ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Linux в сети

Бриджи и туннели

Александр Румянцев

Linux bridge

В linux есть встроенный свитч с поддержкой VLAN и STP, который может объединить до 1012 интерфейсов

Управляется либо с помощью `iproute2` (`ip link`), либо с помощью утилиты `brctl` из пакета `bridge-utils`

Возможно объединить, очевидно, только L2 интерфейсы (eth, tap, wi-fi), L3 (tun, ppp) в бридж добавить нельзя

При объединении ethernet и wifi нужно, что бы MAC-адресом bridge был установлен MAC-адрес wifi-интерфейса, иначе невозможно будет подключиться к wifi (а некторые драйвера и чипы не позволяют в принципе сменить MAC на wifi-интерфейсе)

Linux bridge

RH/CentOS для конфигурации интерфейса использует brctl

```
# cat ifcfg-br0
DEVICE="br0"
BOOTPROTO="static"
IPADDR="192.168.12.10"
NETMASK="255.255.255.0"
GATEWAY="192.168.12.2"
DNS1=192.168.12.2
ONBOOT="yes"
TYPE="Bridge"
NM_CONTROLLED="no"
```

```
# cat ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
BOOTPROTO=none
ONBOOT=yes
NM_CONTROLLED=no
BRIDGE=virbr0
```


Linux bridge

```
ip link add name bridge_name type bridge
ip link set bridge_name up
ip link set eth0 up
ip link set eth0 master bridge_name
bridge link
ip link set eth0 nomaster
ip link set eth0 down
ip link delete bridge_name type bridge
```

iproute2

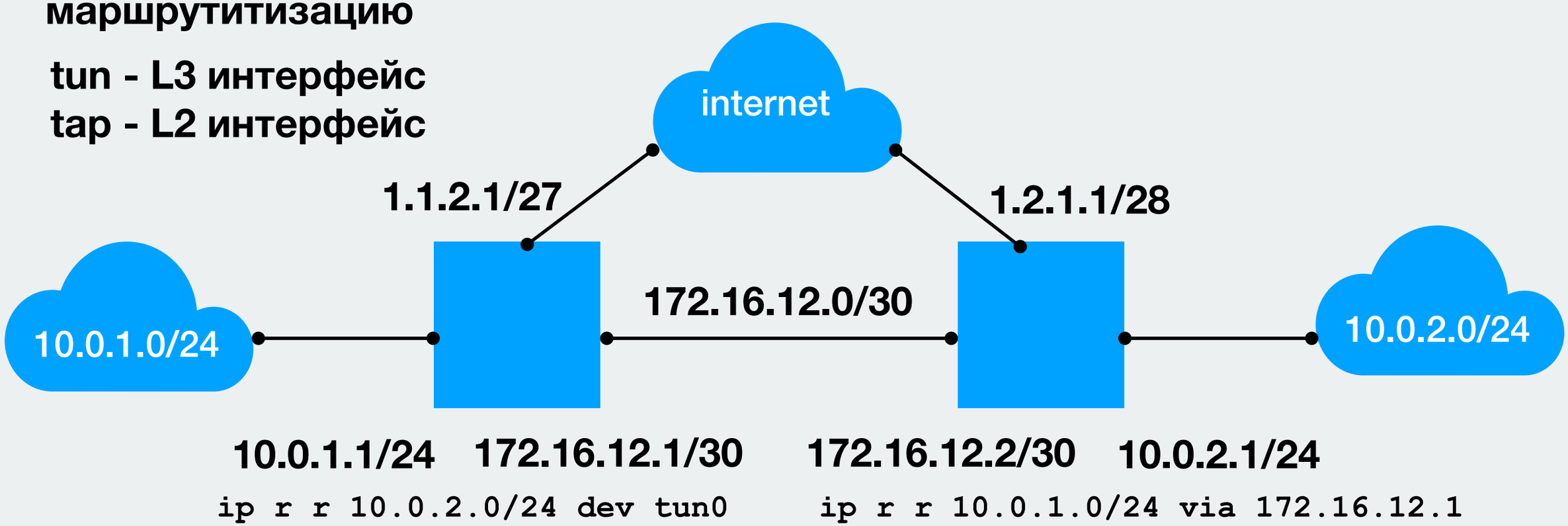
```
brctl addbr bridge_name
brctl addif bridge_name eth0
brctl show
ip link set up dev bridge_name
ip link set dev bridge_name down
brctl delbr bridge_name
```

brctl

Туннели

Туннелирование - инкапсуляция пакетов в IP. Может быть L2 и L3.
Протоколы, реализующие туннелирование могут быть L4 и L7.
Для создания туннелей применяются виртуальные интерфейсы, драйверы которых упаковывают принятые данные в IP-пакет и отправляют снова на маршрутитизацию

tun - L3 интерфейс
tap - L2 интерфейс



Простейшие L3-туннели

На L3, очевидно, не поддерживаются link-state протоколы маршрутизации, такие как OSPF, RIP. Так-же не будет работать multicast и vrrp/carp

IPIP, GRE (Linux, FreeBSD, IOS)

```
# ip tunnel add tun0 mode <ipip|gre> local 10.1.1.1 remote 10.2.2.2 dev eth0
# ip address add dev tun0 10.0.0.1 peer 10.0.0.2/32
```

```
# cat ifcfg-tun0
DEVICE=tun0
MY_OUTER_IPADDR=10.1.1.1
PEER_OUTER_IPADDR=10.2.2.2
MY_INNER_IPADDR= 10.0.0.1
PEER_INNER_IPADDR=10.0.0.2/32
TYPE=<IPIP|GRE>
```

IPIP просто инкапсулирует IP-пакеты, тогда как GRE добавляет еще свой заголовок, который позволяет инкапсулировать, теоретически, любые L3-пакеты, например тот-же VRRP

IPSEC

Немного стоит в стороне, т.к. в своей идеологии использует понятие "трансформации". Трансформируются пакеты, отобранные фильтром, по определенному алгоритму. При этом меняются только адреса назначения и контрольные суммы, тело шифруется симметричным шифрованием ключами, выработанными по протоколу IKE (на деле всё тот-же X.509 и Diffie-Hellman или PSK), который уже работает на L7 (приложения)

Point to Point Protocol

Протокол туннелирования, предполагающий согласование параметров туннеля, таких как адрес, маска, способ шифрования, аутентификацию

На базе него работают:
Модемные соединения, включая мобильные вплоть до HSPA
PPTP - PPP over GRE (over IP)
PPPoE - PPP over Ethernet

IPoE - к сетям не имеет отношения, это чисто маркетинговый термин, обозначающий отсутствие туннелей на последней миле

Реализуется в linux, демоном pppd с поддержкой в ядре (специальный тип интерфейса ppp)который, несколько устарел.
Для работы использует терминал (исторически так сложилось).
Alan Kox, автор терминала, править код отказывается, мотивируя это тем, что "там кошмар, я ничего не помню"

OpenVPN

Фактически, единственное, что нам остаётся для связи между двумя linux-роутерами

Режимы работы интерфейса:
- **P2P**
- **Subnet**

Режимы аутентификации:
- **PSK**
- **Certificate-based**

Может работать поверх:
- **tcp**
- **udp**

Может туннеллировать:
- **L2 (tap)**
- **L3 (tun)**

P.S. давно наблюдаю за проектом https://www.softether.org/
Но он управляется windows-based клиентом

Лирическое отступление. TUN/TAP

Виртуальные сетевые интерфейсы, предоставляющие доступ из ядра в userspace через псевдоустройства /dev/net/tun или /dev/net/tap.

Не путать с vtun/vtap, использующимися в виртуализации

OpenVPN

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

опция `proto`
- `udp`
- `tcp-client`
- `tcp-server`

Может работать поверх:
- **tcp**
- **udp**

Режим tcp используется для клиентов за NATом
При потере пакета вызывает retransmission hell: ретрансмиссия инициируется на обоих уровнях: и на уровне протокола openvpn, и внутри туннеля, порождая разного рода задержки.

Во всех остальных случаях надо использовать режим udp

OpenVPN

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

опция `dev`
- **`tun`**
- **`tap`**

Использование tun более экономно, динамический роутинг возможен на базе iBGP.

Использование tap позволяет прозрачно соединить две сети с помощью bridge. На tap возможно использовать link-state динамические протоколы роутинга. Имеет смысл использовать при хорошем канале с оплатой за линк (без учёта данных и процентилей). Клиент может получать конфигурацию напрямую из dhcp.

Может туннеллировать:
- **L2 (tap)**
- **L3 (tun)**

OpenVPN

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

Режимы работы интерфейса:
- **P2P**
- **Subnet**

опция `topology`
- `p2p`
- `subnet`

subnet реализует виртуальную сеть, роутинг реализуется внутри openvpn. С опцией client-to-client клиенты могут общаться между собой. Используется в multiclient конфигурации

в режиме p2p все подключения имеют свой tun/tap интерфейс, роутинг и свитчинг осуществляется на стороне ОС. Основной режим в site2site конфигурации.

OpenVPN

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

psk - самый простой способ, используется в site2site, удобен для создания full mesh vpn-сетей.

Режимы аутентификации:
- **PSK**
- **Certificate-based**
- **Password based**

certificate-based используется в случае, когда одна из сторон (клиент) - не является доверенной. Используются обыкновенные ssl сертификаты, со сроком действия, возможностью отзыва самый удобный способ раздачи доступа клиентам, т.к. сертификат можно напрямую прописать в файл конфигурации

OpenVPN

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

Мета-опция `server` за вас конфигурирует часть параметров. Предпочитаю не использовать.

Опция `ccd` позволяет для каждого пользователя, имя которого берется из, собственно, имени пользователя или CN сертификата, иметь свой динамический конфиг

Опция `config` позволяет включать куски общего конфига. Интересна для full-mesh vpn или при использовании ccd

Опции `up`, `down`, `down-pre`, `client-connect`, `client-disconnect` позволяют использовать скрипты для конфигурации сети при соответствующих событиях.

Site-to-Site конфигурация

Или самая простейшая. https://openvpn.net/index.php/open-source/documentation/miscellaneous/78-static-key-mini-howto.html

```
openvpn --genkey --secret static.key
```

```
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret static.key
```

```
remote myremote.mydomain
dev tun
ifconfig 10.8.0.2 10.8.0.1
secret static.key
```


Multiclient with SSL

```
local 1.2.3.4
port 1194

dev tun
mode server
proto udp
topology subnet
client-to-client

tls-server
dh   ssl/OpenVPN-DH-1024.pem
ca   ssl/OpenVPN-CA.crt
cert ssl/OpenVPN-Server.crt
key  ssl/OpenVPN-Server.key
cipher AES-256-CBC

client-config-dir ccd

ifconfig 10.17.2.1 255.255.255.0
ifconfig-pool 10.17.2.16 10.17.2.32 255.255.255.0

ping 10
ping-restart 120

log "/var/log/openvpn-server.log"
verb 3
status "/var/log/openvpn-server.status"
script-security 2
```

Для создания ssl можно использовать Easy RSA, который везде рекомендуют, но лучше один раз разобраться в openssl. Пример тут: https://github.com/thedolphin/openvpn-configs/tree/master/auth

Эти же скрипты пригодятся для создания собственного CA

Бонус. AnyConnect/OpenConnect

https://ocserv.gitlab.io/www/index.html, в EPEL - ocserv/openconnect

Для сложных случаев. Работает поверх HTTPS. Реализует Cisco проприетарный протокол AnyConnect. Может работать как клиент к Cisco ASA или как сервер для Cisco AnyConnect-клиентов. Cisco Anyconnect можно достать для любой платформы, что дополнительно упростит вашу жизнь.

Спасибо за внимание!

Вопросы?