

Конспект по курсу Сети ¹

Александра Лисицына ²

29 ноября 2019 г.

¹Читаемый в 2019-2020 годах

²Студентка группы М3435

Оглавление

1	Введение	2
1.1	Модель OSI	2
1.1.1	Прикладной уровень (application layer)	2
1.1.2	Уровень представления данных (presentation layer)	2
1.1.3	Сеансовый уровень (session layer)	2
1.1.4	Транспртный уровень (transport layer)	3
1.1.5	Сетевой уровень (network layer)	3
1.1.6	Канальный уровень (data link layer)	3
1.1.7	Физический уровень (physical layer)	3
1.1.8	Взаимодействие сетевого канального уровня	3
2	Lecture 2	5
2.1	Физический и канальный уровни корпоративных сетей	5
2.2	Соединение IP сетей	5
2.2.1	Виды маршрутизации	5
2.2.2	NAT (Network Address Translation)	5

Глава 1

Введение

1.1 Модель OSI

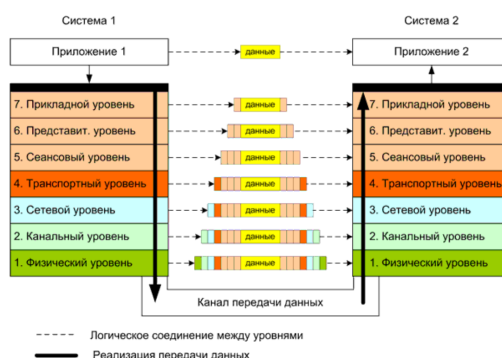


Рис. 1.1:

1.1.1 Прикладной уровень (application layer)

Основные функции:

- Передача служебной информации приложений
- Предоставляет приложениям информацию об ошибках

Примеры протоколов: **FTP** (File Transfer Protocol), **Telnet** (TErminaL NETwork), **HTTP** (HyperText Transfer Protocol), **POP3** (Post Office Protocol Version 3), **SMTP** (Simple Mail Transfer Protocol).

1.1.2 Уровень представления данных (presentation layer)

Основные функции:

- Сжатие данных
- Шифрование данных
- Перекодировка данных

Примеры протоколов: **SSL** (Secure Socket Layer), **RDP** (Remote Desktop Protocol).

1.1.3 Сеансовый уровень (session layer)

Основные функции:

- Обеспечивает установление, поддержание и завершение сеанса связи, позволяя приложениям взаимодействовать между собой длительное время

Примеры протоколов: **L2TP** (Layer 2 Tunneling Protocol), **NetBIOS** (Network Basic Input Output System), **PAP** (Password Authentication Protocol), **PPTP** (Point-to-Point Tunneling Protocol), **RPC** (Remote Procedure Call Protocol).

1.1.4 Транспортный уровень (transport layer)

Основные функции:

- Обеспечивает надёжную доставку данных, подтверждение приёма и сегментацию потока, получаемого от транспортного уровня

Примеры протоколов: **TCP** (Transmission Control Protocol), **UDP** (User Datagramm Protocol).

1.1.5 Сетевой уровень (network layer)

Основные задачи:

- Решает задачу доставки данных по составной сети, межсетевую адресацию, трансляцию физических адресов в сетевые.

Примеры протоколов: **IP/IPv4/IPv6** (Internet Protocol), **IPX** (Internetwork Packet Exchange), **IPsec** (Internet Protocol Security), **ICMP** (Internet Control Message Protocol), **RIP** (Routing Information Protocol), **OSPF** (Open Shortest Path First), **ARP** (Address Resolution Protocol).

1.1.6 Канальный уровень (data link layer)

Основные задачи:

- Обеспечивает формирование фреймов (frames) — кадров
- Обеспечивают контроль ошибок и управление потоком данных (data flow control)
- Логическое кодирование данных

Примеры протоколов: **ATM**, **Ethernet**, **EAPS** (Ethernet Automatic Protection Switching), **FDDI** (Fiber Distributed Data Interface), **MPLS** (Multiprotocol Label Switching), **PPP** (Point-to-Point Protocol), **SLIP** (Serial Line Internet Protocol).

1.1.7 Физический уровень (physical layer)

Основные функции:

- Обеспечивает физическое кодирование бит кадра в электрические (оптические) сигналы и передачу их по линии связи
- Определяет тип кабелей и разъёмов, назначение контактов и формат физических сигналов

Примеры протоколов: **IEEE 802.15** (Bluetooth), **IRDA**, **EIA-RS-232**, **EIA-422**, **Ethernet**, **DSL**, **ISDN**, **IEEE 802.11**.

1.1.8 Взаимодействие сетевого канального уровня

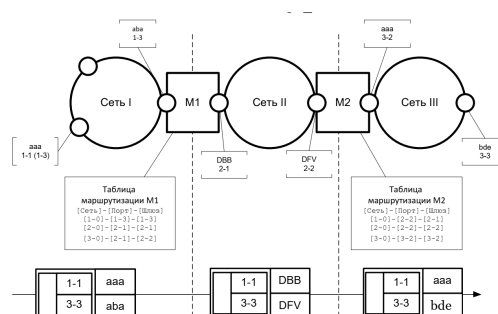


Рис. 1.2:

Замечания:

- В сетях 1 и 3 есть узлы с одинаковыми адресами канального уровня. Это возможно, так как область действия адресации канального уровня — локальная сеть.

- В составной сети адреса сетевого уровня из одной локальной сети должны иметь одинаковую сетевую часть. Это нужно для решения задачи маршрутизации.
- В составной сети адреса сетевого уровня должны быть уникальными.
- За счет процедуры инкапсуляции межсетевое взаимодействие не зависит от природы канальных протоколов в локальных сетях.

Глава 2

Lecture 2

2.1 Физический и канальный уровни корпоративных сетей

Структурированные кабельные системы

2.2 Соединение IP сетей

2.2.1 Виды маршрутизации

Маршрутизацию можно классифицировать двумя способами:

- Статическая и динамическая
- Внешняя и внутренняя

Внешняя необходима для маршрутизации между автономными системами (EGP, BGP).

Внутренняя — внутри одной системы (RIP, OSPF).

OSPF — открытие кратчайшего пути первым. Информации включения/отключения сетей пересылается сразу, по мере появления. По этой информации строится нагруженный граф сети (веса назначаются по таблице в зависимости от скорости линии связи). Маршрут считается по алгоритму Дириха. Быстрее получаем маршрутную информацию, понимаем скорости и быстро перестраиваем при изменении конфигурации. Но его гораздо сложнее настраивать.

Сеть в маршрутизации описывается в виде таблицы маршрутизации.

В TCP/IP мы занимаемся каждым отдельным пакетом. В этом есть минус, так как обычно все пакеты дают один и тот же пакет.

Таблицы маршрутизации строит либо админ, либо протокол маршрутизации.

2.2.2 NAT (Network Address Translation)

Основная причина появления — постоянная нехватка IP адресов.

Не всем хостам нужен IP адрес, а использовать маршрутизацию нельзя.

Цель: обеспечить связь хостов из немаршрутизуемой сети во внешнюю IP сеть.

Виды:

- Публикация адреса
- Клиентский NAT
- Публикация порта

Публикация адреса

Когда: Вы - провайдер домашнего интернета. И один из пользователей вашей сети захотел себе NAS (Network Attached Storage — компьютер с диском, к которому мы ходим из разных мест по разным протоколам), ему нужен реальный IP адрес. Вариант с разделением всей сети масками очень сложен и плох. Поэтому мы делаем подстановку: маршрутизатор провайдера, когда получает пакет на реальный адрес, то меняет его на локальный и посылает по сети, обратно наоборот. Но эта схема работает только, если используется один адрес, для большего количества не работает.

Клиентский NAT

Плюсы: любое количество хостов можем выпустить наружу в интернет через один IP адрес.

Публикация порта

Теперь можно из интернета попасть на устройство. Нам нужен лишь один IP адрес. И обратившись на опубликованный сокет мы попадем на нужное кстройство.

Глава 3

IPv6

3.1 Предпосылки

Нехватка адресов IPv4.

IANA (Internet Assigned) раздает сетки RIR, раньше были /8. Но в 2011 такие сетки закончились. Некоторыми сетками еще располагали RIR'ы.

RIR у которого осталась только одна сетка /8, начал раздавать сетки /22, а это всего 1024 адресов, что естественно быстро исчерпается.

Критика в адрес IPv4:

- Контрольная сумма, на которую просто жадко тратить время, тем более, что она считается в протоколах высших уровней — это просто архаика.
- Фрагментация IP: размер поля данных в каждом канальном протоколе разный, поэтому было решено заниматься фрагментацией.
- Наличие большого количества смежных протоколов
- современные технологии требуют реализации слишком большого числа сессий, работающих параллельно
- развитие IoT
- стремление снизить анонимность в сети

3.2 Проблемы и препятствия

- огромное количество сетей на IPv4
- необходимость адаптации оборудования и системного ПО
- некоторое снижение пропускной способности

3.3 Цели

- расширения адресации
- восстановления end-to-end связность
- спецификация формата заголовков
- улучшенная поддержка расширений и опций
- возможность пометки потоков данных
- идентификация и защита частных обменов
- встроенная поддержка мобильных сетей

3.4 Сравнение IPv4 и IPv6

3.5 Сущности

3.5.1 Формат заголовка

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 "

Длина

Следующий заголовок: 8-битное поле, соотве

Предел перехода: счетчик время жизни.

Адрес источника

Адрес назначения

3.6 Адреса

Правила сокращения записи:

- убираем ведущие нули
- убираем самую длинную последовательность нулей

3.6.1 Типы адресов

- Unicast
- Anycast
- Multicast

3.6.2 Логические части адреса

Вместо масок сетей префиксы

3.6.3 Виды адресов

- Global unicast адрес Аналог адреса
- Link-local
- Loopback
- Unspecified address
- Unique local
- IPv4 embedded
- Multicast

3.6.4 Структура адреса

Префикс выдает IANA

3.7 Конфигурирование узла

- включение узла
- выбор узлом адреса из Link-local
- рассылка на ff01:0:0:0:0:0:1 (все узлы) запроса на возражение
- рассылка на ff01:0:0:0:0:0:2 (все роутеры) запроса на конфигурацию
- получение от ближайшего роутера данных: адрес, длину префикса, MTU, DNS

3.8 Фрагментация в IPv6

Нет фрагментации, когда маршрутизатор не может передать пакет из-за нехватки места в MTU — он сбрасывает пакет и сообщает отправителю о необходимости снизить MTU.

3.9 ICMPv4

3.9.1 ICMPv4 назначение

- ICMP — internet control protocol (протокол сетевого уровня передачи команд и сообщений об ошибках)
- Служебный дейтаграммный протокол

ICMP

- осуществляет передачу отклика на пакет или эхо на отклик;
- осуществляет контроль времени жизни дейтограмм в системе;
- реализует переадресацию пакета;
- выдает сообщение о недостижимости адресата или о некорректности параметров;
- формирует и пересылает временные метки

ICMP-сообщения об ошибках никогда не выдаются в ответ на:

- ICMP-сообщение о невозможности доставки сообщения
- При мультикастинге или широковещательной адресации
- Для фрагмента дейтограммы (кроме первого)
- Для дейтограмм, чей адрес отправителя является нулевым,

3.9.2 Заголовок ICMP

Контрольная сумма считается по заголовку.

3.9.3 Инкапсуляция в Ethernet-кадр

3.9.4 Тип и Код в ICMPv4

3.9.5 ICMP утилиты

- ping Посылает эхо-реплаи и эхо-реквест
- tracert Собирает статистику о передачи трафика между узлами
- traceroute
- pathping
- mtr ping + tracerout

3.9.6 ICMPv4 -> ICMPv6

ICMPv6 нужен:

- для оптимизации
- для реализации идей IPv6

3.9.7 ICMPv6 назначение

- ICMPv6 часть IPv6
- RFC 4443, 2710
- Код следующего заголовка = 58
- Тот же формат заголовков что и ICMP
- Заменяет собой
 - ICMP
 - ARP
 - DHCP
 -

3.9.8 Neighbor Discovery

Вместо ARP:

- 135 Neighbor Solicitation (запрос канального адреса)

SNMA

Solicited-node multicast address — группа узлов для которых ip6 адрес заканчивается на одинаковые 24 бита.

- ff02::1::ff00:0/104
 - ff — мультикаст, 02 — в нашум канале
- 24 бита из-за структуры MAC адреса
 - MAC 00:AA:00:28:9C:5A OUI-VID
 - LinkLocal fe80::2aa:ff:fe28:9c5a EUI-64
 - SNMA ff02::1:ff28:9c5a
 - MAC 33:33:ff:28:9c:5a

3.9.9 Определение MAC in ICMPv6

- Запрос на SNMA адрес
- Ответ на всех
- Также работает механизм DAD (Duplicate Address Detection)
- Также работает NUD (Neighbor Unreachability Detection) если нет других механизмов

3.9.10 Кэш ND

-