Лекция 5. ПРОТОКОЛЫ СЕТЕВОГО УРОВНЯ (IP, ICMP, DHCP)

Основные положения

1. Протокол IP

Протокол IPv4 (Internet Protocol) работает на сетевом уровне стека TCP\IP. Он предназначен для передачи данных между хостами по составной сети, но при использовании стека TCP\IP используется для связи хостов и в локальной сети.

Протокол IP маршрутизируемый, то есть его сообщения могут быть перенаправлены от одного узла к другому, используя IP адреса. IP адрес представляет собой уникальный идентификатор сетевого устройства. С помощью данного идентификатора пакеты доставляются конечным узлам и определяется оптимальный маршрут прохождения пакета.

Протокол IP – дейтаграммный, то есть не обеспечивает надежность доставки данных.

Протокол IP может инкапсулировать:

a. Протоколы транспортного уровня TCP или UDP
b. Протоколы сетевого уровня ICMP и DHCP
c. Пакеты протокола IP (для организации туннелей)
d. И т.д.

В сетях общего назначения используются два протокола IPv4 и IPv6.

2. Заголовок IPv4

<table>
<tr><td>Версия (4 бита)</td><td>IHL(4 бита)</td><td>Тип обслуживания (8 бит)</td><td colspan="2">Длина пакета(16 бит)</td></tr>
<tr><td colspan="3">Идентификатор(16 бит)</td><td>Флаги(3 бита)</td><td>Смещение фрагмента</td></tr>
<tr><td colspan="2">Время жизни(8 бит)</td><td>Протокол(8 бит)</td><td colspan="2">Контрольная сумма заголовка</td></tr>
<tr><td colspan="5">IP-адрес отправителя (32 бита)</td></tr>
<tr><td colspan="5">IP-адрес получателя (32 бита)</td></tr>
<tr><td colspan="5">Параметры (от 0 до 10-ти 32-х битных слов)</td></tr>
<tr><td colspan="5">Данные (до 65535 байт минус заголовок)</td></tr>
</table>

Заголовок IPv4

Версия (Version) - для ip-протокола версии 4 значение поля должно быть равно 4.

IHL - длина заголовка IP-пакета в 32-битных словах (dword), указывающая начало блока данных в пакете.

Тип обслуживания (Type of Service) - байт, содержащий информацию о типе обслуживания IP-пакетов.

Длина пакета (Total Lenght) – поле указывающее общую длину пакета в байтах.

Идентификатор (ID) - значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке датаграммы. Для фрагментированного пакета все фрагменты имеют одинаковый идентификатор.

Флаги (Flags) - первый бит всегда равен нулю, второй бит определяет возможность фрагментации пакета и третий бит показывает, не является ли этот пакет последним в цепочке пакетов.

Смещение фрагмента (Fragment Offser) - значение, определяющее позицию фрагмента в потоке данных.

Время жизни (Time To Live) – параметр, определяющий время существования пакета в сети. Представляет собой численное поле в заголовке пакета, значение которого уменьшается при прохождении очередного маршрутизатора минимум на единицу, если передача данных через устройство заняла больше времени, то на величину этой задержки. Если значения этого поля равно нулю то, пакет должен быть отброшен.

Протокол (Protocol) - идентификатор интернет-протокола следующего уровня указывает, данные какого протокола содержит пакет, например, TCP или ICMP.

Контрольная сумма заголовка(Header Checksum) - контрольная сумма заголовка пакета. Пересчитывается каждый раз при смене заголовка - например, если он проходит через очередной маршрутизатор.

Адрес отправителя (Source Address) - IP-адрес источника, отославшего пакет.

Адрес получателя (Destination Address) - IP-адрес назначения, куда был послан пакет.

Поле опций (Options) – необязательное поле, задающее дополнительные параметры пакета.

3. Изменение заголовка пакета IPv4 при прохождении маршрутизатора

При прохождении маршрутизатора уменьшается поле Время жизни.

Но поле «Контрольная сумма» также рассчитывается по всему заголовку с использованием операций сложения 16-разрядных слов заголовка по модулю 1. Следовательно оно тоже будет пересчитываться при прохождении маршрутизатора пакета IPv4. Кроме того, поле контрольной суммы будет меняться при:

a. Фрагментации (см. далее)
b. Трансляции адресов
c. Изменения поля опций
d. И любой иной модификации заголовка пакета.

Таким образом продвижение пакета IPv4 связано со значительными вычислительными затратами.

4. Тип обслуживания IPv4

Восьмибитное поле тип сервиса (TOS - type of service) показывает то, как должна обрабатываться дейтограмма. Интерпретация поля со временем менялась.

Изначально применялся RFC 1349. По нему:

a. Первые два бита определяли приоритет (0 Обычный уровень, 1 Приоритетный, 2 Немедленный, 3 Срочный, 4 Экстренный, 5 ceitic/ecp, 6 Межсетевое управление, 7 Сетевое управление)
b. Далее шли четыре однобитовых флага (D=1 требует минимальной задержки, T=1 - высокую пропускную способность, R=1 - высокую надежность, а C=1 - низкую стоимость)
c. Восьмой бит не использовался.

В настоящее время используется RFC-2474, по которому поле TOS содеражательно заменено на байт DS (Differentiated Services).

Биты DS0-DS5 определяют селектор класса. Стандартным значением DSCP по умолчанию является 000000.

Если точнее, то:

a. Первые 3 бита определяют селектор класса
b. Следующие 3 бита определяют приоритет отбрасывания пакета в случае перегрузки

Последние 2 бита поля по RFC 3168 используются для передачи значения Explicit Congestion Notification (ECN), которым можно передать признак появления «затора» на маршруте.

5. Фрагментация IPv4

Фрагментация IP это попытка решить проблему разных MTU (Maximum transmission unit) - максимальной длины пакета в разных локальных сетях, входящих в составную сеть, по которой идет пакет.

Предполагалось, что произойдет разбиение дейтаграммы на множество частей, которые могут быть повторно собраны позже. Каждая из частей содержит свой фрагмент исходного поля данных и снабжается своим заголовком.

Для IP-фрагментации и повторной сборки используются поля из IP заголовка:

a. Идентификатор;
b. Полная длина;
c. Смещение фрагмента;
d. Флаги фрагментации:
   Бит 1 – не используется
   Бит 2 – НеФрагментировать
   Бит 3 – ЕстьЕщеФрагменты

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

IP Fragments (Ethernet)

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

Первый фрагмент имеет смещение 0, длина этого фрагмента - 1500; она включает 20 байтов для измененного оригинального IP заголовка.

Второй фрагмент имеет смещение 185 (185 x 8 = 1480), которое означает, что порция данных этого фрагмента начинается с 1480 байта в оригинальной IP дэйтаграмме. Длина этого фрагмента - 1500; она включает дополнительный IP заголовок, созданный для этого фрагмента.

Третий фрагмент имеет смещение 370 (370 x 8 = 2960), которое означает, что данные этого фрагмента начинаются с 2960 байта в оригинальной IP дэйтаграмме. Длина этого фрагмента - 1500; она включает дополнительный заголовок IP, созданный для этого фрагмента.

Четвертый фрагмент имеет смещение 555 (555 x 8 = 4440), которое означает, что часть данных этого фрагмента начинается с 4440 байтов в оригинальной IP дэйтаграмме. Длина этого фрагмента - 700 байтов.

Если добавить байты данных от последнего фрагмента (680 = 700 - 20), это даст 5120 байтов, что является порцией данных оригинальной IP дэйтаграммы. Затем, добавляя 20 байтов для IP заголовка мы получим размер оригинальной IP дэйтаграммы (4440 + 680 + 20 = 5140).

6. Поле опций IPv4

Поле опций является необязательным и используется для управления и диагностики.

Стандартными являются первые 2 байта. Первый байт содержит поля управляющие работой поля опций (бит признака копирования опций в фрагменты, класс и код опции). Второй байт содержит длину поля опций. Потом идет поле данных опций.

Например: класс опции = 0, номер опции=7. Это значит, что в поле данных опции будут записываться IP адреса промежуточных узлов при передаче.

7. Предпосылки перехода на IPv6

Уже в 1996 году началась разработка IPv6, так как уже тогда было понятно, что IPv4 имеет ряд недостатков. Предпосылками перехода является:

a. Нехватка адресов IPv4 (последняя сеть /8 была передана для распределения в 2011 году),
b. накопившаяся критика в адрес IPv4 (частая модификация заголовка, наличие трансляции адресов, медленный механизм фрагментации и др.),
c. развитее 4G/5G, которая ориентирована исключительно на IPv6, развитие IoT,
d. стремление восстановить полную связанность в сети,
e. стремление провести рефакторинг служебных протоколов,
f. стремление снизить анонимность в сети.

8. Основные сущности IPv6

Узел - оборудование, использующее IPv6.

Маршрутизатор - узел, который переадресует пакеты IPv6, которые не адресованы ему непосредственно.

Канал - средство коммуникации или среда, через которую узлы могут взаимодействовать друг с другом на связном уровне, т.е., уровень непосредственно под IPv6. Примерами могут служить Ethernet; PPP; X.25, Frame Relay, или ATM; а также Интернет "туннели", такие как туннели поверх IPv4 или IPv6.

Соседи - узлы, подключенные к общему каналу.

Интерфейс - средство подключения узла к каналу.

MTU канала - максимальный размер пакета в канале

MTU пути - минимальный MTU канала для пути от узла источника до получателя.

9. Заголовок IPv6

В протоколе IPv6 формат заголовка упрощен и существенно переработан.

<table>
<tr><td>Версия (4 бита)</td><td>Класс трафика (8 бит)</td><td colspan="2">Маркер потока (20 бит)</td></tr>
<tr><td colspan="2">Длина полезной нагрузки (16 бит)</td><td>Следующий заголовок (8 бит)</td><td>Предел перехода (8 бит)</td></tr>
<tr><td colspan="4">Адрес отправителя (128 бит)</td></tr>
<tr><td colspan="4">Адрес получателя (128бит)</td></tr>
</table>

Версия: поле, содержащее 4-битное двоичное значение, которое определяет версию IP-пакета. Для пакетов IPv6 в этом поле всегда указано значение 0110.

Класс трафика: 8-битное поле, соответствующее полю «Дифференцированные сервисы (DS)» в заголовке IPv4. Оно также содержит 6-битное значение точки кода дифференцированных сервисов (DSCP), которое используется для классификации

пакетов, а также 2-битное значение явного уведомления о перегрузке (ECN), используемое для управления перегрузками трафика.

Метка потока: 20-битное поле, предоставляющее специальную службу для приложений реального времени. Используя это поле, маршрутизаторам и коммутаторам передается информация о необходимости поддерживать один и тот же путь для потока пакетов, что поможет избежать их переупорядочивания.

Длина полезной нагрузки: 16-битное поле, соответствующее полю «Общая длина» в заголовке IPv4. Оно определяет размер всего пакета (фрагмента), включая заголовок и дополнительные расширения.

Следующий заголовок: 8-битное поле, соответствующее полю «Протокол» в заголовке IPv4. Оно указывает тип полезной нагрузки данных, которые переносит пакет, что позволяет сетевому уровню пересылать данные на соответствующий протокол более высокого уровня. Это поле также используется в тех случаях, когда в пакет IPv6 добавляются дополнительные заголовки расширений.

Предел перехода: 8-битное поле, заменяющее поле «Время существования» (TTL) в IPv4. Это значение уменьшается на единицу каждым маршрутизатором, пересылающим пакет. Когда счетчик достигает 0, пакет отбрасывается, и на отправляющий узел пересылается сообщение ICMPv6, которое означает, что пакет не достиг своего назначения.

Адрес источника: 128-битовое поле, определяющее IPv6-адрес принимающего узла.

Адрес назначения: 128-битное поле, определяющее IPv6-адрес принимающего узла.

10. Служебный протокол DHCP

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла). Предназначен для автоматического конфигурирования сетевого узла. В качестве конфигурационных параметров могут быть переданы: IP, mask, gate, адреса DNS, адрес сервера загрузки, сервера времени и т.п. Как правило клиентов идентифицируют по MAC адресу, к которому привязывается назначенный IP. Адреса вделаются из специального диапазона – пула адресов.

С точки зрения протокола DHCP адрес может быть назначен:

a. Динамически – из пула на время аренды, по истечении времени аренды происходит повторный запрос для обновления времени аренды.
b. Вручную – из пула вручную, по заранее определённой записи.
c. Статически – из пула, автоматически на навсегда.

В любом случае DHCP-клиент запрашивает через широковещание (для IPv4) или через мультикаст (для IPv6) сервис (сообщение DHCP-discover). Все доступные DHCP сервера сообщают о готовности предоставить конфигурацию (DHCP-offer). Клиент выбирает подходящий сервер и шлет ему запрос на конфигурацию (DHCP request). После сервер передает конфигурацию серией пакетов (DHCP-ACK).

11. Служебный протокол ICMP

ICMP (англ. Internet Control Message Protocol — протокол межсетевых управляющих сообщений). Является диагностическим протоколом стека TCP\IP. Предназначен для запроса и оповещении о состояниях связи по протоколу IP и TCP, UDP. При передаче инкапсулируется в IP. Оповещение реализовано конечным количеством кодов запроса и кодов ответа. Пример ответов: код 3 — Порт недостижим, код 5 —

Неверный маршрут от источника. Пример запросов: 8 — Эхо-запрос, 30 — Трассировка маршрута (RFC-1393).
Пакет ICMP инкапсулируется в IP пакет.
Заголовок ICMP пакета содержит поле Код (1 байт) и Тип (1 байт). Их комбинация управляет работой протокола. Например, если при передаче IP пакета оказывается недоступным порт, то отправителю будет выслано ICMP сообщение с Типом 3 и Кодом 3. Тип 8 Код 0 советуют эхо-запросу (команда ping), а тип 0 код 0 – эхо ответу.

Основные термины

1. Узел – сетевое устройство, подключенное к сети и имеющее MAC адрес и один или несколько IP адресов.
2. Хост – узел, на котором работают приложения протоколов прикладного уровня
3. Маршрутизатор – устройство, осуществляющее пересылку пакетов между сетями на основании IP адресов получателя в заголовке пакета и таблиц маршрутизации
4. Фрагментация – процесс разбиения IP пакета на пакеты меньшей длинны.
5. TOS – type of service – тип обслуживания для передачи пакета.
6. Дейтаграмма – сообщение не требующее подтверждение приема.
7. RCF - Request for Comments — пронумерованными документами, содержащими технические спецификации и стандарты TCP\IP, управляемые IETF (Internet Engineering Task Force).

Дополнительная литература

1. https://www.rfc-editor.org
2. http://rfc.com.ru
3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020 г.
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2019 г.