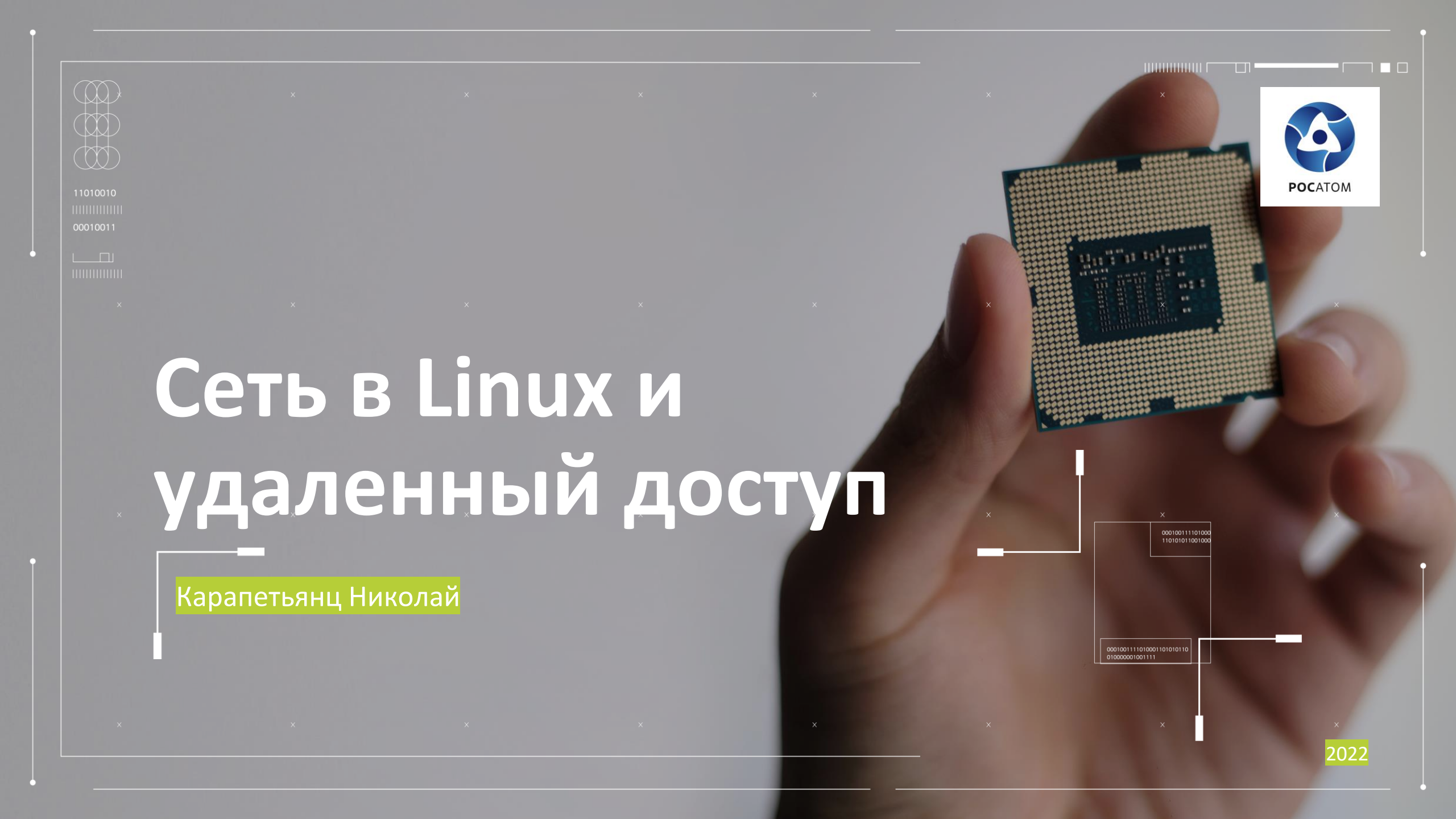
Сеть в Linux и удаленный доступ

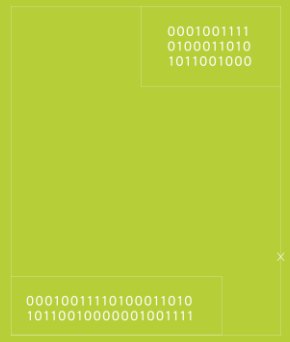
Карапетьянц Николай



2022

СОДЕРЖАНИЕ

- Модель OSI
- Протоколы
- Управление сетью
- VPN
- SSH
- RDP, VNC
- UFW, IPtables



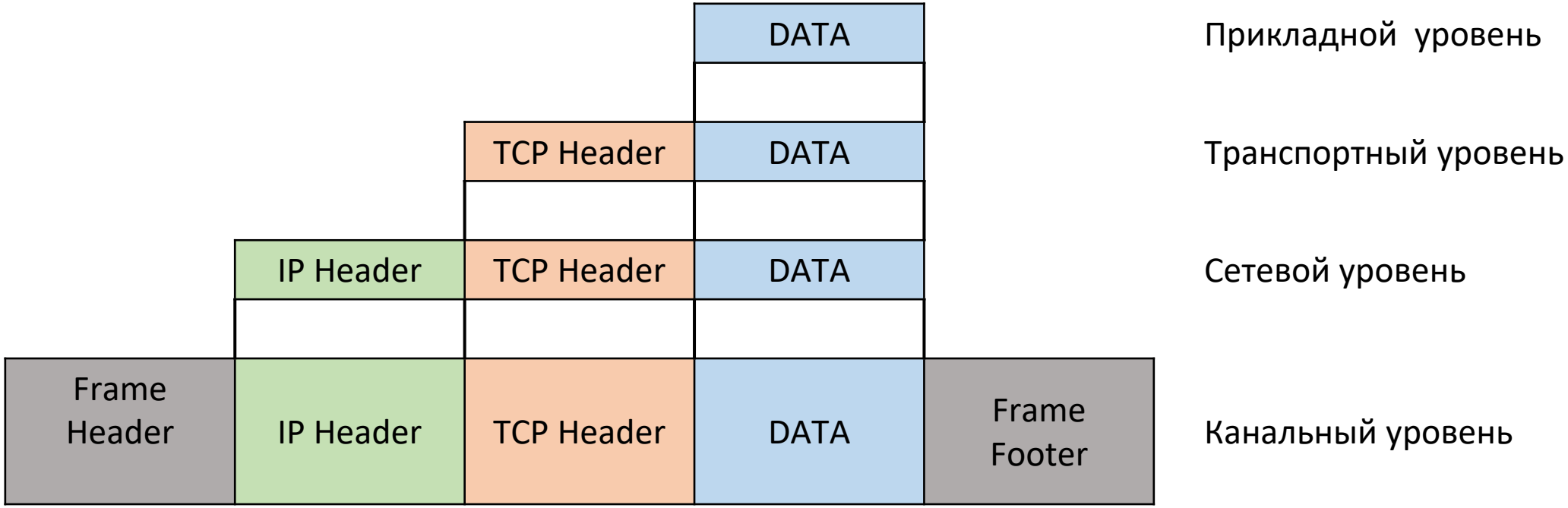
2022

МОДЕЛЬ OSI

OSI – модель взаимодействия открытых систем.

Уровень	Вид информации	Функции	Протоколы
Прикладной	Данные	Обеспечение взаимодействие между пользователем и сетью	HTTP, FTP, Telnet, SSH, SNMP
Представления	Данные	Преобразование данных в нужный вид	MIME, SSL
Сеансовый	Данные	Управление сеансом связи	L2TP, RTCP
Транспортный	Блоки	Обеспечение доставки данных без ошибок	TCP, UDP
Сетевой	Пакеты	Маршрутизация(логическая адресация)	IP, ICMP, IGMP, BGP, BGP, OSPF
Канальный	Кадры	Физическая адресация	ARP, PPP, IEEE 802.11
Физический	Биты	Обеспечение передачи данных в разных средах	IEEE 802.11, ISDN

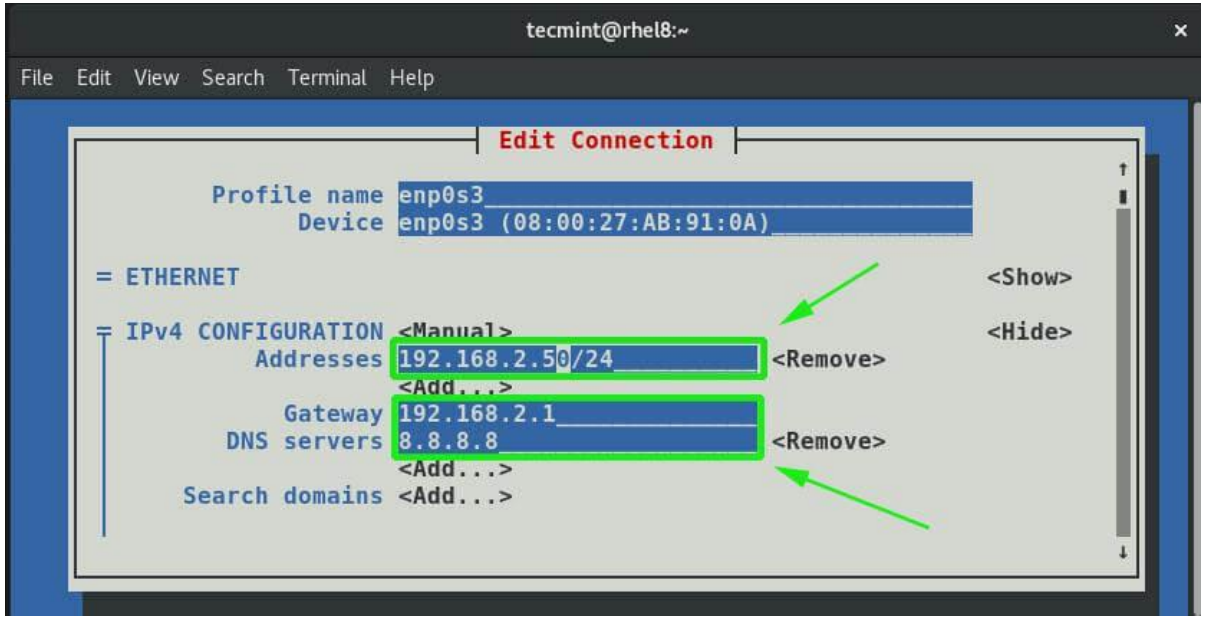
TCP/IP


DATA
TCP Header
DATA
IP Header
TCP Header
DATA
Frame Header
IP Header
TCP Header
DATA
Frame Footer
Прикладной уровень
Транспортный уровень
Сетевой уровень
Канальный уровень

ПРОТОКОЛЫ

ARP	Address Resolution Protocol	преобразование сетевых адресов в адреса физических устройств MAC
RARP	Reverse Address Resolution Protocol	преобразование MAC–адреса в IP–адрес
DHCP	Dynamic Host Configure Protocol	автоматизация конфигурирования хоста
IP	Internet Protocol	маршрутизация пакетов в сети Internet
ICMP	Internet Control Message Protocol	контроль сообщений в сети Internet
IDRP	ICMP Router–Discovery Protocol	обнаружение маршрутизатора
UDP	User Datagram Protocol	передача блоков данных без подтверждения соединения
TCP	Transfer Control Protocol	передача блоков данных с подтверждением соединения

УПРАВЛЕНИЕ СЕТЬЮ



Network–manager – системная сетевая служба для управления сетевыми устройствами.

Функции:

- Wi–Fi подключение
- Подключение к WWAN
- Ethernet–подключение
- Создание точки доступа
- Общее подключение

РАБОТА С СЕТЬЮ

Вспомогательные утилиты:

ping – проверка доступности хоста

traceroute – трассировка маршрута до определенного хоста

ip – базовая утилита для управления сетью

nslookup – интерактивные запросы к DNS

nmap – сканирование сети и портов

dig – запрос информации о домене

mtr – отображение статистики трассировки

tcpdump – анализатор заголовков пакетов

wget – скачать файл

netstat – отображение статистики сети

host – информация о домене

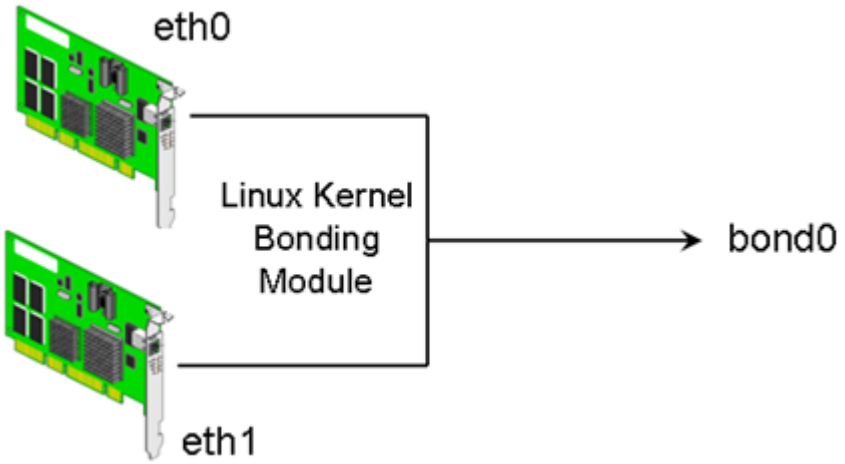
nc – прослушивание порта, создание соединения TCP/UDP

КОНФИГУРАЦИОННЫЕ ФАЙЛЫ

- **/etc/hosts** – перечень IP адресов и соответствующих им имен
- **/etc/networks** – определяет порядок поиска имени хоста/сети
- **/etc/resolv.conf** – содержит список DNS серверов
- **/etc/nsswitch.conf** – определяет порядок поиска имени хоста/сети
- **/etc/netplan/*** – конфигурационные файлы сетевых интерфейсов
- **/etc/network/interface** – конфигурации сетевых интерфейсов (используется в предыдущих версиях и Debian)

LINUX BOND

Bonding – механизм объединения сетевых интерфейсов в Linux для повышения пропускной способности и отказоустойчивости сети.

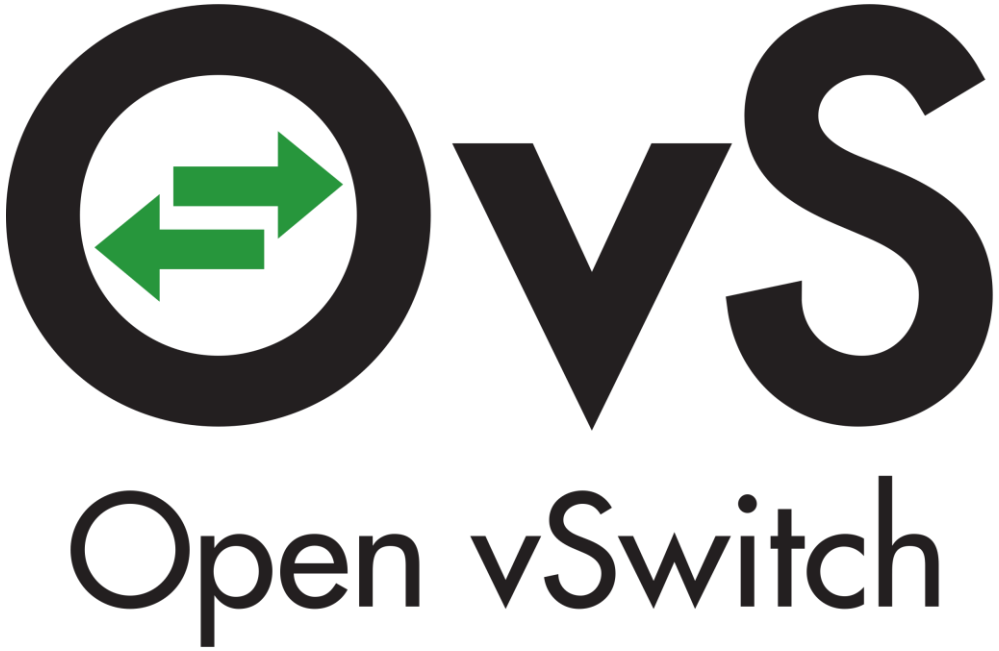


OPENSWITCH

Возможности:

- LACP (IEEE 802.1AX–2008)
- 802.1Q VLAN
- IPv6 support
- Per VM interface traffic policing
- BFD and 802.1ag link monitoring
- Multicast snooping

…..



OPENVPN

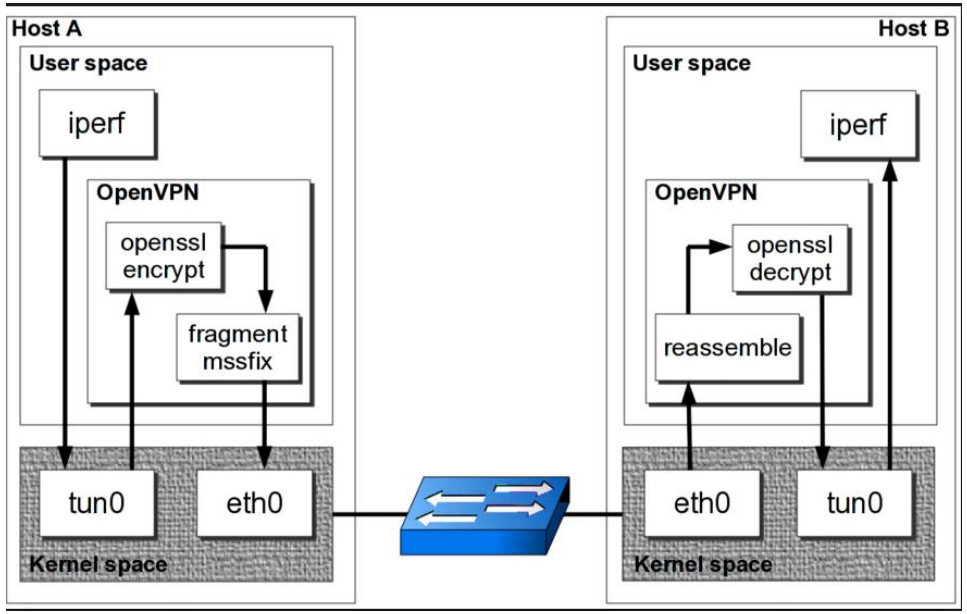
Свободная реализация технологии виртуальной частной сети с открытым исходным кодом для создания зашифрованных каналов типа точка–точка или сервер–клиенты между компьютерами.

Работает на уровнях 2 и 3 модели OSI

OPENVPN

Возможности:

- шифрование с использованием TLS
- поддержка 802.11Q
- гибкая настройка системы аутентификации
- работа через UDP или TCP
- мультиплатформенность

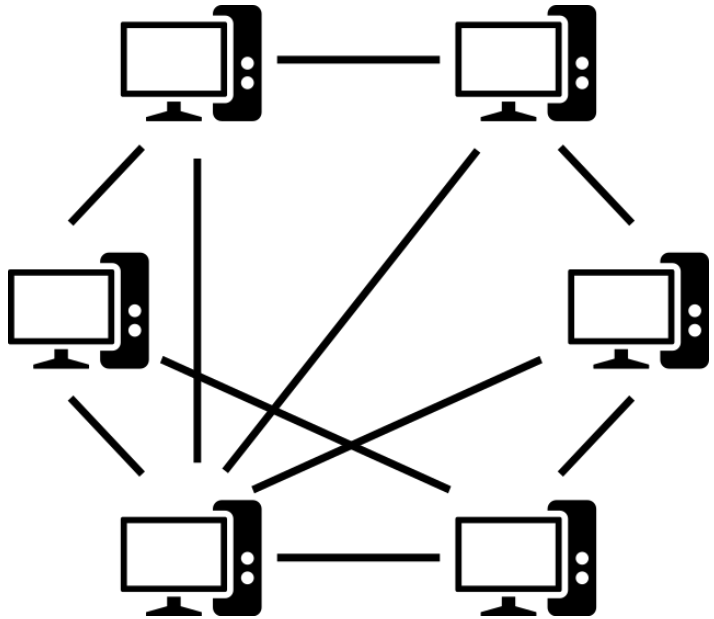


WIREGUARD

Возможности:

- простой в настройке
- маленький объем кодой базы
- мультиплатформенность
- высокая скорость работы

Работает на 3 уровне модели OSI.

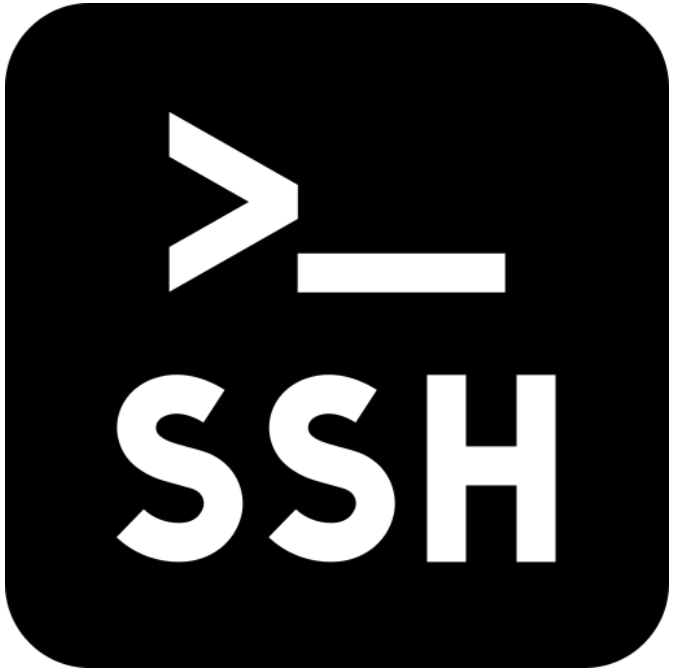


SSH

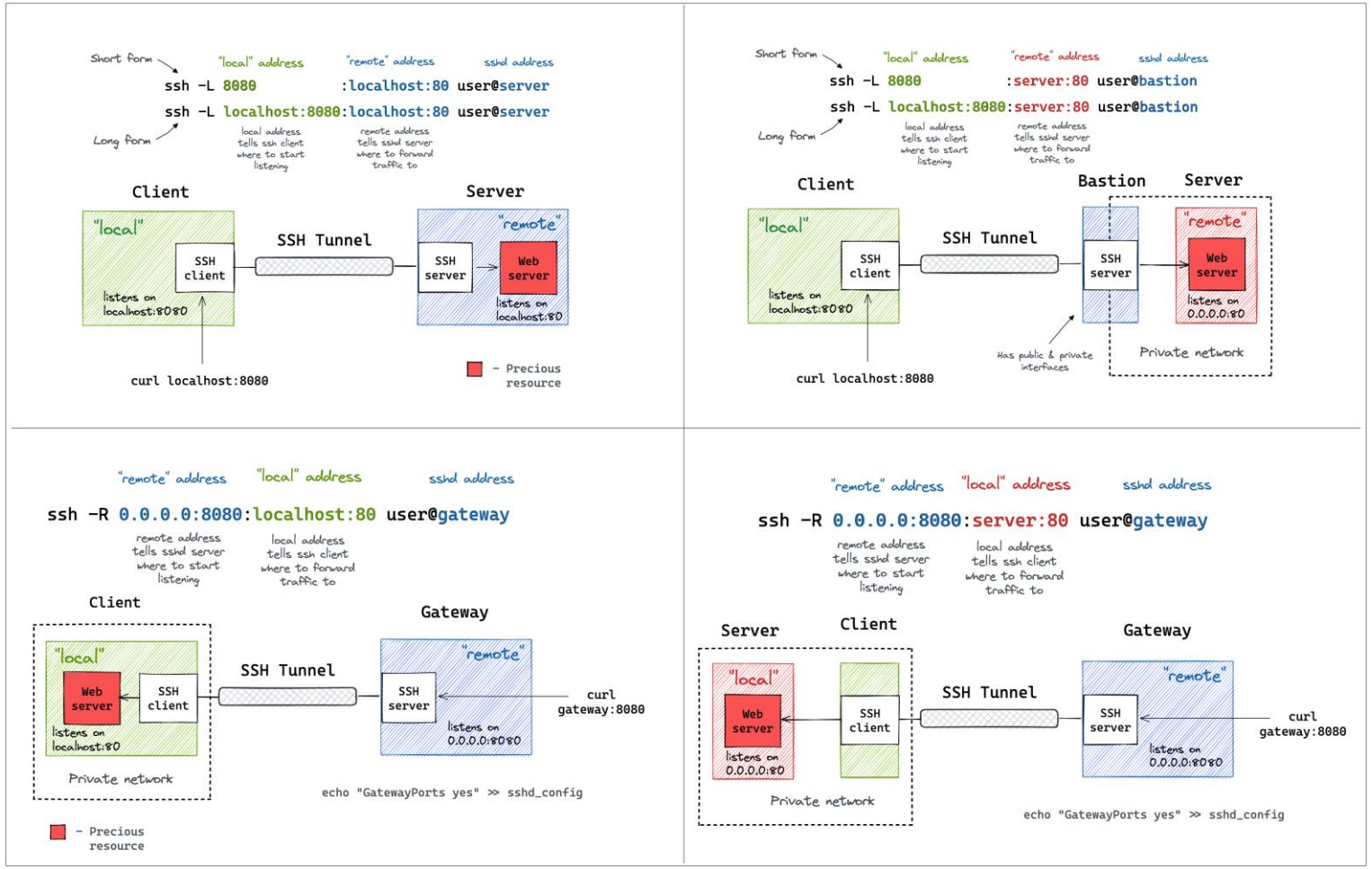
Secure Shell – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP–соединений.

Возможности:

- Безопасный удаленный вход в систему
- Безопасная передача файлов
- Безопасное удаленное выполнение команд
- Гибкая система аутентификации
- Контроль доступа
- Проброс портов



SSH ТУННЕЛИРОВАНИЕ



https://iximiuz.com/ssh–tunnels/ssh–tunnels.png

RDP, VNC

RDP - протокол удалённого рабочего стола.

FreeRDP – реализация с открытым исходным кодом.

Хорошо совместим с ОС семейства Windows.

VNC - система удалённого доступа к рабочему столу компьютера, использующая протокол RFB.

Легковесное программное обеспечение для задач администрирования с открытым исходным кодом.

IPTABLES

Встроенный межсетевой экран в Linux.
Обеспечивает проверку пакетов и их обработку в соответствии с заданными цепочками правил в системе.

Виды правил:

- input – входящие пакеты и подключения
- forward – пересылаемые пакеты
- output – исходящие пакеты и сведения
- prerouting – предобработка пакета
- postrouting – все пакеты после цепочки forward

IPTABLES

Действия:

- ACCEPT – разрешить пакет
- DROP – отбросить пакет
- REJECT – отклонить пакет и вывести сообщение пользователю
- LOG – сделать запись о пакете в лог файл
- QUEUE – оправить пакет пользовательскому приложению

Таблицы – уровень абстракции выше уровня цепочки правил. Используются для выполнения действий над пакетами.

Виды таблиц:

- raw – для обработки сырых пакетов
- mangle – для модификации пакетов
- nat – преобразование сетевых адресов
- filter – фильтрация пакетов

IPTABLES

$ iptables –t таблица действие цепочка дополнительные_параметры

Действие:
–A – добавить правило в цепочку
–C – проверить все правила
–D – удалить правило
–I – вставить правило с нужным номером
–L – вывести все правила в текущей цепочке
–S – вывести все правила
–F – очистить все правила
–N – создать цепочку
–X – удалить цепочку
–P – установить действие по умолчанию

Доп. параметры:
–p – указать протокол, один из tcp, udp, udplite, icmp, icmpv6, esp, ah, sctp, mh
–s – указать ip адрес устройства–отправителя пакета
–d – указать ip адрес получателя
–i – входной сетевой интерфейс
–o – исходящий сетевой интерфейс
–j – выбрать действие, если правило подошло

UFW

Uncomplicated FireWall – надстройка над Iptables для простой работы с правилами.

$ ufw опции действие параметры

Опции:

- **—version** – вывести версию брандмауэра
- **—dry–run** – тестовый запуск, никакие реальные действия не выполняются

Действия:

- **enable** – включить фаерволл и добавить его в автозагрузку
- **disable** – отключить фаерволл и удалить его из автозагрузки
- **reload** – перезагрузить файервол
- **default** – задать политику по умолчанию
- **logging** – включить журналирование или изменить уровень подробности
- **reset** – сбросить все настройки до состояния по умолчанию
- **status** – посмотреть состояние фаервола
- **show** – посмотреть один из отчётов о работе
- **allow** – добавить разрешающее правило
- **deny** – добавить запрещающее правило
- **reject** – добавить отбрасывающее правило
- **limit** – добавить лимитирующее правило
- **delete** – удалить правило

UFW

```
$ ufw allow имя_службы
$ ufw allow порт
```

```
$ ufw allow порт/протокол
$ ufw allow направление порт
```

```
$ ufw allow in on ethin out on ethout from ip_источника
```

```
$ ufw allow proto протокол from ip_источника to ip_назначения port порт_назначения
```

ССЫЛКИ

- Сетевые адаптеры VirtualBox: https://www.nakivo.com/blog/virtualbox–network–setting–guide/
- Управление сетью в Ubuntu https://help.ubuntu.com/community/InternetAndNetworking?action=show&redirect=Internet
- OpenvSwitch: https://www.openvswitch.org/features/
- Ubuntu Bonding: https://help.ubuntu.com/community/UbuntuBonding
- Настройка UFW: https://losst.pro/nastrojka–ufw–ubuntu
- Настройка Iptables: https://losst.pro/nastrojka–iptables–dlya–chajnikov
- Установка Freerdp: https://sanotes.ru/ustanovka–freerdp–v–ubuntu–debian/
- Настройка VNC: https://www.digitalocean.com/community/tutorials/how–to–install–and–configure–vnc–on–ubuntu–20–04–ru
- Настройка Wireguard: https://www.procustodibus.com/blog/
- Безопасная настройка SSH https://adminguide.ru/2021/02/01/nastrojka–bezopasnosti–ssh–soedineniya/