**Глава 14. Устранение неполадок в сети**

**1) Понмание адресации TCP/IP**

Основной единицей сети является IP-адрес, который должен быть назначени каждому устройству сети и долже быть уникальным. IPv4 имеет 4 восьмибитных октета – 32 бита, максимальное число адресов около 4 миллиардов (2564). Этого нехватает для всех устройств в мире, только Андроид смартфонов больше 1 миллиарда.

Решения проблемы адресации:

* Переход на новый стандарт IPv6
* Механизм NAT (преобразование адресов).

**1.1. NAT адресация**

Основана на том, что публичный IP адрес имеет только маршрутизатор, который соединен непосредственно с глобальной сетью, а устрйоствам, присоединенным к этому маршрутизатору назначать локальные (частные) адреса. За назначание частных NAT адресов отвечает DHCP.

**1.2. Работа с адресацией NAT.**

Протокол NAT выделяет 3 диапазона адресов IPv4 (17 млн адресов):

* 10.0.0.0 – 10.255.255.255
* 172.16.0.0 – 172.31.255.255
* 192.168.0.0-192.168.255.255

Для разделения групп ресурсов, чтобы давать доступ одним группам и не давать другим, Обычно выделенные адреса разделяют на подсети: 192.168.1.x, 192.168.2.x. (DHCP не назначает x = 0, 1, 255)

Стандарты обозначения подсетей:

* CIDR : 192.168.1.0/24
* Масочная : 192.168.1.0 255.255.255.0

**2) Установление сетевого подключения**

Если что-то в сети не работает, то следует поэтапно искать неисправность, от локальных проблем (сбой оборудования на локальном компьютере), до глобальных (звонка провайдеру).

**3) Устранение неполадок исходящего соединения**

Возможно, после всего компьбтер так и не получил сетевой адрес, посмотреть это можно, вызвав:

* ip addr

**3.1 Отслеживание статуса сети**

**Peripheral Component Interconnect (**PCI) – аппаратный стандарт, используемый для подключения перефирийных устройств к материнской плате через шину PCI. Существуют и новые стандарты - PCI Express (PCIe).

Нужно убедиться, что компьютер видит сетевой адаптер(карту) PCI:

* lspci
* lshw -class network

Проверить записи, связанные с Ethernet, в записях, связанных с ядром и устройсвами:

* dmesg | grep -A 2 Ethernet

Проверить записи, свзяанные с eth0^

* dmesg | grep eth0 (если будет строка renamed from, значит некое устройство было переименовано, к примеру с eth0 в enp1s0)

**3.2 Назначение IP адресов**

Сетевые устройства могут получить свой адрес 2 способами:

* Вручную
* Автоматически, DHCP сервер сделаетт это

DHCP сервер гарантирует то, что адреса не будут повторяться, но не гарантирует, что они будут всегда одинаковы, что может стать проблемой при подключении по SSH.

**Определение сетевого маршрута**

* ip route – (просмотр таблицы маршрутизации компьютера)
  + default via 192.168.0.1 - адрес шлюза маршрутизации, через котор. Лок. Комп. Получает доступ к остальной сети
  + 192.168.0.0/24 - cеть NAT и маска локальной сети NAT

Если рабочего маршрута в списке нет, надо его создать. Если есть други компьютеры, использующие ту же сеть:

УНАЕМ их IP адрес→ к примеру, 192.168.1.34, отсбда можно предположить, что адрес маршрутизатора 192.168.1.1,

Eсли IP адрес → 10.0.0.45, отсюда можно предположить, что адрес маршрутизатора 10.0.0.1.

Команда для создания нвоого маршрута по умолчанию к шлюзу:

* ip route add default via 192.168.1.1 dev eth1

**Запрос динамического адреса**

Для получения адреса, следует запустить dhclient, для поиска сервера DHCP в нашей сети (Если адрес уже есть, то, возможно, будет: RTNETLINK answers: File exists):

* dhclient eth1

**Конфигурирование статического адресации**

Можно присвоить временный статический ip адрес, который будет действовать до следующей презагрузки системы:

* ip addr add 192.168.1.10/24 dev eth0

Для постоянного изменения, следует отредактировать файл /etc/network/interfaces/,

он может содержать раздел, указывая, что интерфейс dhcp, но это можно изменить на static, введя желаемый IP-адрес, маску сети (x.x.x.x) и IP-адрес шлюза.

В CentOS каждый интерфейс имеет свой файл конфигураций в каталоге /etc/sysconfig/network-scripts/. . см файл ifcg-enp0s3. Основное : BOOTPROTO=none – отключение dhcp.

Чтобы изменения вступили в силу, нужно перезагрузить сеть или интерфейс:

* systemctl restart network
* ip link set dev eth1 up

В некоторых местах NetworkManager скрывает свои рабочие файлы:

* /etc/NetworkManager/NetworkManager.conf – общий файл конфигурации
* /etc/NetworkManager/system-connections/ - файлы конфигураци для каждого сетевого подключения, которые устанвавливал компьютер за все время работы.
* /var/lib/Netwo rkManager/. - данные, описывающие DHCP компьютера.

**3.3. Конфигурирование службы DNS**

Система доменных имен (DNS) – интсрумент, которй переводит текст (wikipedia.org) в IP-адреса (208.80.153.244).

Проверить работу можно пропинговав сначала через ip адрес сайта, потом пропинговав через название(wikipedia.org),если через имя не сработает, то дело в DNS.

Настроить параметры DNS можно на маршрутизаторе, а можно на компьютере:

* /etc/network/interfaces (Ubuntu) dns-nameserver1 8.8.8.8 (Google)
* /etc/sysconfig/network-scripts/ifcg-enp0s3 (CentOS) DNS1=8.8.4.4 (OpenDNS)

**3.4 Обслуживание сети**

Если есть рабочий интерфейс, маршрут, IP-адрес и служба DNS работает, но все ще нет связи, значит что-то блокирует поток.

Маршрут прохождения потока (traceroute):

* traceroute google.com (\* - устройства, которые не могут вернуть пакет, Ошибка – полный сбой).

Если все еще ничего не работает, то следует позвонить провайдеру.

**4) Устранение неполадок при входящем соединении**

Всегда следует знать о сотсоянии сети при входящем трафике, чтобы клиенты могли подключиться и получить быстрый доступ к ресурсам.

**4.1 Сканирование внутреннего соединения: netstat**

**Сокет – IP-адрес сервера + порт (192.168.0.1:80)**

Просмотр списка служб, прослушивающих сетевые запросы:

* netstat -l | grep http (-l – все отрытые сокеты. Http – оставить только http)

Вывод сетевых интерфейсов:

* netstat -i (lo - localhost)
  + RX,TX – сколко передано пакетов, получено
  + OK – безошибочная передача
  + ERR – поврежденные пакеты
  + DRP – отброшенные пакеты.

**4.2 Сканирование внешнего соединения: netcat**

**netcat** может быть использован для потоковой передачи фалов по сети или в качестве приложения для чата (функционал наряду с cat, zcat).

Запуск по удаленному адресу:

* nc -z -v bootstrap-it.com 443 80
  + -z – ограничивает сканирование демонами
  + -v – добавляет подробности к выводу
  + + Порты которые нужно сканировать
* nmap -sT -p80 bootstrap-it.com
* nmap -sT -p1-1023 bootstrap-it.com (сканируем открытые порты от 1 до 1023)