нетология

Компьютерные сети,
лекция 3

Сергей
Мясников

Сергей Мясников
Сетевой Инженер, T-Systems
ex Mail.ru Group

План модуля

1. Работа в терминале, лекция 1
2. Работа в терминале, лекция 2
3. Операционные системы, лекция 1
4. Операционные системы, лекция 2
5. Файловые системы
6. Компьютерные сети, лекция 1
7. Компьютерные сети, лекция 2
8. **Компьютерные сети, лекция 3**
9. Элементы безопасности информационных систем

План занятия

1. Таблица маршрутизации
2. Отказоустойчивость сети
3. L4: TCP/UDP
4. Балансировка нагрузки
5. Документирование сети
6. Итоги
7. Домашнее задание

Таблица маршрутизации

Статические и динамические маршруты

Статические маршруты прописываются вручную на каждом маршрутизаторе, через который проходит пакет. Например, если на пути пакета 10 маршрутизаторов, чтобы добавить 1 маршрут, нужно прописать этот маршрут 10 раз.

Преимущества статических маршрутов: не требуются дополнительные протоколы.

Статические и динамические маршруты

Динамические маршруты распространяются протоколами маршрутизации. Например RIP, OSPF, BGP.
Динамический маршрут настраивается один раз на маршрутизаторе-источнике (origin) и далее анонсируется по сети автоматически.
Преимущество динамических маршрутов: простота администрирования сети.

Таблица маршрутизации в Cisco

Основные правила выбора маршрута:

1. Маршрут с длинной маской выигрывает. Например /24 приоритетней чем /18.
2. У каждого протокола есть приоритет (preference). Чем меньше preference, тем приоритетней маршрут. Например, preference для eBGP = 20, Static = 1.
3. Внутри одного протокола выигрывает маршрут с лучшей метрикой. Для eBGP, как правило, это атрибут AS-PATH – список всех AS на пути к сети. Чем меньше кол-во AS, тем выше приоритет у маршрут.

Таблица маршрутизации в Cisco

Маршрутизаторы с открытым доступом – http://www.routeservers.org/

Пример: просмотр таблицы маршрутизации на Cisco

```
telnet route-views.routeviews.org
Username: rviews

> show ip route

Gateway of last resort is 128.223.51.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 128.223.51.1
      1.0.0.0/8 is variably subnetted, 3110 subnets, 17 masks
B        1.0.0.0/24 [20/10] via 89.149.178.10, 1d16h
B        1.0.4.0/22 [20/0] via 64.71.137.241, 3w4d
B        1.0.4.0/24 [20/0] via 64.71.137.241, 3w4d
B        1.0.5.0/24 [20/0] via 64.71.137.241, 7w0d
B        1.0.6.0/24 [20/0] via 64.71.137.241, 3w4d
B        1.0.7.0/24 [20/0] via 64.71.137.241, 7w0d
B        1.0.64.0/18 [20/0] via 64.71.137.241, 7w0d
B        1.0.128.0/17 [20/0] via 94.142.247.3, 6d11h
B        1.0.128.0/18 [20/0] via 94.142.247.3, 6d11h
```

Временные статические маршруты в Linux

Для добавления временных маршрутов используется утилита ip.

```
# Добавление маршрута через шлюз:
ip route add 172.16.10.0/24 via 192.168.1.1

# Добавление маршрута через интерфейс:
ip route add 172.16.10.0/24 dev eth0

# Маршрут с метрикой:
ip route add 172.16.10.0/24 dev eth0 metric 100

# Просмотр маршрутов до определенной сети
ip route show 10.0.0.0/8

# Пересылка пакетов между интерфейсами
 cat /proc/sys/net/ipv4/ip_forward
 echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
[sm@manjaro ~]$ ip -br route
default via 192.168.1.1 dev wlp4s0 proto dhcp metric 600
172.16.109.0/24 dev vmnet1 proto kernel scope link src 172.16.109.1
172.16.118.0/24 dev vmnet8 proto kernel scope link src 172.16.118.1
192.168.1.0/24 dev wlp4s0 proto kernel scope link src 192.168.1.21 metric 600
192.168.250.0/24 via 192.168.250.1 dev wlp4s0 proto static metric 600
192.168.250.1 dev wlp4s0 proto static scope link metric 600
```

Таблицы маршрутизации в Linux

В Linux можно настроить несколько таблиц маршрутизации.
По умолчанию, если не указано имя таблицы, используется таблица main.

```
cat /etc/iproute2/rt_tables
#
# reserved values
#
255     local
254     main
253     default
0       unspec
#
# local
#
```

Постоянные статические маршруты в Linux

Добавление постоянных маршрутов в файл /etc/network/interfaces.

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The production network interface
auto eth0
allow-hotplug eth0
# iface eth0 inet dhcp
# Remove the stanzas below if using DHCP.
iface eth0 inet static
  address 10.10.10.140
  netmask 255.255.255.0
  gateway 10.10.10.1

# The management network interface
auto eth1
allow-hotplug eth1
iface eth1 inet static
  address 172.16.100.10
  netmask 255.255.255.0
  post-up ip route add 172.16.100.0/24 dev eth1 src 172.16.100.10 table mgmt
  post-up ip route add default via 172.16.100.1 dev eth1 table mgmt
  post-up ip rule add from 172.16.100.10/32 table mgmt
  post-up ip rule add to 172.16.100.10/32 table mgmt
```

[Источник файла конфига]

Dummy интерфейсы в Linux

Dummy – виртуальный интерфейс, удобно использовать для анонса маршрутов.

```
echo "dummy" >> /etc/modules
echo "options dummy numdummies=2" > /etc/modprobe.d/dummy.conf


vim /etc/network/interfaces

auto dummy0
iface dummy0 inet static
    address 10.2.2.2/32
    pre-up ip link add dummy0 type dummy
    post-down ip link del dummy0
```

Bird – динамическая маршрутизация в Linux

```
apt install bird2
systemctl enable bird
systemctl restart bird

vim /etc/bird/bird.conf

log syslog all;

protocol kernel {
        ipv4 {
                export all;     # Default is export none
        };
        persist;                # Don't remove routes on BIRD shutdown
}

protocol device {
}

protocol rip {
        ipv4 {
                import all;
                export all;
        };
        interface "ens4";
        interface "ens5";
}
protocol direct {
        ipv4;                   # Connect to default IPv4 table
        interface "dummy*";
}
```

The BIRD Internet Routing Daemon Project

Пример конфигурации сети для Bird

```
# Host Ubuntu-1
auto dummy0
iface dummy0 inet static
    address 10.1.1.1/32
    pre-up ip link add dummy0 type dummy
    post-down ip link del dummy0

allow-hotplug ens4
iface ens4 inet static
    address 192.168.12.1
    netmask 255.255.255.0

allow-hotplug ens5
iface ens5 inet static
    address 192.168.120.1
    netmask 255.255.255.0
```

```
# Host Ubuntu-2
auto dummy0
iface dummy0 inet static
    address 10.2.2.2/32
    pre-up ip link add dummy0 type dummy
    post-down ip link del dummy0

allow-hotplug ens4
iface ens4 inet static
    address 192.168.12.2
    netmask 255.255.255.0

allow-hotplug ens5
iface ens5 inet static
    address 192.168.120.2
    netmask 255.255.255.0
```

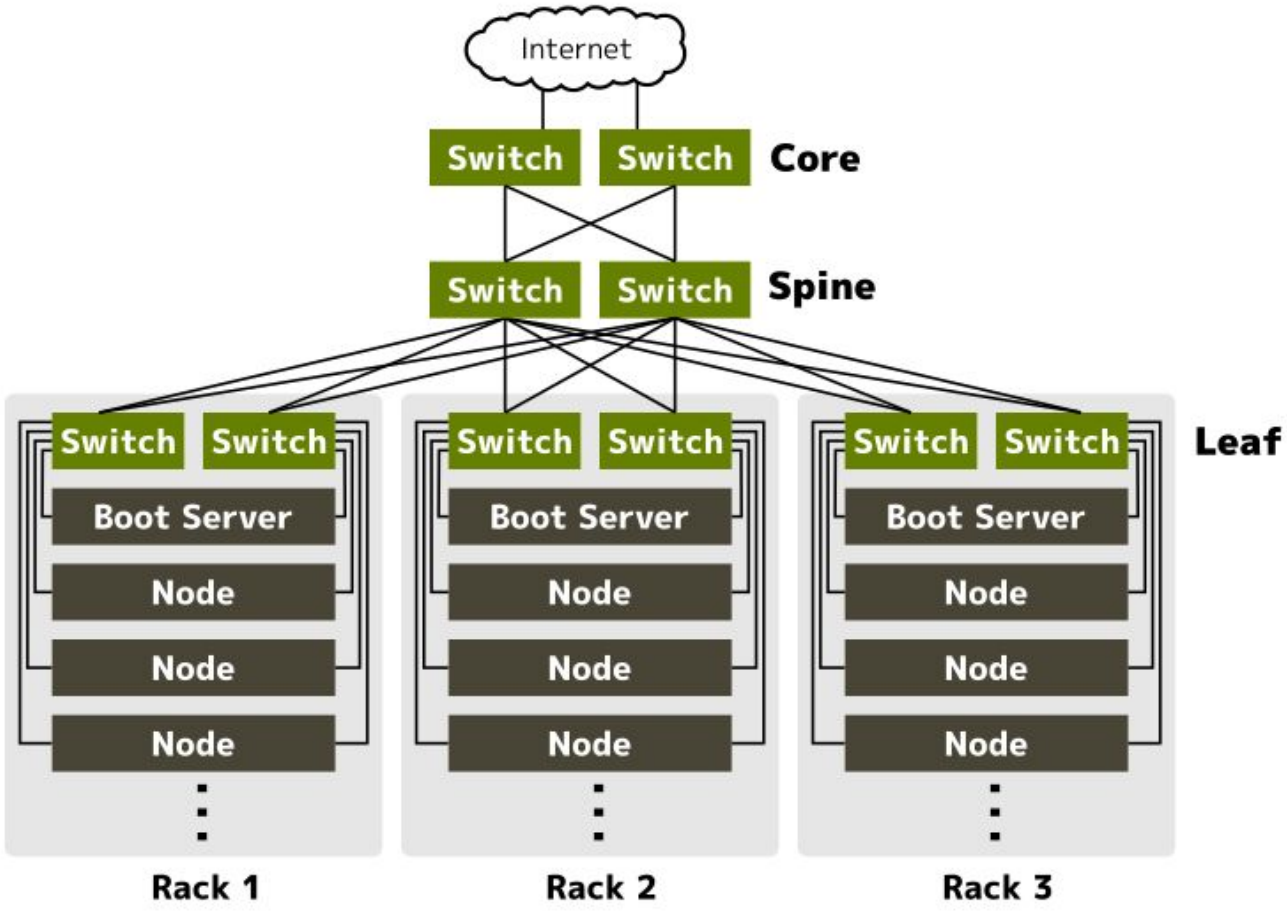
```
root@ubuntu:~# ip -br r
default via 192.168.255.1 dev ens3
10.1.1.1 dev dummy0 proto bird scope link metric 32
10.2.2.2 proto bird metric 32
        nexthop via 192.168.12.2 dev ens4 weight 1
        nexthop via 192.168.120.2 dev ens5 weight 1
192.168.12.0/24 dev ens4 proto kernel scope link src 192.168.12.1
192.168.120.0/24 dev ens5 proto kernel scope link src 192.168.120.1
192.168.255.0/24 dev ens3 proto kernel scope link src 192.168.255.13
```

birdc – консоль Bird

```
root@ubuntu:~# birdc
BIRD 2.0.7 ready

bird> show protocols
Name       Proto      Table      State  Since         Info
kernel1    Kernel     master4    up     18:05:01.011
device1    Device     ---        up     18:05:01.011
rip1       RIP        master4    up     18:05:01.011
direct1    Direct     ---        up     18:05:01.011

bird> show rip neighbors
rip1:
IP address                Interface  Metric Routes    Seen
192.168.12.2              ens4            1      1  27.016
192.168.120.2             ens5            1      2  13.082

bird> show route
Table master4:
10.1.1.1/32          unicast [direct1 18:05:01.033] * (240)
        dev dummy0
                      unicast [rip1 18:05:01.237] (120/3)
        via 192.168.120.2 on ens5
10.2.2.2/32          unicast [rip1 18:05:01.048] (120/2)
        via 192.168.12.2 on ens4 weight 1
        via 192.168.120.2 on ens5 weight 1
```

Отказоустойчивость сети

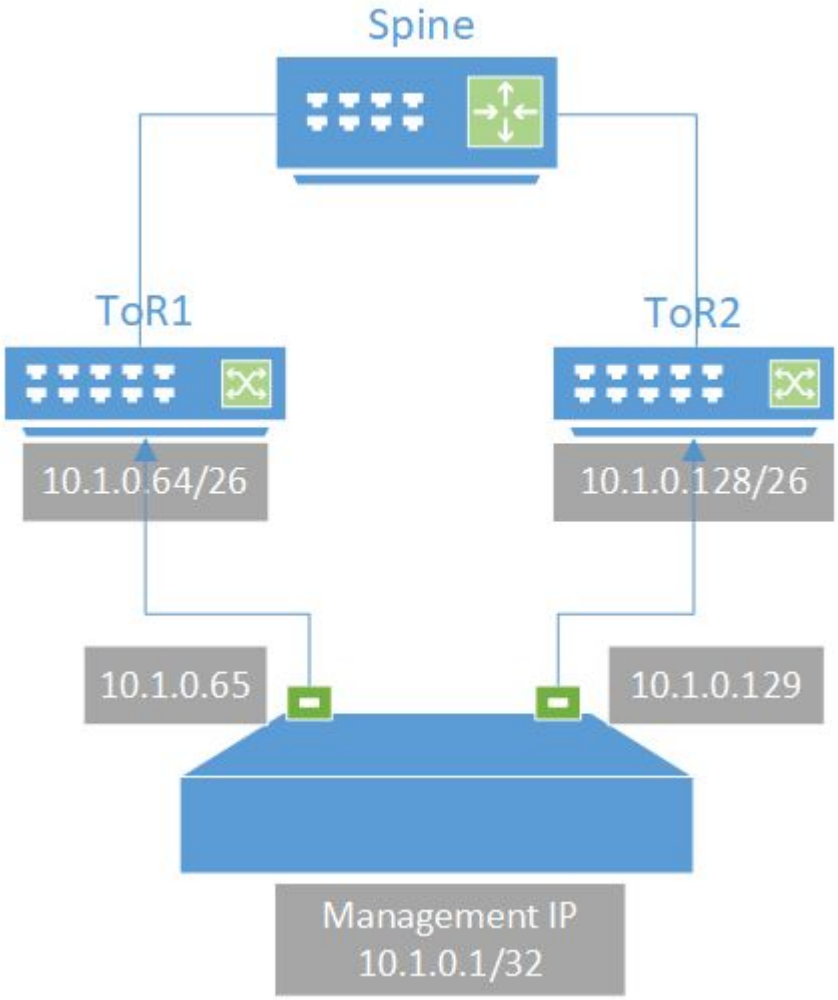
Дизайн сети в Дата-центре



https://blog.kintone.io/entry/neco/network-design

ECMP – несколько равнозначных маршрутов

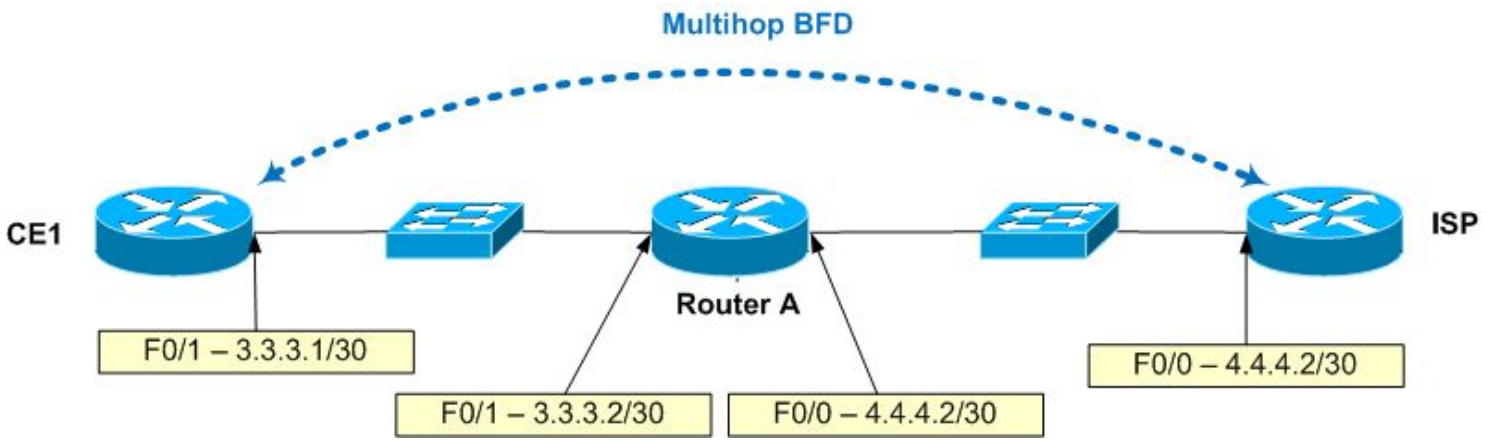
Отказоустойчивость внутри ДЦ



BFD ускоряет сходимость сети

Сходимость сети – время требуемое на перестроение маршрутов при падении линка.
BFD протокол:

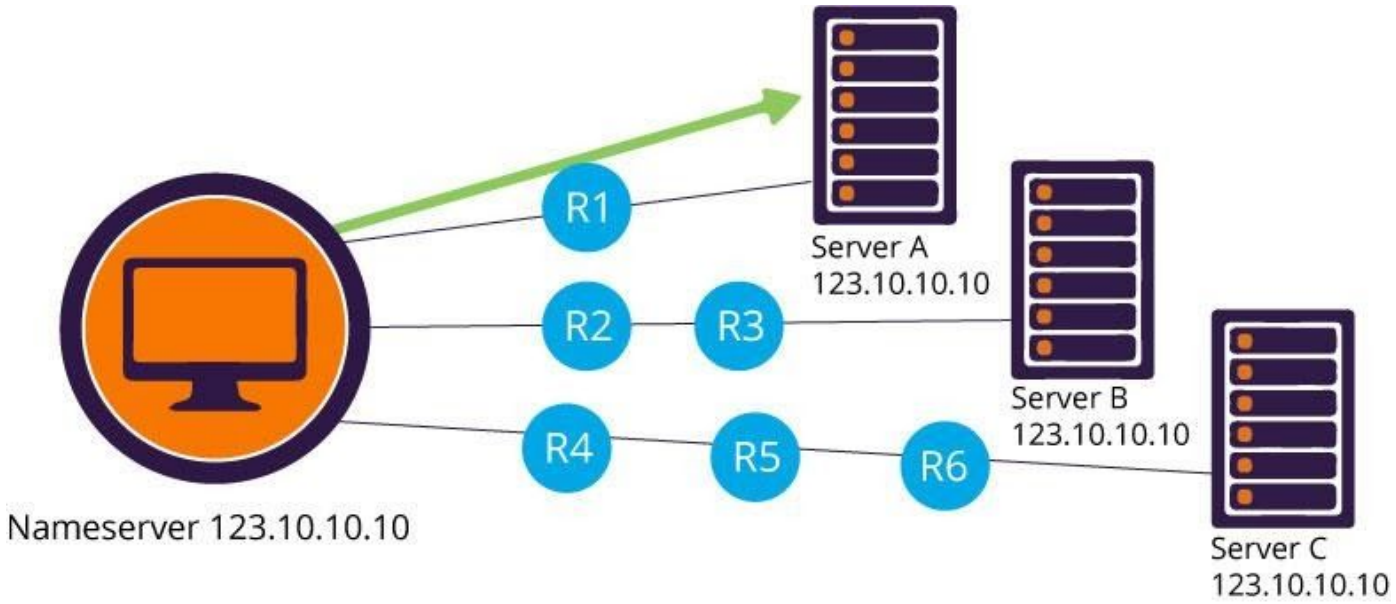
- поднимает сессию между соседями в другом протоколе - RIP, OSPF, BGP;
- BFD заменяет медленный механизм типа keepalive у протоколов маршрутизации;
- обеспечивает сходимость менее 50ms.



http://ciao-cacao.blogspot.com/2011/12/bgp-bfd.html

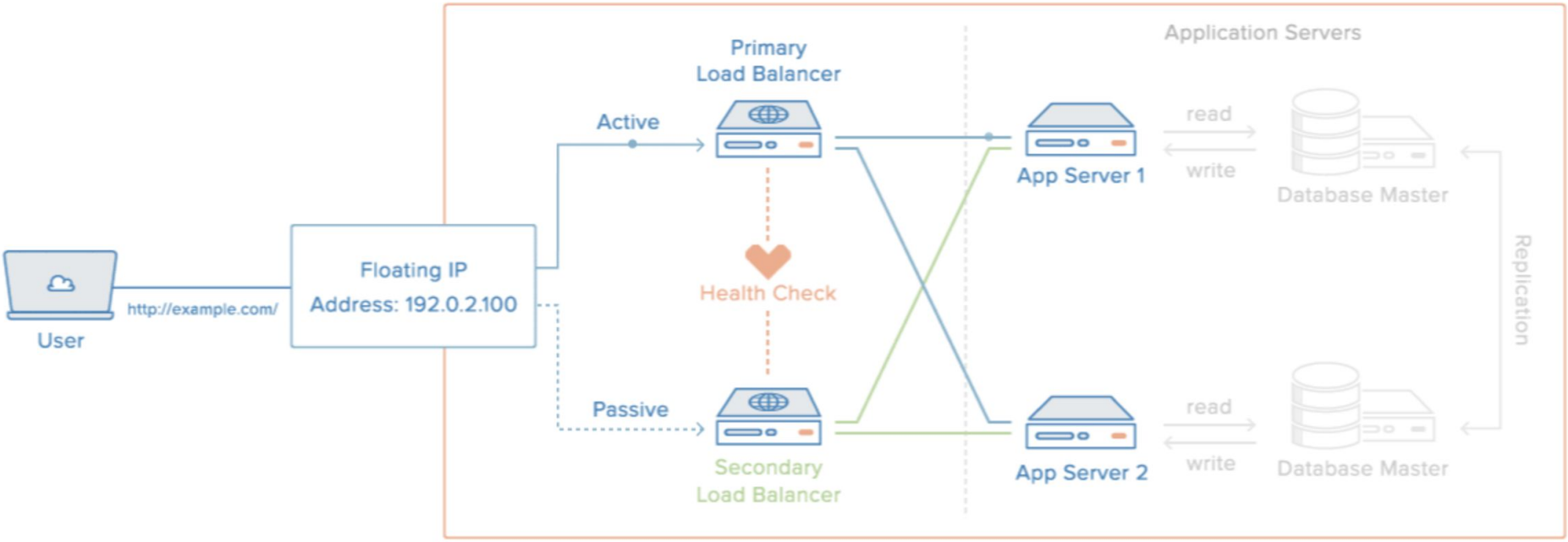
Anycast – одинаковые IP на серверах

- Отказоустойчивость снаружи ДЦ, георезервирование ДЦ;
- Маршрутизация клиента осуществляется к ближайшему серверу.
- Сервера располагаются, как правило, в разных ДЦ.
- При отказе одного ДЦ – трафик уйдет в оставшиеся живые ДЦ



https://habr.com/ru/company/ruvds/blog/511050/

First-Hop Redundancy Protocols – VRRP, HSRP



взято с сайта: DO

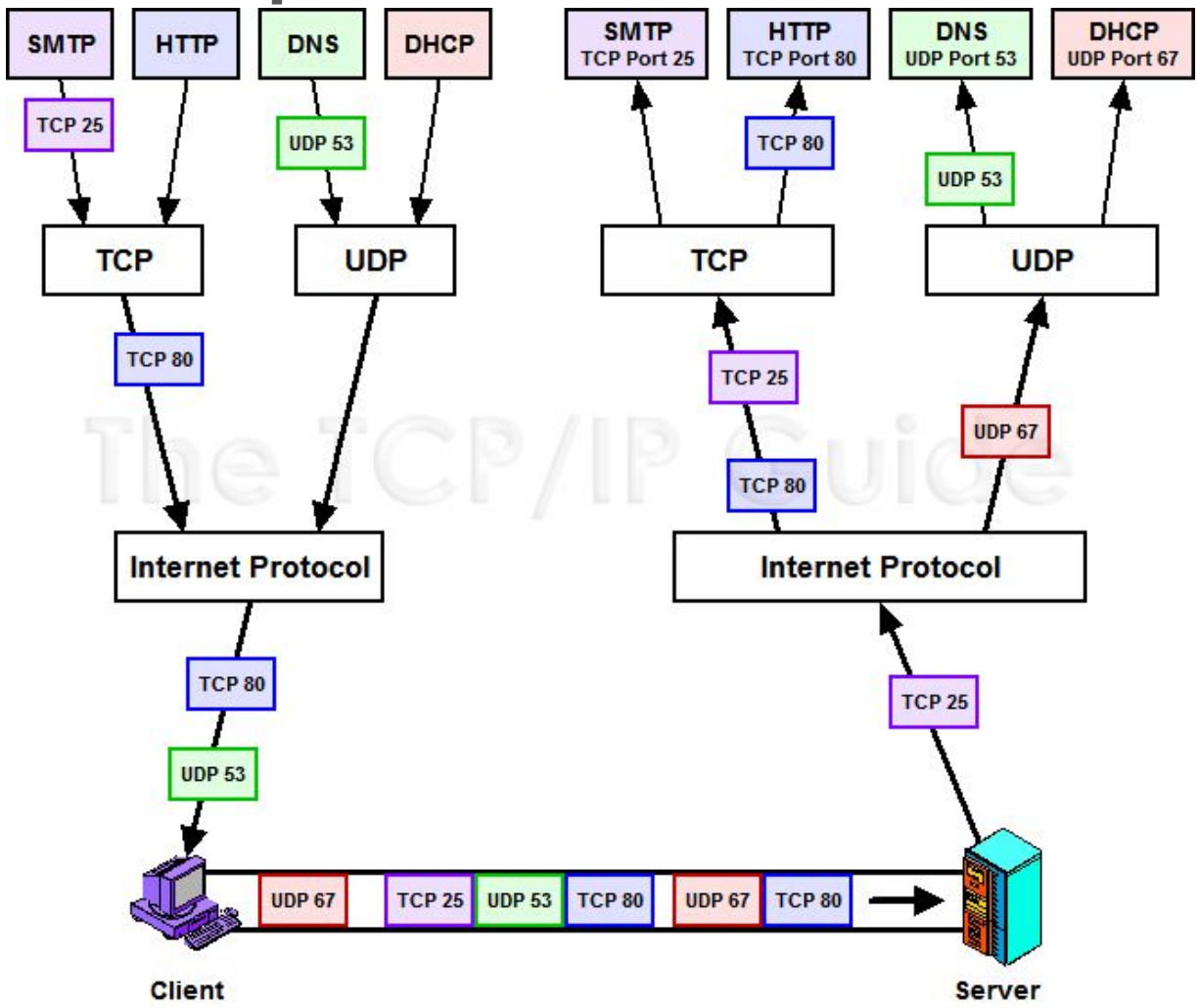
Keepalived – реализация VRRP на Linux

Сервисы, требующие высокой доступности, обычно используют плавающие IP-адреса. Плавающий IP-адрес может быть автоматически переброшен между несколькими серверами в ходе переключения на резерв из-за выхода из строя основного сервера или для обновления программного обеспечения без простоев.

Пример настройки

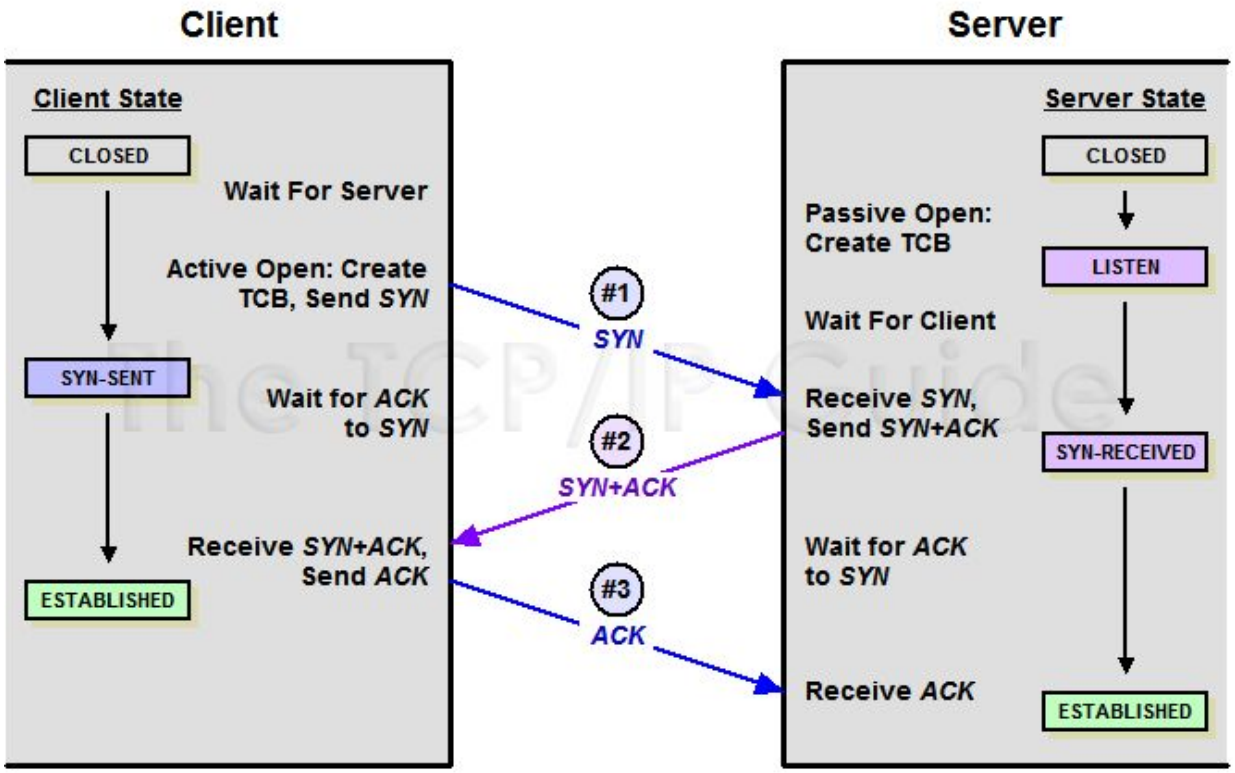
L4: TCP/UDP

TCP/UDP порты



http://www.tcpipguide.com/free/t_TCPIPPortsTransportLayerTCPUDPAddressing-2.htm

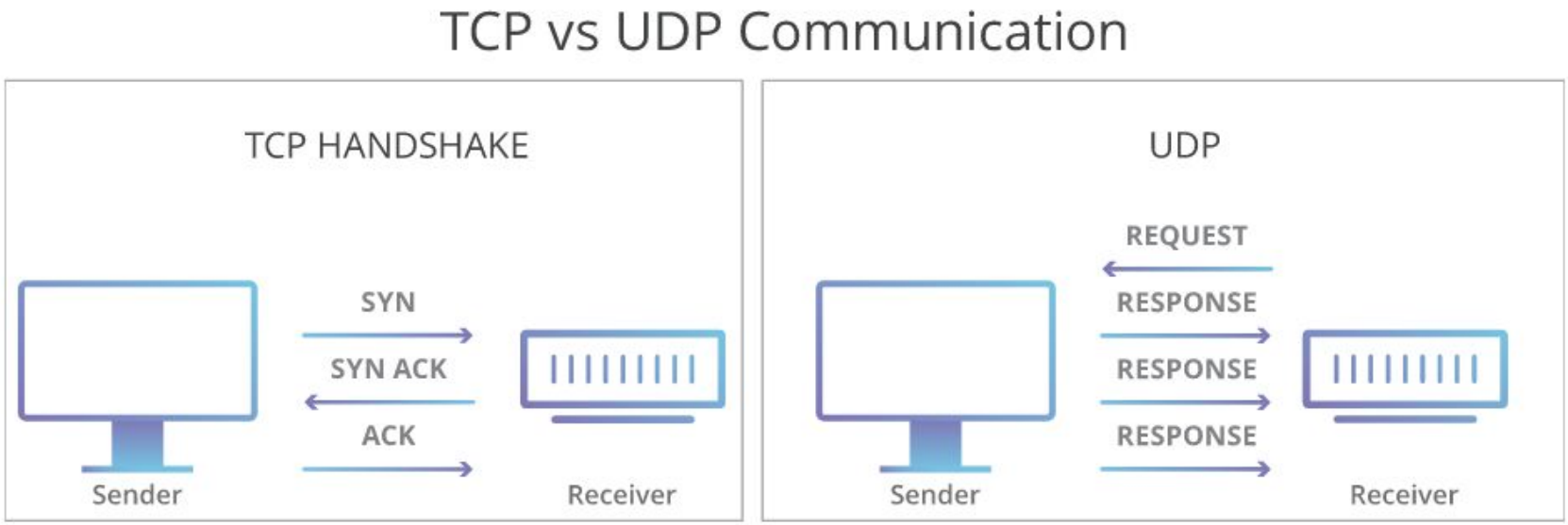
TCP 3-Way Handshake: SYN, SYN-ACK, ACK



http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentProcessTheThreeWayHandsh-3.htm

UDP работает без установки сессии

UDP используется обычно для протоколов чувствительных к задержке, например, RTP для передачи аудио. Также используется для протоколов не чувствительных к потерям пакетов, например, Syslog, SNMP.



SS – Socket Statistics

```
ss -n
State      Recv-Q Send-Q    Local Address:Port     Peer Address:Port
ESTAB      0      240         172.31.0.14:22      172.30.10.202:51831

# порты в ожидании входящего трафика
ss -l
State      Recv-Q Send-Q    Local Address:Port   Peer Address:Port
LISTEN     0      128

# UDP сокеты
ss -ua
State      Recv-Q Send-Q     Local Address:Port     Peer Address:Port
UNCONN     0      0           172.31.0.255:ntp                *:*

# Показать процесс использующий сокет
ss -p
State      Recv-Q Send-Q      Local Address:Port   Peer Address:Port
ESTAB      0      240           172.31.0.14:ssh   172.30.10.202:51831
users:(("sshd",13548,3))

# Фильтр по Source port
ss -au sport = :123
State      Recv-Q Send-Q    Local Address:Port     Peer Address:Port
UNCONN     0      0          172.31.0.255:ntp                *:*

# Статистика
ss -s
Total: 43 (kernel 0)
TCP:   2 (estab 1, closed 0, orphaned 0, synrecv 0, timewait 0/0), ports 0

Transport Total     IP        IPv6
*         0         -         -
RAW       0         0         0
UDP       4         4         0
TCP       2         2         0
```

Балансировка нагрузки

Nginx – L4 балансировщик

https://blog.listratenkov.com/kak-nastroit-nginx-v-kachestve-balansirovshhika-nagruzki/

Nginx – пример конфига

```
http {
  upstream backend1 {
    server 192.168.0.1;
    server 192.168.0.2;
    server 192.168.0.3;
  }

  server {
    listen 80;

    location / {
      proxy_pass http://backend1;
    }
  }
}

# балансировка UDP - DNS
stream {
  upstream dns_backends {
    server 8.8.8.8:53;
    server 8.8.4.4:53;
  }

  server {
    listen 53 udp;
    proxy_pass dns_backends;
    proxy_responses 1;
  }
}
```

Больше примеров

Документирование сети

IP план – таблица в Excel

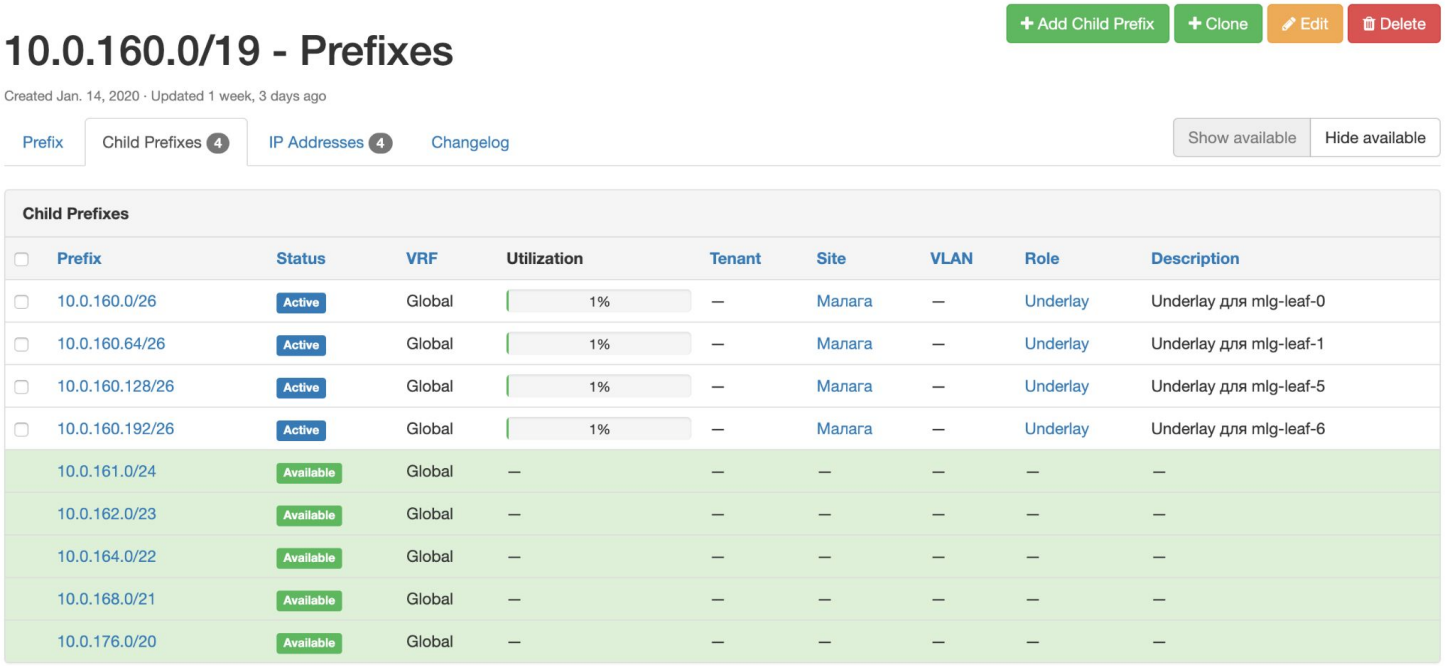
Заполняется вручную, быстро теряет актуальность при изменениях IP.

IP-адрес	Примечание	VLAN
198.51.100.0/28	**Выделено провайдером (МСК)**	6
198.51.100.1	Маршрутизатор провайдера	
198.51.100.2	msk-arbat-gw1	
198.51.100.2-198.51.100.14	Пул адресов для NAT	
198.51.100.2	WEB	
198.51.100.3	FILE	
198.51.100.4	MAIL	
198.51.101.0/30	**Выделено провайдером (НСК)**	
198.51.101.1	Маршрутизатор провайдера	
198.51.101.2	nsk-obsea-gw1	
198.51.102.0/30	**Выделено провайдером (ТМСК)**	
198.51.102.1	Маршрутизатор провайдера	
198.51.102.2	tmsk-lenina-gw1	
198.51.103.0/30	**Выделено провайдером (Брно)**	
198.51.103.1	Маршрутизатор провайдера	
198.51.103.2	brno-gw1	

IP план – IPAM система Netbox

Возможно, настроить автоматизацию – импорт IP из конфигов.

API для скриптов.

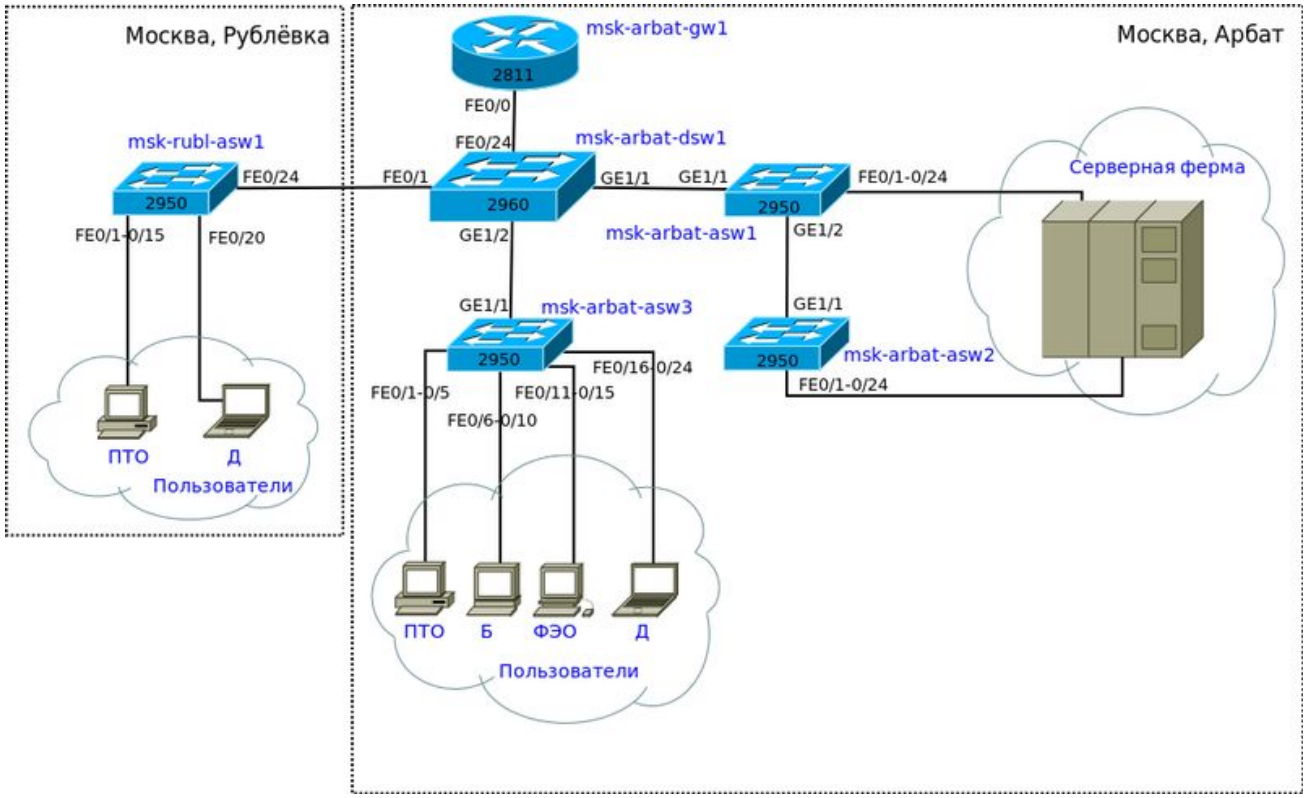


Installing NetBox - NetBox Documentation

Диаграммы diagrams.net

L1/L2 диаграммы, L3 диаграммы

Тип диаграмм в diagrams.net – Network.



Схемы сети

Flowchart Maker & Online Diagram Software

Итоги

Сегодня мы:

- Рассмотрели принципы работы таблиц маршрутизации;
- Изучили основные схемы отказоустойчивости сети;
- Познакомились с протоколами L4 TCP и UDP;
- Познакомились с балансировщиком нагрузки Nginx;
- Рассмотрели инструменты для документирования сетей.

Домашнее задание

Давайте посмотрим ваше домашнее задание.

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

Дополнительные материалы

- Все о Networking в Linux
- Гайд по TCP/IP

нетология

Задавайте вопросы и пишите отзыв о лекции!

Сергей Мясников