Администрирование Linux
Лекция 4.1
Настройка сети (практика)

Иртегов Д.В.

Новосибирский гос. Университет

2014/2023

Минимальная информация, необходимая для настройки IP

- Ваш адрес
- Маска вашей подсети
- Роутер по умолчанию (default router)
- Имя вашего хоста
- Список DNS серверов
- Домен поиска по умолчанию (не обязательно)

Инструменты для диагностики

- ping – шлет ICMP ECHO
- traceroute – шлет ICMP ECHO или TCP SYN с ограниченным TTL
- tcptraceroute – TCP SYN с ограниченным TTL
- host – разрешает имя хоста по hosts/dns/другим механизмам
- nslookup – диагностика DNS

Сетевые интерфейсы

- Ethernet/WiFi
  - Появляются при загрузке драйвера, обычно при загрузке ОС или при hot-plug устройства
  - «Не устройства»: не являются ни символьными, ни блочными устройствами и не имеют файла в /dev
    - Этим Линукс отличается от традиционных юниксов (System V, BSD)
  - Список устройств видно в файле /proc/net/dev
  - Ethernet называются eth[0-9], WiFi – wlan[0-9]

Сетевые интерфейсы

- PPP и туннели
  - Интерфейс поднимается userland-демоном pppd после настройки соединения
  - Физический порт, который используется для соединения с модемом (COM, LPT, USB, eth) сетевым интерфейсом не является

Способы настройки сети

- ifconfig, ip
  - Теряется при перезагрузке
- Network Manager
  - GUI
  - Удобен на ноутбуках (можно быстро подключиться к WiFi или чужой сети)
  - Доступен также nmcli
  - Сохраняет изменения при перезагрузке
- Скрипты /etc/sysconfig/network-scripts (RH) или /etc/network (Debian/Ubuntu)
  - Выпилены в RHeL8 и Ubuntu 22.04
- Systemd-networkd
  - Конфигурация на основе текстовых файлов
  - Можно делать все (brigde, bonding, vlan…)

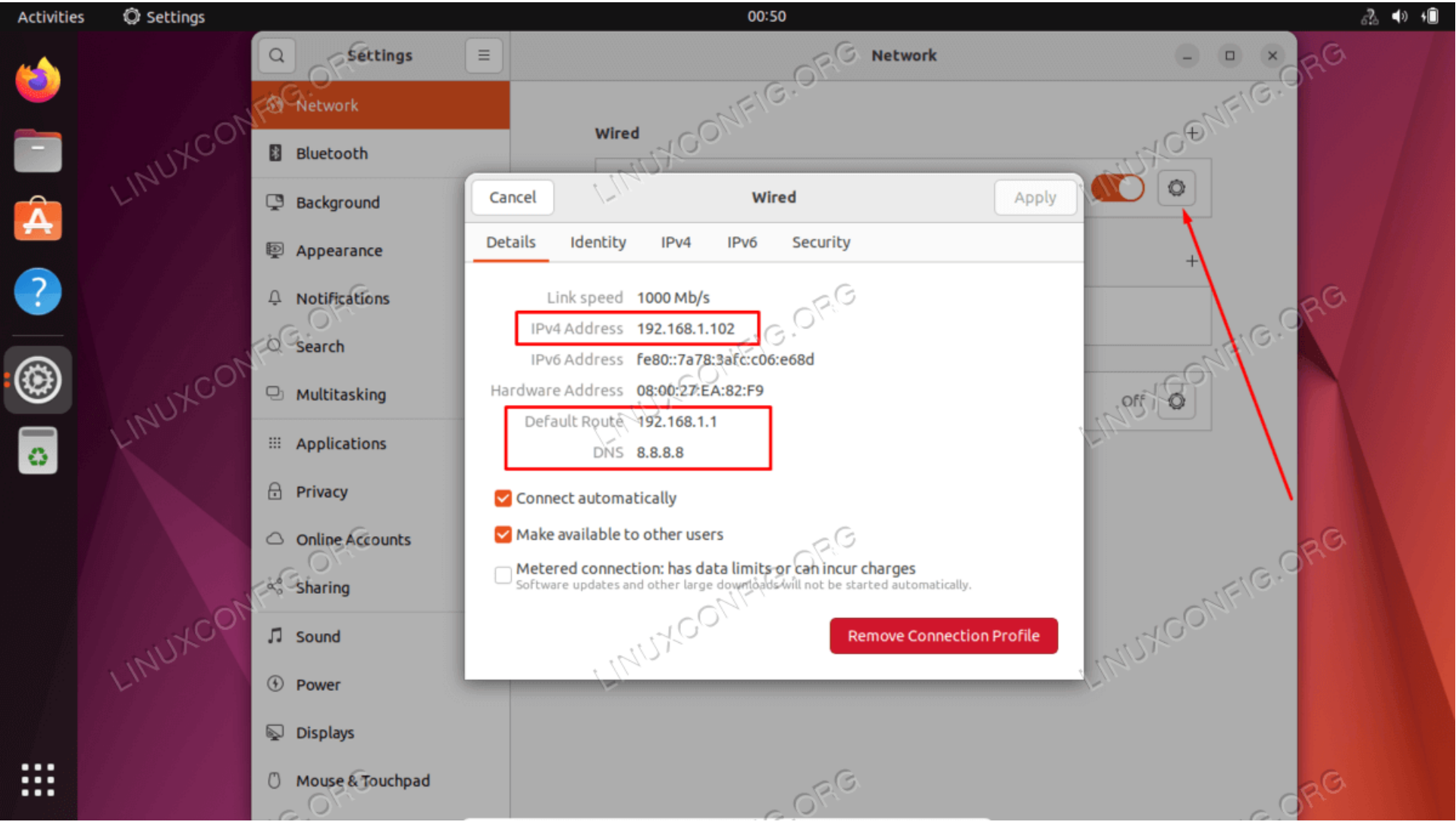
ifconfig, ip, dhclient

- /sbin/ifconfig - считается устаревшим
  - Без параметров – список интерфейсов
  - ifconfig eth0 команда параметры
  - ifconfig eth0 10.4.16.181/24 up
  - ifconfig eth0 address 10.4.16.181 netmask 255.255.255.0
- /sbin/ip – управляет интерфейсами, таблицами маршрутизации, политиками
  - ip link show – список интерфейсов
  - ip address show – список интерфейсов с IP адресами
  - ip address add 10.4.16.181/24 dev eth0
  - ip route add default 10.4.16.1 dev eth0
  - ip neighbor show – ARP таблица
- dhclient – скрипт для настройки через dhcp

Упражнение

- Определите список интерфейсов, их MAC и IP адреса, маску подсети, маршрутизатор по умолчанию

Network Manager



Где он сохраняет настройки

- /run/NetworkManager/system-connections
- /etc/NetworkManager/system-connections
- `sudo nmcli -f NAME,DEVICE,FILENAME connection show`

Демонстрация

- Настройка сети через Network Manager

Упражнение

- Через Network Manager, настройте
  - Включение сети при старте системы
  - Статический IP адрес
    - Не используйте тот же адрес, что раздает DHCP! Если вы неделю не подтверждаете lease, он может раздать тот же адрес другому узлу!
    - Используйте адреса которые укажет преподаватель
  - Netmask и default router возьмите те же, что раздает DHCP
  - Попытайтесь зайти на вашу машину через putty или другой ssh клиент

/etc/sysconfig/network-scripts

- Исполняются при старте системы из /etc/init.d/network
- Настройки интерфейсов хранятся в файлах /etc/sysconfig/network-scripts/ifcfg-IF
  - На самом деле, эти файлы – скрипты, они исполняются командой . (source)
  - Вставлять туда команды не рекомендуется, они могут выполняться в неожиданные моменты
  - В этих файлах настраиваются переменные shell
- Есть инструменты для настройки
  - system-config-network, system-config-network-tui

ifcfg-eth0 и ifcfg-lo

```
[fat@ws53 ~]$ cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=08:00:27:A9:9A:8D
TYPE=Ethernet
UUID=64264d27-f0e6-48f4-a038-3cb375af1e22
ONBOOT=no
NM_CONTROLLED=yes
BOOTPROTO=dhcp
[fat@ws53 ~]$ cat /etc/sysconfig/network-scripts/ifcfg-lo
DEVICE=lo
IPADDR=127.0.0.1
NETMASK=255.0.0.0
NETWORK=127.0.0.0
# If you're having problems with gated making 127.0.0.0/8 a martian,
# you can change this to something else (255.255.255.255, for example)
BROADCAST=127.255.255.255
ONBOOT=yes
NAME=loopback
```

Параметры в ifcfg-IF

- BOOTPROTO=none|bootp|dhcp
- IPADDR=address
- IPV6INIT=yes|no
- MACADDR=MAC-48
  - Позволяет заменить MAC-адрес интерфейса (у разных адаптеров и драйверов механизм замены разный)
- NETMASK=mask
- NM_CONTROLLED=yes|no
- ONBOOT=yes|no
- PEERDNS=yes|no
  - Менять настройки DNS при подъеме этого интерфейса
- GATEWAY=address
  - Есть также глобальная настройка в /etc/sysconfig/network

Systemd-networkd

- Конфигурация в текстовых файлах в /etc/systemd/network
- Windows-ini-style конфиги

```
$ cat /etc/systemd/network/wired-dhcp.network
[Match]
Name=eth*
[Network]
DHCP=ipv4
DHCP=ipv6
```

ssh(1)

- Secure SHell
- RFC 4251 (ssh-2)
- Основное средство удаленного управления Unix-серверами
- Клиенты и серверы доступны также для Windows
- Использует
  - Порт TCP 22 (настраивается на сервере)
  - RSA и DSA для аутентификации,
  - широкий набор шифров с секретным ключом для шифрования сессии

Использование ssh

- ssh [user@]host
  интерактивная сессия shell
  - Если user@ не задан, использует $USER
  - Также ssh -l username hostname
- ssh [user@]host cmd
  запускает команду cmd на узле host
  - ssh server cat file | dd of=file
- scp file [user@]host:file
  - Есть специальное расширение sftp

Как работает ssh

- При установке сервер генерирует пару приватный-публичный ключ RSA или DSA
- Сервер предъявляет публичный ключ при подключении клиента и использует его для согласования сессионного ключа шифрования
- Клиент записывает публичный ключ в ~/.ssh/known_hosts

Как работает ssh (клиентский ключ)

- Пользователь может создать свою пару ключей командой ssh-keygen
- Они размещаются в ~/.ssh/id_dsa и id_dsa.pub
- Приватный ключ можно защитить паролем (passphrase)
- При соединении, клиент предъявляет id_dsa.pub серверу. Если у пользователя на сервере есть соответствующий ключ в ~/.ssh/authorized_keys, сервер примет авторизацию без пароля
- Для копирования id_dsa.pub есть утилита ssh-copy-id (нужно ввести пароль)

Что еще умеет ssh

- ssh -X – форвардинг X11 (удаленный запуск графических приложений)
- ssh -L port:localip:localport – форвард произвольного порта TCP
- ssh -R remoteport:localip:localport – форвард в обратную сторону
- ssh –c blowfish-cbc – алгоритм шифрования сессии
- ssh –b – указать исходящий адрес для TCP соединения

Упражнение

- Создать пару ключей DSA
  - ssh-keygen -t dsa , остальное он спросит (согласиться)
- Настроить авторизацию по ключу на parallels.nsu.ru
  - ssh-copy-id [user@]parallels.nsu.ru
- Дополнительно: скопировать ключи на Windows машину, сконвертировать утилитой puttygent в формат putty и настроить авторизацию по тому же ключу из putty

Теперь немножко ужасов

Spoofing

- Мы видели, что адреса канального и сетевого уровня можно задать
- Это открывает возможность подмены исходящего адреса: spoofing
- Например, вы ждете ответа от google.com, а получаете от хакера за соседним компьютером
- С connection-based протоколами работает не очень хорошо (но тоже работает)

Что с этим делать

- Не доверяйте IP-адресу как средству аутентификациии
  - Следствие – роль файрволлов в системе безопасности, в лучшем случае, вспомогательная
- Опирайтесь на аутентификационные протоколы прикладного уровня (ssh, SSL/TLS)
- Помните, что существуют также аутентификация сетевого (VPN) и канального (IEEE 802.1x) уровней