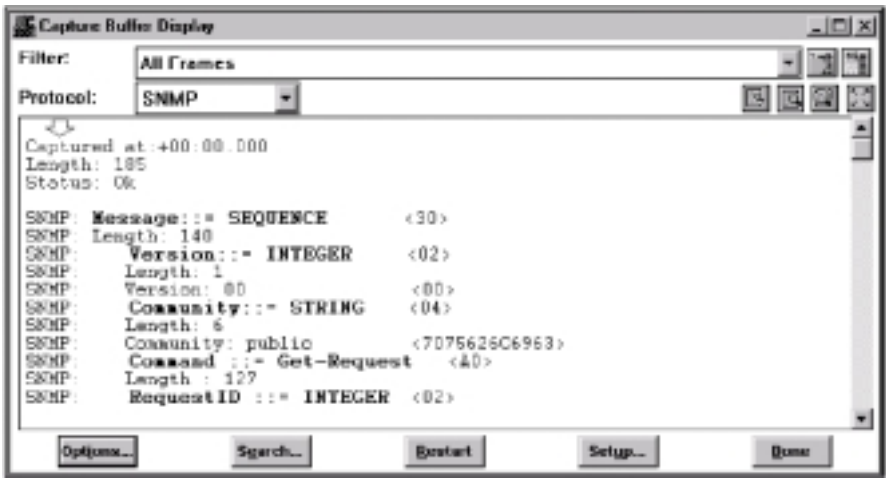
Используется для идентификации отличных от базовых прерываний при установке в поле Generic Trap Type (Базовый тип прерывания) значения enterpriseSpecific.

Временная метка

Значение переменной sysUpTime для объекта, представляющее промежуток времени между последней (ре)инициализацией и генерацией данного прерывания.

Объект/значение

Связанная пара имени и значения переменной.



Пример декодирования SNMP

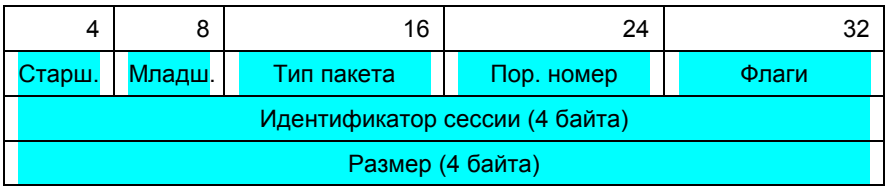
TACACS+

draft *http://info.internet.isi.edu:80/in-drafts/files/draft-grant-tacacs-02.txt*

RFC1492 *http://www.cis.ohio-state.edu/htbin/rfc/rfc1492.html*

Протокол TACACS+ обеспечивает управление доступом для маршрутизаторов, сетевых серверов доступа и других устройств на базе одного или нескольких централизованных серверов, выполняя операции аутентификации, авторизации (проверки полномочий) и ведения учета.

Формат заголовков TACACS+ показан на рисунке.



Структура заголовка TACACS+

Старшие цифры версии

Старшие цифры номера версии протокола TACACS+.

Младшие цифры версии

Младшие цифры номера версии протокола TACACS+. Это поле используется для обеспечения обратной совместимости между различными вариантами протокола TACACS+.

Packet type

Пакеты TACACS+ могут быть следующих типов:

TAC_PLUS_AUTHEN:= 0x01 (Authentication - аутентификация).

TAC_PLUS_AUTHOR:= 0x02 (Authorization - проверка полномочий).

TAC_PLUS_ACCT:= 0x03 (Accounting - ведение учета).

Sequence number

Порядковый номер данного пакета в текущем сеансе. Первый пакет TACACS+ в сеансе должен иметь номер 1, а номера последующих пакетов должны увеличиваться на единицу. Таким образом клиент может передавать только пакеты с нечетными номерами, а демоны TACACS+ - с четными.

Флаги

Битовая маска флагов, указывающих режим шифрования пакетов.

Идентификатор сессии

Идентификатор текущего сеанса TACACS+.

Размер

Общий размер тела пакета TACACS+ (без учета заголовка).

TELNET

RFC854 http://www.cis.ohio-state.edu/htbin/rfc/rfc854.html

RFC855 http://www.cis.ohio-state.edu/htbin/rfc/rfc855.html

RFC857 http://www.cis.ohio-state.edu/htbin/rfc/rfc857.html

TELNET представляет собой протокол эмуляции терминала в стеке TCP/IP. Современные варианты TELNET обеспечивают эмуляцию практически всех функций терминалов различных типов, разработанных в течение последних 20 лет. Набор опций позволяет протоколу TELNET поддерживать передачу двоичных данных, макросы, эмуляцию графических терминалов и передачу информации для поддержки централизованного управления терминалами.

TELNET использует транспортный протокол TCP для организации виртуальных соединений между серверами и клиентами. После организации соединения сервер и клиент TELNET входят в фазу согласования параметров, определяющих режим работы каждой из сторон соединения. В течение сеанса любая из сторон может заново инициализировать старые параметры или согласовать новый набор параметров. В общем случае каждая сторона TELNET-соединения пытается реализовать максимально возможный набор поддерживаемых опций.

В типовой реализации клиент TELNET посылает информацию о нажатии клавиш, в ответ на которую сервер TELNET может передать один или несколько символов. При использовании опции Echo (эхо) сервер TELNET передает клиенту символы, соответствующие нажатиям клавиш на стороне клиента TELNET.

Динамическое согласование режима

Во время соединения пользователем или программой могут быть согласованы дополнительные опции, отличающиеся от опций, предлагаемых NVT. Эта задача выполняется с помощью команд, вложенных в поток передаваемых данных. Коды команд TELNET имеют размер в один или несколько октетов, перед которым располагается символ IAC (interpret as command - интерпретировать как команду), имеющий значение FF (все биты имеют значение 1). Коды команд TELNET перечислены ниже:

Команда	***Код***		***Описание***
	Dec	***Hex***	
data			ввод-вывод данных.
End subNeg	240	FO	завершение команды дополнительного согласования (subnegotiation) опций.
No Operation	241	F1	нет операции.
Data Mark	242	F2	завершение неотложного потока данных.
Break	243	F3	оператор нажал клавишу Break (стоп) или Attention (внимание).

Int process	244	F4	прервать текущий процесс.
Abort output	245	F5	отказ от вывода текущего процесса.
You there?	246	F6	подтверждение запроса.
Erase char	247	F7	запрос на удаление предыдущего символа.
Erase line	248	F8	запрос на удаление предыдущей строки.
Go ahead!	249	F9	завершение ввода для полудуплексного соединения.
SubNegotiate	250	FA	начало дополнительного согласования (subnegotiation) опций.
Will Use	251	FB	согласие на использование указанной опции.
Won't Use	252	FC	отказ от предложенной опции.
Start use	253	FD	отказ от начала использования указанной опции.
Stop Use	254	FE	запрос на прекращение использования указанной опции.
IAC	255	FF	интерпретировать как команду.

Каждая согласуемая опция имеет идентификатор, следующий непосредственно за командой согласования опции (IAC, команда, код опции). Ниже приведен список кодов опций TELNET:

ID		***Коды***	***Описание***
Dec	***Hex***		
0	0	Binary Xmit	разрешить передачу бинарных данных.
1	1	Echo Data	заставляет сервер передавать эхо-символы.
2	2	Reconnect	подключение к другому хосту TELNET.
3	3	Suppress GA	запрет команды Go Ahead!.
4	4	Message Sz	указывает приблизительный размер сообщения.
5	5	Opt Status	перечисляет состояния опций.
6	6	Timing Mark	маркирует положение в потоке данных для ссылок.
7	7	R/C XmtEcho	удаленное управление терминальными принтерами.
8	8	Line Width	установка ширины строки вывода.
9	9	Page Length	установка числа строк на странице вывода.
10	A	CR Use	определяет обработку символов возврата каретки.
11	B	Horiz Tabs	устанавливает горизонтальную табуляцию.
12	C	Hor Tab Use	определяет обработку символов горизонтальной табуляции.
13	D	FF Use	определяет обработку символов перевода страницы.
14	E	Vert Tabs	устанавливает вертикальную табуляцию.

15	F	Ver Tab Use	определяет обработку символов вертикальной табуляции.
16	10	Lf Use	определяет обработку символов перевода строки.
17	11	Ext ASCII	определяет расширенные символы ASCII.
18	12	Logout	разрешает форсированный выход (log-off).
19	13	Byte Macro	определяет байтовый макрос.
20	14	Data Term	разрешает передавать субкоманды для Data Entry.
21	15	SUPDUP	позволяет использовать протокол отображения SUPDUP.
22	16	SUPDUP Outp	позволяет передавать вывод SUPDUP.
23	17	Send Locate	позволяет передавать местоположение терминала.
24	18	Term Type	разрешает обмен информацией о типе терминала.
25	19	End Record	разрешает использовать код завершения записи (End of record - 0xEF).
26	1A	TACACS ID	используется обмен идентификаторами пользователей для предотвращения множественного входа в систему (log-in).
27	1B	Output Mark	позволяет передавать на устройство вывода баннерные маркеры.
28	1C	Term Loc#	для идентификации терминала используется цифровое значение (numeric ID).
29	1D	3270 Regime	разрешает эмуляция семейства терминалов 3270.
30	1E	X.3 PAD	разрешает использование эмуляции протокола X.3.
31	1F	Window Size	передает размер окна для экрана эмуляции.
32	20	Term Speed	передает информацию о скорости.
33	21	Remote Flow	обеспечивает управление потоком (XON, XOFF).
34	22	Linemode	поддержка транзакций linemode bulk character.
255	FF	Extended options list список расширенных опций.	

X-Window

RFC1013 http://www.cis.ohio-state.edu/htbin/rfc/rfc1013.html

Протокол X-Window обеспечивает удаленный оконный интерфейс для распределенных сетевых приложений. Это протокол уровня приложений, использующий в качестве транспортного протокола TCP/IP или DECnet.

Сетевой протокол X-Window основан на архитектуре клиент-сервер, где сервер представляет собой управляющую программу на рабочей станции пользователя, а клиентские приложения могут размещаться в любом месте сети. Управляющая программа X-сервер на рабочей станции пользователя может одновременно поддерживать множество окон для различных сетевых приложений с асинхронным обновлением содержимого окон в соответствии с информацией протокола X-Window.

Для обеспечения взаимодействия пользователя с удаленными приложениями программа X-сервер на станции пользователя генерирует события в ответ на действия пользователей (нажатие клавиш или работа с мышью). При отображении множества приложений система передает событияприложению, связанному с активным в настоящий момент окном. В некоторых случаях приложения могут также генерировать события, передаваемые управляющей программе X-сервер.

Кадры запросов и откликов

В запросах и откликах могут использоваться следующие команды:

Команда	***Описание***
BackRGB	Фоновый цвет в форме значений красной, зеленой и синей компонент.
BackPM	Пиксельная маска (Pixel map) фона.
BellPitch	звуковой сигнал (Bell pitch).
BellVol	Уровень звукового сигнала в процентах.
BM	Битовая маска отображаемого элемента.
BordPM	Маска границы (Border pixel map), используемая для окна.
b	Ширина границы отображаемого элемента.
Click	Уровень звука при нажатии клавиш в процентах.
Ord	Click order. Drawable clip order - <Unsorted>, <Y-sorted>, <YX-sorted> или <YX-banded>.
CMap	Отображение цветов (Color map) для рисуемых элементов.
CID	Идентификатор контекста (Context ID) для частного графического контекста.
Cur	Курсор - код цвета курсора
d	Текущая глубина окна.
DD	Отображаемый элемент (Destination drawable) в виде растра.

D	Отображаемый элемент (Drawable) - код, служащий для идентификации окна или растра.
Exp	Отображаемый элемент (Exposure), выводимый в настоящее время.
Fam	Используемое семейство протоколов (Internet, DECnet, CHAOSnet).
Font	Код, используемый для идентификации шрифта.
Font(a,d)	Вертикальные границы шрифта (Font ascent/descent).
ForeRGB	Цвет вывода (Foreground color) в форме красной, зеленой и синей компонент.
Fmt	Формат текущего окна.
GC	Графический контекст - код, используемый для идентификации частного графического определения.
h	Высота отображаемого элемента.
Key	Код клавиши.
KeySym	Код, служащий для обозначения семейства используемых кодов клавиш.
MinOp	Рабочий код X-Windows (младшая часть).
MajOp	Рабочий код X-Windows (старшая часть).
N	Число отображаемых элементов списка.
P	Родительское окно текущего окна.
PixMap	Растр - код используемый для идентификации фрагмента растра.
p	Плоскость - используемая битовая плоскость.
PM	Маска битовой плоскости, связанной с отображаемым элементом.
Prop	Принадлежность (Property) - указывает принадлежность окна.
SW	Дочернее окно, произведенное данным окном.
SD	Отображаемый элемент в форме растровой копии.
T/O	Время активизации программы сохранения экрана (Screen saver).
Typ	Тип текущего окна.
w	Ширина отображаемого элемента.
W	Окно - код используемый для идентификации частного окна.
X	X-координата для отображаемого элемента.
Y	Y- координата для отображаемого элемента.

Кадры событий

Кадры событий могут содержать следующие команды:

Команда	***Описание***
Btn	Нажата числовая клавиша.
C	Дочернее окно, связанное с событием.
F	Флаги событий - набор флагов отображаемых символами верхнего (активный флаг) или нижнего (неактивный флаг) регстра:

	f,F	фокус вода относится к событию.
	s,S	события на одном экране.
E(x,y)	Местоположение события - координаты X и Y, связанные с событием.	
E	Окно, в котором произошло событие.	
Key	Номер нажатой клавиши.	
O	Владелец окна, связанного с событием.	
R	Корневое окно, связанное с событием.	
R(x,y)	Координаты X и Y для корневой позиции.	
SN	Порядковый номер последовательных событий.	