Администрирование Linux
Лекция 4
Настройка сети (теория)

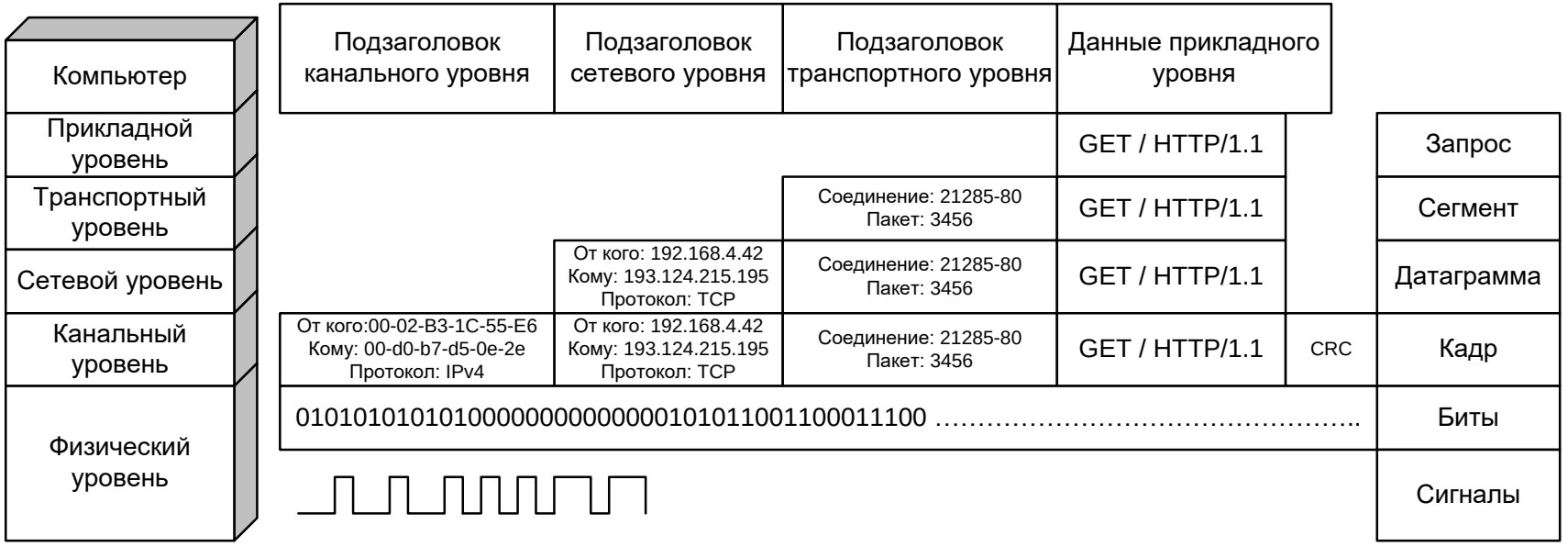
Иртегов Д.В.

Новосибирский гос. Университет

2014

Сначала маленький экскурс в теорию

- 4-уровневая модель DoD, лежащая в основе стека TCP/IP
- На этой картинке нижний уровень разделен на 2: физический и канальный



Канальный уровень

- Наиболее распространенные типы сетей канального уровня
  - Широковещательные сети IEEE 802
    - Ethernet (IEEE 802.3)
    - WiFi (IEEE 802.11)
    - Ethernet over ATM
  - Сети точка-точка
    - PPP
    - Различные туннели:
      PPPoE, PPP over GPRS/3G, PPPoA

Сети IEEE 802

- Логическая шина (все слышат всех)
- Адреса IEEE MAC-48
- OUI – уникальный идентификатор производителя сетевой карты
  http://standards.ieee.org/develop/regauth/oui/oui.txt

Сети IEEE 802 (продолжение)

- Кадры 1500 байт
- Начиная с 802.3z – поддержка Jumbo Frames (до 9216 байт)
- Современные сети имеют звездообразную топологию и основаны на свитчах
- IEEE 802.1Q – виртуальные сети (VLAN)
- IEEE 802.1x – аутентификация и шифрование (изучать не будем)

Протоколы точка-точка

- PPP – Point to Point Protocol RFC 1661
- Первоначально разработан для передачи данных по модемам и нуль-модемам (последовательным портам)
- Используется через ISDN/x.25
- Сейчас чаще всего встречается в виде туннелей
  - PPPoE, PPPoA
  - Не путать с PPTP/L2TP (это туннели IP over IP)
- Поддерживает аутентификацию EAP (RFC 2284) и автосогласование настроек IP

Сетевой уровень

- Главное отличие сетевого уровня DoD от канального
  - На канальном уровне адресация плоская все устройства в одной сети
  - На сетевом уровне адресация иерархическая адрес состоит из номера сети и номера хоста

Сетевой уровень IP

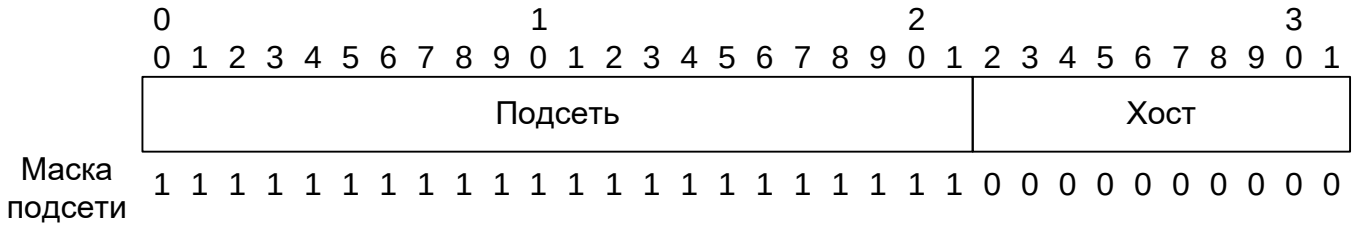
- Stateless
  - Каждый пакет маршрутизуется независимо от остальных
  - Это не всегда верно: бывают маршрутизаторы с connection tracking
    - Файрволлы, NAT

Сетевой уровень IP (продолжение)

- В первом приближении можно сказать, что адрес выдается сетевому интерфейсу
  - У узла с 4 интерфейсами должно быть 4 адреса
  - Это не всегда верно
    - Один адрес у нескольких интерфейсов: бондинг, бридж, proxy arp
    - Несколько адресов у одного интерфейса: IP aliasing
    - Интерфейсы без адресов

Сетевой уровень IPv4

- 32-битный адрес
- Обычно записывается в дот-нотации
  - 4 байта, каждый в десятичной записи например, 10.4.16.253
- Маска подсети



CIDR маска подсети IPv4

- Старшие биты всегда равны 1, младшие – всегда равны 0
  - Маска 11110000111100000000 недопустима
- Маску можно описать дот-нотацией или числом единичных бит
  - Дот-нотация: 255.255.255.0
  - Число единиц: /24

Сети IPv4 (продолжение)

- Специальные диапазоны адресов
  - 127.0.0.0/8 – подсеть для коммуникации внутри хоста. 127.0.0.1 - localhost
  - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 site-local - частные сети, «фейковые адреса»
  - 169.254.0.0/16 – link-local address, используются для автоконфигурации без DHCP
  - 224.0.0.0/4 – мультикастные адреса
  - 255.255.255.255 – link-local броадкаст

ARP и DHCP

- Address Resolution Protocol
  - Протокол поиска MAC адресов на основе IPv4 адреса
  - Широковещательный
    поэтому уязвим для спуфинга
- Dynamic Host Configuration Protocol
  - Протокол автоматической настройки IP
  - В сети должен быть DHCP сервер, который раздает IP адреса и другую информацию (роутер, DNS, сервер удаленной загрузки)
  - Широковещательный
  - Работает по схеме «аренды» (lease)
    одному и тому же хосту стараются давать один и тот же адрес

IPv6

- 128-битный адрес
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Трехуровневая иерархия:
  - Старшие 48 или больше бит – префикс маршрутизации
  - Потом, 16 или меньше бит – номер подсети
  - Младшие 64 бита – MAC-адрес MAC-48 или EUI-64
  - ARP не нужен!
  - Выделены global, organization-local, site-local и link-local префиксы
  - Также выделен диапазон IPv4-совместимых адресов

Автоконфигурация IPv6

- DHCPv6
- Neighbor Discovery Protocol/Router Solicitation
  - Широковещательный протокол
  - Сообщает узлу префикс сети и маршрутизатор.
  - Этого достаточно, т.к. младшие биты адреса совпадают с MAC-адресом

Маршрутизация IP

- У каждого узла есть таблица маршрутизации
- Простейший случай:
  - Eth0: 10.4.16.22
  - 10.4.16.0/24 via Eth0
  - Default via 10.4.16.1
- Сложный случай
  - Много интерфейсов
  - По маршрутной записи на каждую из соответствующих сетей
  - Может быть, за некоторыми сетями есть другие сети, которые нужно явно прописать
- Есть протоколы автосогласования таблиц маршрутизации: RIP, OSPF
  - Мы их проходить не будем

Что еще умеют маршрутизаторы

- Source routing: в зависимости от исходящего адреса, отправлять по разным маршрутам
- Traffic shaping и классы обслуживания
- Туннели IP over IP (VPN)
- Фильтрация: файрволл или сетевой экран
- Network Address Translation: обеспечивает доступ link-local и site-local адресов к глобальной сети

Минимальная информация, необходимая для настройки IP

- Ваш адрес
- Маска вашей подсети
- Роутер по умолчанию (default router)
- Это еще не все!

DNS

- Domain Naming System
- Преобразует имена в формате www.nsu.ru в IP-адреса
- Не только IP, есть разные типы записей и разные типы запросов
- Иерархическая система с рекурсивными запросами:
  - mail.google.com
    - NS к корневому серверу, найти зону .com
    - NS к серверам зоны .com, найти google.com
    - A к серверу зоны google.com

Альтернативы DNS

- /etc/hosts
- NIS/NIS+ (проходить не будем)
- NETBIOS/WINS (проходить не будем)
- LDAP (извращение, но возможно)

Минимальная информация, необходимая для настройки IP

- Ваш адрес
- Маска вашей подсети
- Роутер по умолчанию (default router)
- Имя вашего хоста
- Список DNS серверов
- Домен поиска по умолчанию (не обязательно)