Лекция 5. СОЕДИНЕНИЕ IP СЕТЕЙ

Основные положения

1. **Построение составных сетей в TCP\IP**

   Стек TCP\IP изначально создавался для построения крупных сетей, в состав которых входят локальные сети с разнообразными канальными протоколами.

   Принципы работы канальных протоколов могут различаться, но наличие общего сетевого уровня позволяет узлам сети взаимодействовать друг с другом.

   Можно выделить два типа соединения локальных сетей в составную сеть:

   a. Маршрутизация
   b. Трансляция адресов.

2. **Маршрутизация**

   Маршрутизация является основным способом соединения сетей по протоколу IP, причем как для IPv4, так и для IPv6.

   Маршрутизация основана на следующих положениях:

   a. каждый узел в сети имеет уникальный IP адрес;
   b. каждая локальная сеть имеет свой уникальный IP адрес;
   c. все узлы обладают возможностью организации end-to-end связи, то есть прямого взаимодействия на сетевом уровне;
   d. топология сети может быть сложносвязанной;
   e. локальные сети соединены специальным оборудованием – маршрутизаторами;
   f. на маршрутизаторах есть информация о путях передачи пакетов до целевой сети;
   g. маршрутизатор обрабатывает каждый IP пакет отдельно.

   К задачам маршрутизации относятся:

   a. Обработка пакетов при передаче (передача от входного к выходному интерфейсу маршрутизатора);
   b. Определение того, как направлять пакеты (сбор и упорядочивание маршрутной информации).

   Информация о маршрутах хранится в особых структурах – таблицах маршрутизации.

   Выбор следующего шага пересылки пакетов маршрутизатор принимает исходя из:

   a. минимизации длины маршрута (длина пути по графу, нагруженному или не нагруженному),
   b. балансировки нагрузки,
   c. минимизации задержки,
   d. минимизации потери пакетов,
   e. минимизации стоимости.

   Маршрутизация бывает:

   a. статической и динамической;

b. внутренней и внешней.

Статическая маршрутизация предполагает, что инженер составляет таблицы маршрутизации вручную. При динамической маршрутизации – таблицы маршрутизации составляются автоматически с помощью специальных протоколов маршрутизации.

Внутренняя маршрутизация – это динамическая маршрутизация внутри автономных систем, внешняя – динамическая маршрутизация между автономными системами.

3. Таблицы маршрутизации

Таблица маршрутизации — структура данных, хранящаяся на маршрутизаторе или сетевом компьютере, описывающая соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации.

Таблица маршрутизации обычно содержит:

a. адрес сети или узла назначения, либо указание, что маршрут является маршрутом по умолчанию
b. маску сети назначения (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети)
c. шлюз, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения
d. интерфейс (в зависимости от системы это может быть порядковый номер, GUID или символьное имя устройства)
e. метрику — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

Маршрут может быть написан на сеть, на хост (это определяется или флагом или маской 255.255.255.255 или /128).

Маршрут с адресом назначения 0.0.0.0 и маской 0.0.0.0 – маршрут по умолчанию.

4. Порядок обработки таблицы маршрутизации

При определении маршрута маршрутизатор берет IP-адрес получателя в IP пакете и ищет для него сначала маршрут на этот хост, потом на сеть, в которую входит IP назначения, потом, если маршрутов не найдено, используется маршрут по умолчанию, а если его нет – пакет сбрасывается. Отправителю обычно отправляется ICMP сообщение об ошибке.

5. Динамическая маршрутизация на примере RIP2

Типичным протоколом внутренней маршрутизации является RIP2. Это протокол дистанционно-векторного типа. Маршрутизаторы рассылают свою таблицу маршрутизации соседям.

Принимая маршрутную запись маршрутизатор заменяет поле порт – на тот свой порт, через который получена таблица, а в поле шлюз вписывает IP с которого была получена запись. Метрика увеличивается на единицу.

Метрика в RIP2 считается в количестве промежуточных маршрутизаторов. То есть вес ребра = 1. Максимальное значение метрики = 16. Если метрика = 16 то маршрут считается недоступным. Т.о. если маршрутизатор определяет, что маршрут более не доступен, то метрика на этот маршрут принимается = 16 и при получении этой записи маршрутизаторы-соседи удаляют этот маршрут.

При всей его простоте, протокол RIP2 имеет ряд недостатков:

a. Простая метрика, не учитывающая канальную скорость локальной сети,
b. Возможность появление маршрутных петель
c. Ограниченная длина маршрута.

Следует отметить, что современный протокол RIP2 содержит ряд опций, которые позволяют практически исключить возникновение ложных маршрутов. К ним относятся методы триггерных обновлений, расщепления горизонта и др.

6. Трансляция адресов (NAT)

Трансляция адресов NAT – является типичной технологией для IPv4. Для IPv6 существуют RFC для трансляции адресов, но они решают частные задлачи и не соответствуют общей идеологии IPv6. По этой причине мы будем рассмаривать только NAT для IPv4.

Существует три основных режима работы NAT:

a. публикация адреса
b. клиентский NAT
c. публикация порта.

В независимости от режима работы NAT предполагает, что внутреннюю сеть с «серыми» IP соединяет с Интернет шлюз-транслятор, подключенный к внешней сети, например к Интернет. Технически это может быть программный или аппаратный маршрутизатор.

7. NAT. Публикация адреса

Публикация адреса — это режим, предназначенный для предоставления сервиса «белого» IP клиенту в локальной сети за шлюзом.

Все исходящие пакеты модифицируются, в них меняется «серый» IP адрес отправителя из локальной сети на «белый» IP, закреплённый за клиентом.

Входящие пакеты, направленные на этот, закреплённый, адрес тоже модифицируются – адрес назначения меняется на внутренний «серый» адрес, и после этого пакет передается в локальную сеть за шлюзом.

8. Клиентский NAT

Клиентский NAT предназначен для подключения множество абонентов к внешней сети через один шлюз. В этом случае в исходящем пакете меняется не только адрес, но и порт. То есть заменяется сокет исходящего сообщения на новый внешний сокет (внешний IP и порт). Замена сохраняется в

динамической таблице. Уникальность внешнего сокета отправителя гарантирует возможность связи со стороны нескольких внутренних хостов, в случае совпадения на них портов отправителя. Ответные пакеты модифицируются при передаче в локальную сеть по записи в динамической таблице.

9. **NAT. Публикация порта**

   В случае клиентского NAT соединение можно установить только изнутри. Если нужно установить соединение с приложением внутри локальной сети, то на шлюзе публикуется порт приложения с помощью статического назначения локального сокета и внешнего сокета. В этом случае все входящие сообщения на внешний сокет модифицируются и направляются в локальную сеть на локальный сокет. Ответы идут с обратной модификацией. Можно публиковать порты для различных локальных хостов. Для внешнего наблюдателя все будет выглядеть так, как будто все сервисы работают на компьютере с IP шлюза.

Основные термины

1. Автономная система (AS) в интернете — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом (RFC 1930)
2. Маршрутизатор – устройство, осуществляющее пересылку пакетов между сетями на основании IP адресов получателя в заголовке пакета и таблиц маршрутизации.
3. NAT – Network Address Translation – технология модификации заголовков сетевого и транспортного уровней для соединения сетей без непрерывного пространства IP адресов.
4. 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.