



# Базовое Администрирование Linux

Занятие 5



Дмитрий  
Молчанов

## 1. Сетевые настройки

1. интерфейсы
2. маршруты, фильтры
3. DNS

## 2. Сеть

1. Слои
2. Адреса
3. Протоколы
4. Оверхеды

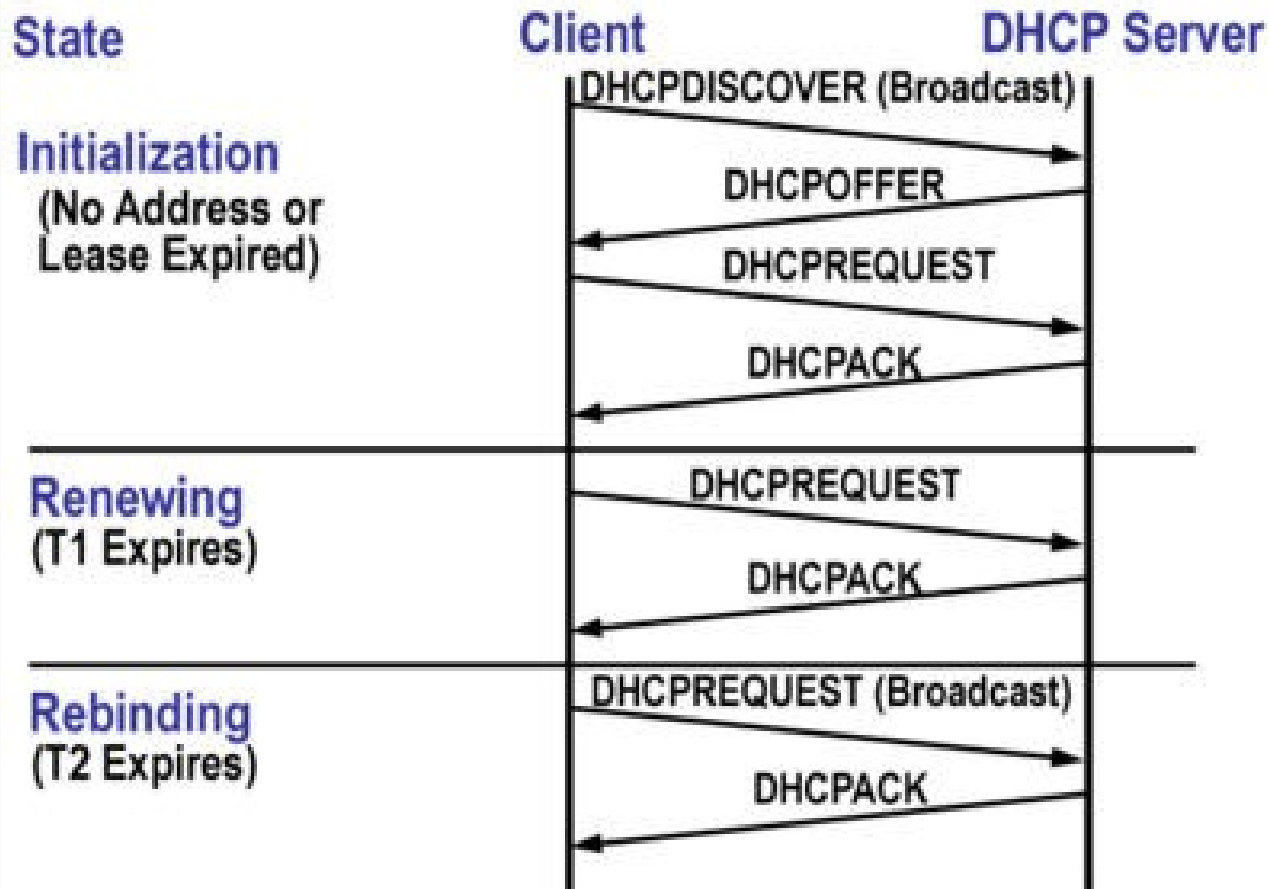
## 3. Сетевые возможности

1. iptables
2. Бриджи, Бонды, dummy
3. тоннели

Чтобы в Linux работала сеть необходимо, чтобы следующие настройки были корректны:

- Адреса на интерфейсах
- Маршруты
- DNS
- Фильтры

# DHCP



# Настройки интерфейсов

---



- `/etc/network/interfaces`
- `ifconfig`, `ifup/ifdown`
- `ip addr`, `link`

# Маршруты.

---

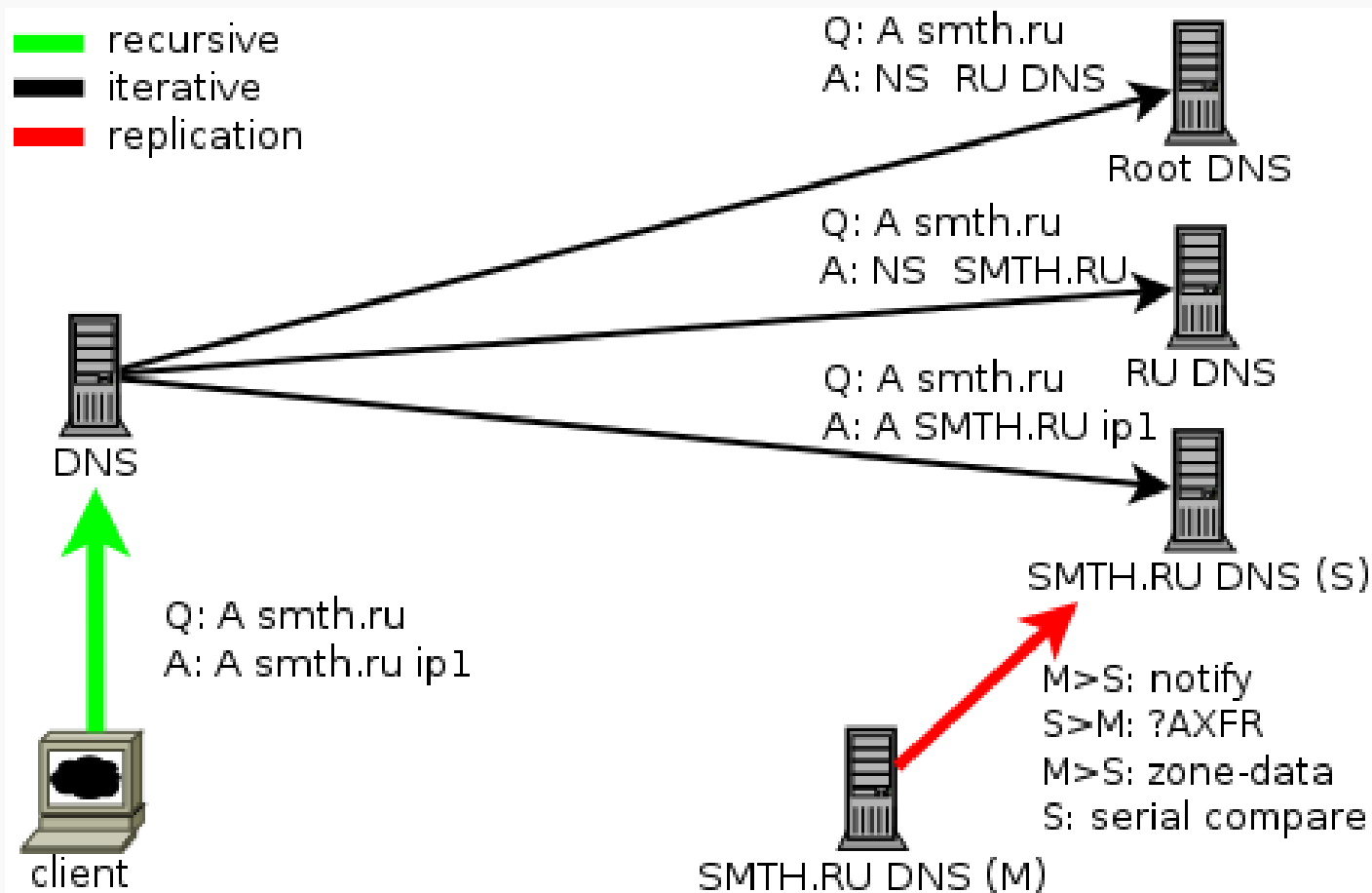


Главное правило – шлюз должен быть в той же сети, что и комп. Но есть исключения.

Так же есть возможность настраивать «хитрые» policy based маршруты

- Как работает
  - ✂ Прямое соответствие (name-ip)
  - ✂ обратное
  - ✂ Рекурсивные запросы
  - ✂ Итеративные запросы

# DNS - типы запросов





- Как работает
  - ✂ Прямое соответствие
  - ✂ обратное
  - ✂ Рекурсивные запросы
  - ✂ Итеративные запросы
- Где настраивается
  - ✂ /etc/resolv.conf
  - ✂ /etc/hosts
  - ✂ nsswitch, nscd

# Фильтры: iptables

---



iptables – мощнейший инструмент для фильтрации и манипуляции с трафиком в linux.

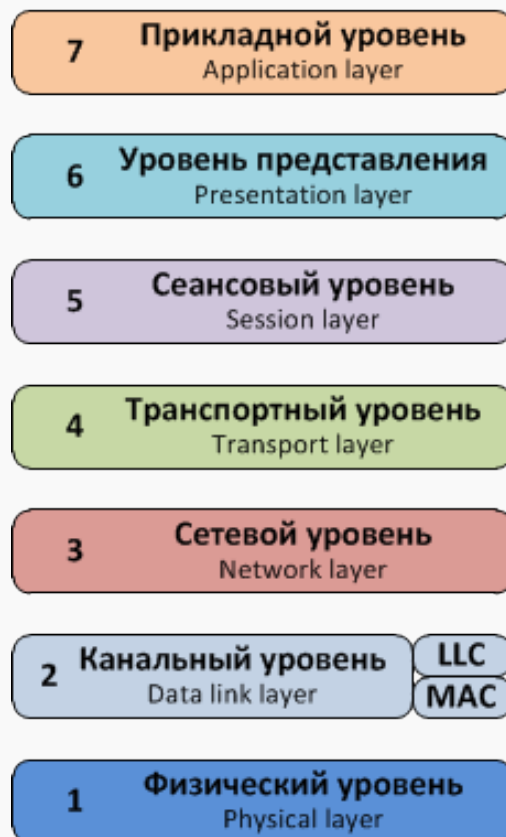
Он позволяет:

- Фильтровать
- Изменять пакеты
- «помечать» пакеты
- Отслеживать соединения

# Сеть: слои и модели



## OSI



## TCP/IP (DOD)



Представления ip-адреса:

- 4 числа разделенные точкой 1.2.3.4
- 4 байта (unsigned int: 127.0.0.1 = 2130706433)
- 4 числа + маска:
  - ✂ cidr 1.2.3.4/24
  - ✂ 1.2.3.4/255.255.255.0
  - ✂ wildcard 1.2.3.4/0.0.0.255
- Маска нужна для того, чтобы отделить адрес сети от адреса хоста.

# ipcalc



```
d.molchanov@balinux201502-net1:~$ ipcalc -n 127.0.0.1
Address:    127.0.0.1          01111111.00000000.00000000. 00000001
Netmask:    255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard:   0.0.0.255         00000000.00000000.00000000. 11111111
=>
Network:    127.0.0.0/24      01111111.00000000.00000000. 00000000
HostMin:    127.0.0.1        01111111.00000000.00000000. 00000001
HostMax:    127.0.0.254      01111111.00000000.00000000. 11111110
Broadcast:  127.0.0.255      01111111.00000000.00000000. 11111111
Hosts/Net:  254              Class A, Loopback
```

## Виды адресов:

- Серые / Белые
  - ✂ 192.168.0.0/16
  - ✂ 10.0.0.0/8
  - ✂ 172.16.0.0/12
  - ✂ 127.0.0.0/8 - loopback
- Unicast
- Broadcast – последний адрес в сети.
- Multicast

- IP (src-ip,dst-ip,protocol)
  - ✂ TCP (src-port,dst-port)
    - ✂ HTTP (Host)
    - ✂ SMTP
    - ✂ DNS
  - ✂ UDP (src-port,dst-port)
    - ✂ DNS
    - ✂ NTP
  - ✂ ICMP (icmp-type)

# TCP

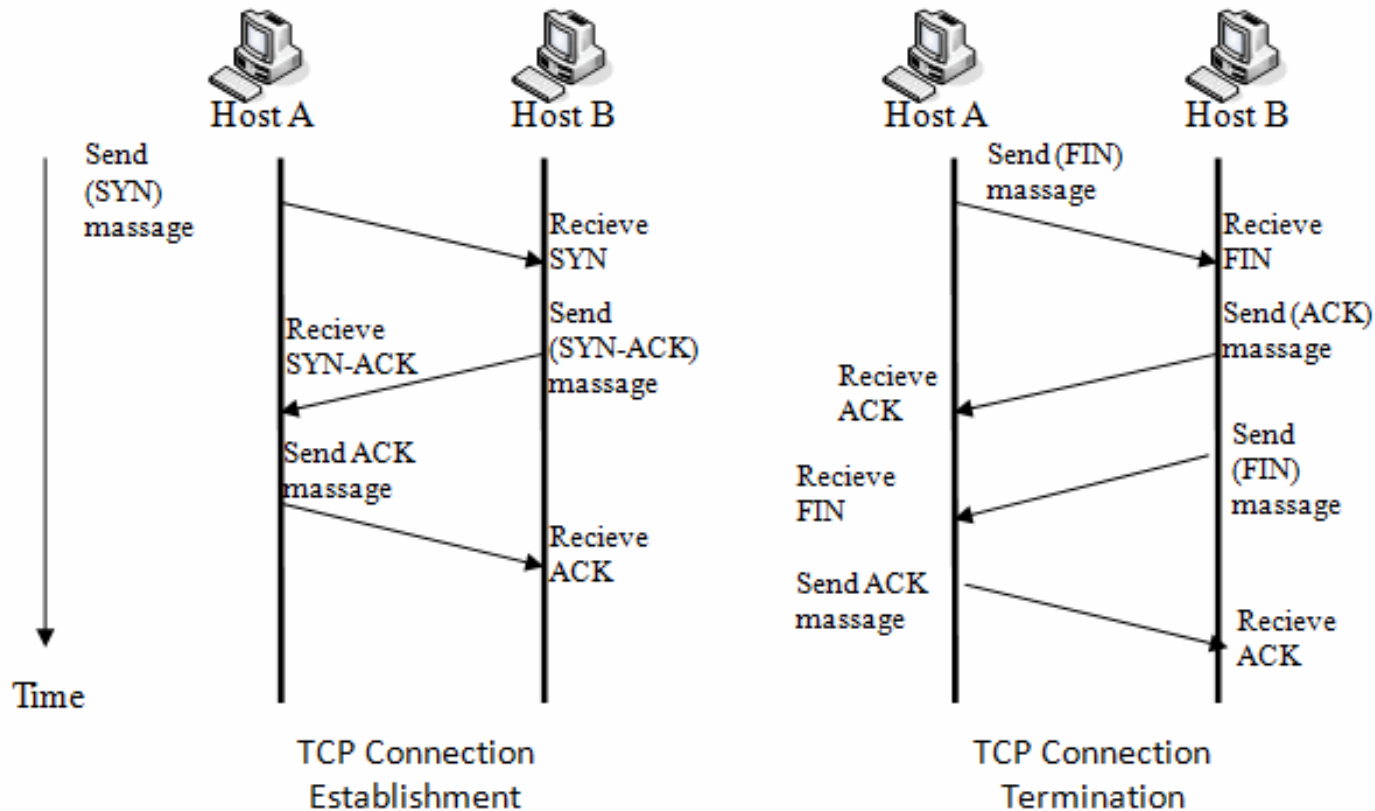


Figure 2.1. TCP session establishment and termination





# HTTP



## \$telnet mail.ru 80

Trying 94.100.180.199...

Connected to mail.ru.

Escape character is '^['.

GET /HTTP/1.1

Host: mail.ru

HTTP/1.1 302 OK

Server: nginx/1.4.4

Date: Wed, 01 Oct 2014 20:18:47 GMT

Content-Type: text/html

Content-Length: 37

Connection: keep-alive

X-Fram e-Options: SAMEORIGIN

Location: https://mail.ru/

Set-Cookie: mrcu=5874542C61A700252CA2459F0905; expires= Sat, 28 Sep 2024 20:18:47 GMT; path= /; domain= mail.ru

Cache-Control: no-cache, no-store, must-revalidate

Pragma: no-cache

Expires: Tue, 01 Oct 2013 20:18:47 GMT

Last-Modified: Thu, 02 Oct 2014 00:18:47 GMT

<html><body>Redirect...</body></html>^]q

telnet> q

Connection closed.



# SMTP



## \$telnet em x.m ail.ru 25

```
Trying 94.100.180.180...
Connected to em x.m ail.ru.
Escape character is '^]'.
220 MailRu ESMTP
ehlo htz-vps01.m olchanov.pp.ru
250-m xpdd10.im ail.ru ready to serve
250-SIZE 73400320
250 8BITM E
mail from :<m dv@ htz-vps01.m olchanov.pp.ru>
250 OK
rcpt to:<dm itry@ m olchanov.pp.ru>
250 OK
data
354 Go ahead
From :m e
To: you
Subject: test

.
550 spam m message rejected. Please visit http://help.m ail.ru/notspam -support/id?c=0T78nRqbSry41lkqH7hQgNXH M 2m SdgAAAAW TAAAXVxB or report details to abuse@ corp.m ail.ru. Error code: 9DFC3E392A6D891A6459E3F242E17EA8831C5703A264DA09. ID: 0000000E0000930501195717.

500 Unknown com m and
quit
221 m xpdd10.im ail.ru closing connection
Connection closed by foreign host.
```

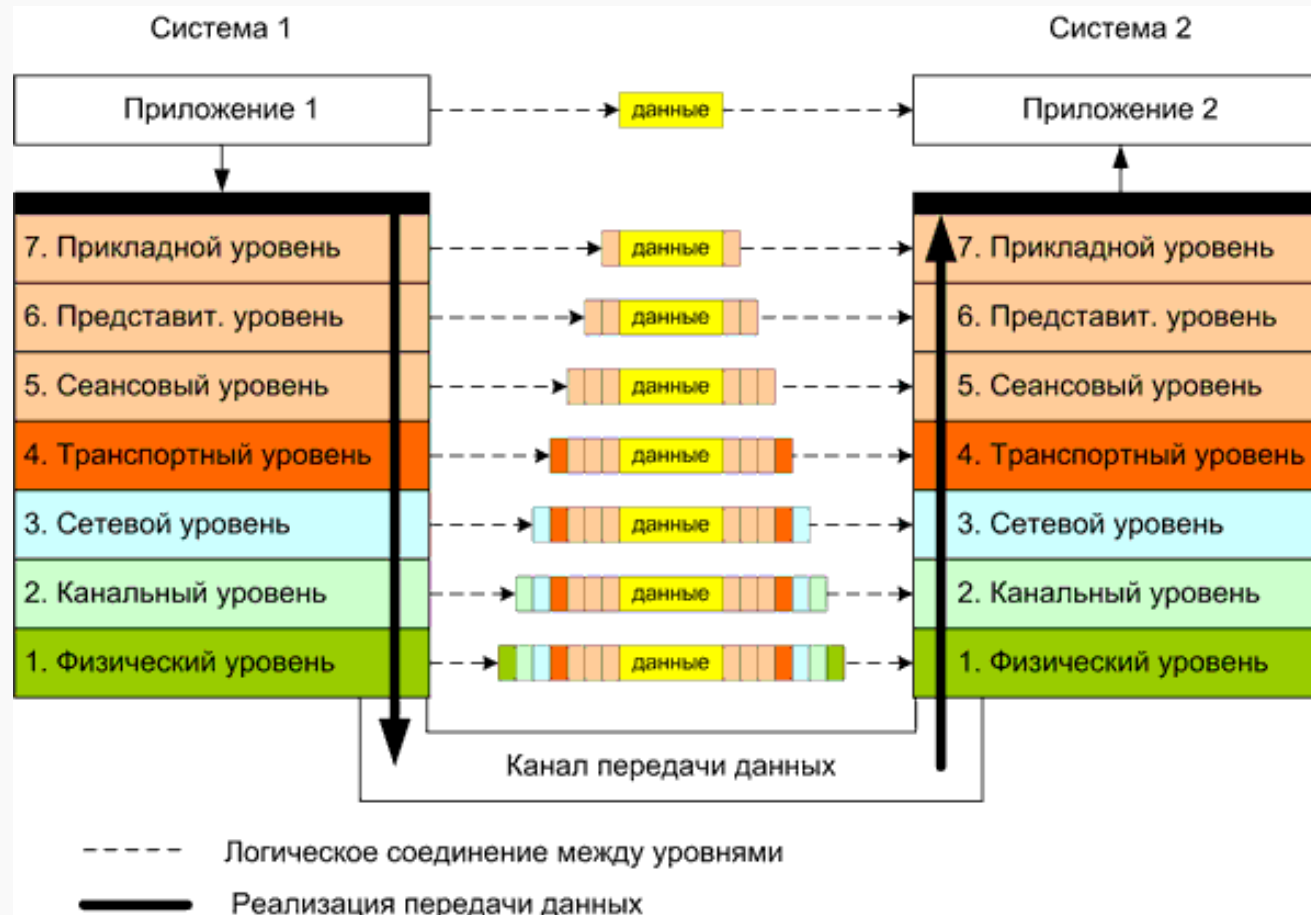
# Overhead'ы



- каждый уровень добавляет свой оверхед
- 100 байт данных
- + 14+bytes HTTP
- + 20-26 bytes TCP
- + 20 bytes IP
- + 22-26 bytes L2

Получается, что в 1500 байт пакете у нас полезной информации примерно на 4% (~62 байта) меньше размера пакета при передаче по tcp/ip.

# Overhead'ы

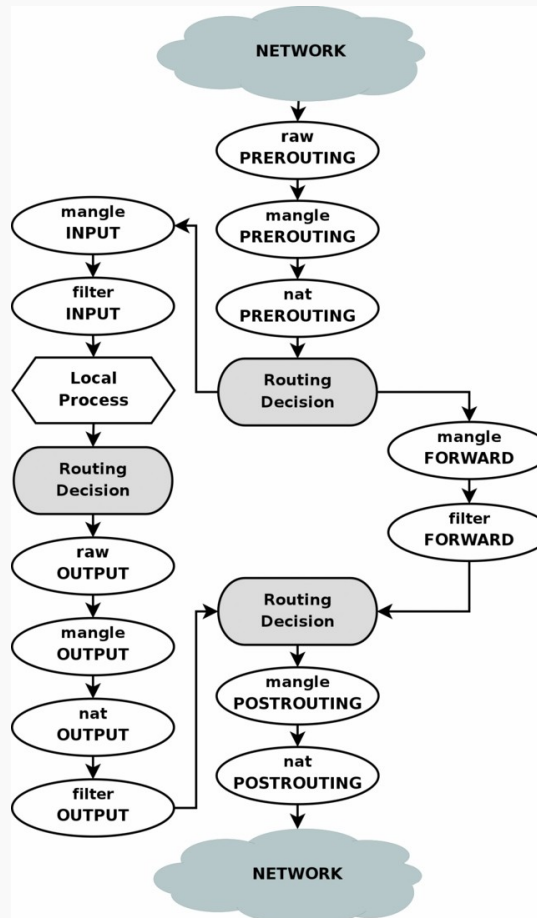


# iptables



- Жизнь пакета в системе
- Таблицы
  - ✂ raw
  - ✂ mangle
  - ✂ nat
  - ✂ filter
- Схема работы iptables

# iptables



# Типы интерфейсов

---



- loopback
- dummy
- bridge
- bond
- tunnels

# Утилиты для работы с сетью:

---



- tcpdump
- ngrep
- netstat
- ss
- ping
- traceroute