Version : **2022.01**

Updated : 2022/06/05 17:58

LCE513 - Managing the Network

Contents

Presentation

RHEL/CentOS 8 uses **Network Manager** to manage the network. Network Manager is composed of two things:

- a service that manages the connections and reports on their status,
- front-ends that use an API to configure the service.

Important : Note that IPv6 is activated by default.

Start by checking the status of the service:

```
[root@centos8 ~]# systemctl status NetworkManager.service
● NetworkManager.service - Network Manager
   Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor pr>
   Active: active (running) since Thu 2021-07-22 05:05:29 EDT; 1 months 7 days ago
     Docs: man:NetworkManager(8)
 Main PID: 1002 (NetworkManager)
    Tasks: 3 (limit: 23535)
   Memory: 6.8M
   CGroup: /system.slice/NetworkManager.service
           └─1002 /usr/sbin/NetworkManager --no-daemon

Warning: Journal has been rotated since unit was started. Log output is incomplete or>
lines 1-11/11 (END)
```

```
[^q] <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<Type CONTROL Q
```

The nmcli Command

The Network Manager Command Line Interface or **nmcli** is used to configure NetworkManager.

The command line switches of the nmcli command are:

```
[root@centos8 ~]# nmcli help
Usage: nmcli [OPTIONS] OBJECT { COMMAND | help }

OPTIONS
  -a, --ask                                      ask for missing parameters
  -c, --colors auto|yes|no                       whether to use colors in output
  -e, --escape yes|no                            escape columns separators in values
  -f, --fields <field,...>|all|common            specify fields to output
  -g, --get-values <field,...>|all|common        shortcut for -m tabular -t -f
  -h, --help                                     print this help
  -m, --mode tabular|multiline                   output mode
  -o, --overview                                 overview mode
  -p, --pretty                                   pretty output
  -s, --show-secrets                             allow displaying passwords
  -t, --terse                                    terse output
  -v, --version                                  show program version
  -w, --wait <seconds>                           set timeout waiting for finishing operations

OBJECT
  g[eneral]       NetworkManager's general status and operations
  n[etworking]    overall networking control
  r[adio]         NetworkManager radio switches
  c[onnection]    NetworkManager's connections
  d[evice]        devices managed by NetworkManager
  a[gent]         NetworkManager secret agent or polkit agent
```

```
  m[onitor]       monitor NetworkManager changes
```

LAB #1 - Configuring the Network

1.1 - Connections and Profiles

NetworkManager uses **connections** and **profiles** that allow for different configurations of the same interface or **device**. To see the current connections, use the following command:

```
[root@centos8 ~]# nmcli c show
NAME    UUID                                  TYPE      DEVICE
ens18   fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  ens18
virbr0  03f6c432-2a09-47e7-9693-208431a572ee  bridge    virbr0
```

Now create another profile attached to **ens18** :

```
[root@centos8 ~]# nmcli connection add con-name ip_fixed ifname ens18 type ethernet ip4 10.0.2.46/24 gw4 10.0.2.1
Connection 'ip_fixed' (0f48c74d-5d16-4c37-8220-24644507b589) successfully added.
```

Check that it is visible:

```
[root@centos8 ~]# nmcli c show
NAME     UUID                                  TYPE      DEVICE
ens18    fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  ens18
virbr0   03f6c432-2a09-47e7-9693-208431a572ee  bridge    virbr0
ip_fixed 0f48c74d-5d16-4c37-8220-24644507b589  ethernet  --
```

Note that the output does not show that the **ip_fixed** profile is associated with **ens18** device because it has not yet been activated:

```
[root@centos8 ~]# nmcli d show
GENERAL.DEVICE:                         ens18
```

```
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         4E:B1:31:BD:5D:B2
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ens18
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         10.0.2.45/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
IP4.DNS[1]:                             8.8.8.8
IP6.ADDRESS[1]:                         fe80::86b6:8d39:cab2:d84d/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255

GENERAL.DEVICE:                         virbr0
GENERAL.TYPE:                           bridge
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected (externally))
GENERAL.CONNECTION:                     virbr0
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
IP4.ADDRESS[1]:                         192.168.122.1/24
IP4.GATEWAY:                            --
IP4.ROUTE[1]:                           dst = 192.168.122.0/24, nh = 0.0.0.0, mt = 0
IP6.GATEWAY:                            --

GENERAL.DEVICE:                         lo
GENERAL.TYPE:                           loopback
GENERAL.HWADDR:                         00:00:00:00:00:00
GENERAL.MTU:                            65536
GENERAL.STATE:                          10 (unmanaged)
```

```
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
IP4.ADDRESS[1]:                         127.0.0.1/8
IP4.GATEWAY:                            --
IP6.ADDRESS[1]:                         ::1/128
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = ::1/128, nh = ::, mt = 256

GENERAL.DEVICE:                         virbr0-nic
GENERAL.TYPE:                           tun
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          10 (unmanaged)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
lines 28-50/50 (END)
[q]
```

To activate the ip_fixed profile, use the following command:

```
[root@centos8 ~]# nmcli connection up ip_fixed
```

Note that because of the IP address change, your terminal is now blocked.

To do - Reconnect to the VM using the **CentOS8_SSH_10.0.2.46** connection.

The ip_fixed is now activated and the enp0s3 has been disactivated:

```
[root@centos8 ~]# nmcli c show
NAME     UUID                                  TYPE      DEVICE
ip_fixed 0f48c74d-5d16-4c37-8220-24644507b589  ethernet  ens18
```

```
virbr0   03f6c432-2a09-47e7-9693-208431a572ee  bridge    virbr0
ens18    fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  --
[root@centos8 ~]# nmcli d show
GENERAL.DEVICE:                         ens18
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         4E:B1:31:BD:5D:B2
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ip_fixed
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         10.0.2.46/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
IP6.ADDRESS[1]:                         fe80::5223:aee1:998e:9f27/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255

GENERAL.DEVICE:                         virbr0
GENERAL.TYPE:                           bridge
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected (externally))
GENERAL.CONNECTION:                     virbr0
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
IP4.ADDRESS[1]:                         192.168.122.1/24
IP4.GATEWAY:                            --
IP4.ROUTE[1]:                           dst = 192.168.122.0/24, nh = 0.0.0.0, mt = 0
IP6.GATEWAY:                            --

GENERAL.DEVICE:                         lo
GENERAL.TYPE:                           loopback
```

```
GENERAL.HWADDR:                         00:00:00:00:00:00
GENERAL.MTU:                            65536
GENERAL.STATE:                          10 (unmanaged)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
IP4.ADDRESS[1]:                         127.0.0.1/8
IP4.GATEWAY:                            --
IP6.ADDRESS[1]:                         ::1/128
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = ::1/128, nh = ::, mt = 256

GENERAL.DEVICE:                         virbr0-nic
GENERAL.TYPE:                           tun
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          10 (unmanaged)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
lines 27-49/49 (END)
[q]
```

To see the characteristics of **ens18** connection, use the following command:

```
[root@centos8 ~]# nmcli -p connection show ens18
===============================================================================
                    Connection profile details (ens18)
===============================================================================
connection.id:                          ens18
connection.uuid:                        fc4a4d23-b15e-47a7-bcfa-b2e08f49553e
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              ens18
connection.autoconnect:                 yes
connection.autoconnect-priority:        0
```

```
connection.autoconnect-retries:         -1 (default)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1630224060
connection.read-only:                   no
connection.permissions:                 --
connection.zone:                        --
connection.master:                      --
connection.slave-type:                  --
connection.autoconnect-slaves:          -1 (default)
connection.secondaries:                 --
connection.gateway-ping-timeout:        0
connection.metered:                     unknown
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
---------------------------------------------------------------------------
802-3-ethernet.port:                    --
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
802-3-ethernet.mac-address-blacklist:   --
802-3-ethernet.mtu:                     auto
802-3-ethernet.s390-subchannels:        --
802-3-ethernet.s390-nettype:            --
802-3-ethernet.s390-options:            --
802-3-ethernet.wake-on-lan:             default
802-3-ethernet.wake-on-lan-password:    --
---------------------------------------------------------------------------
ipv4.method:                            manual
```

```
ipv4.dns:                               8.8.8.8
ipv4.dns-search:                        ittraining.loc
ipv4.dns-options:                       --
ipv4.dns-priority:                      0
ipv4.addresses:                         10.0.2.45/24
ipv4.gateway:                           10.0.2.1
ipv4.routes:                            --
ipv4.route-metric:                      -1
ipv4.route-table:                       0 (unspec)
ipv4.routing-rules:                     --
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-iaid:                         --
ipv4.dhcp-timeout:                      0 (default)
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.dhcp-fqdn:                         --
ipv4.dhcp-hostname-flags:               0x0 (none)
ipv4.never-default:                     no
ipv4.may-fail:                          yes
ipv4.dad-timeout:                       -1 (default)
ipv4.dhcp-vendor-class-identifier:      --
ipv4.dhcp-reject-servers:               --
---------------------------------------------------------------------------
ipv6.method:                            auto
ipv6.dns:                               --
ipv6.dns-search:                        --
ipv6.dns-options:                       --
ipv6.dns-priority:                      0
ipv6.addresses:                         --
ipv6.gateway:                           --
ipv6.routes:                            --
ipv6.route-metric:                      -1
```

```
ipv6.route-table:                       0 (unspec)
ipv6.routing-rules:                     --
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       0 (disabled)
ipv6.addr-gen-mode:                     stable-privacy
ipv6.ra-timeout:                        0 (default)
ipv6.dhcp-duid:                         --
ipv6.dhcp-iaid:                         --
ipv6.dhcp-timeout:                      0 (default)
ipv6.dhcp-send-hostname:                yes
ipv6.dhcp-hostname:                     --
ipv6.dhcp-hostname-flags:               0x0 (none)
ipv6.token:                             --
------------------------------------------------------------------------------
proxy.method:                           none
proxy.browser-only:                     no
proxy.pac-url:                          --
proxy.pac-script:                       --
------------------------------------------------------------------------------
lines 56-100/100 (END)
[q]
```

To see the characteristics of the **ip_fixed** profile, use the following command:

```
[root@centos8 ~]# nmcli -p connection show ip_fixed
===============================================================================
                    Connection profile details (ip_fixed)
===============================================================================
connection.id:                          ip_fixed
connection.uuid:                        0f48c74d-5d16-4c37-8220-24644507b589
connection.stable-id:                   --
```

```
connection.type:                        802-3-ethernet
connection.interface-name:              ens18
connection.autoconnect:                 yes
connection.autoconnect-priority:        0
connection.autoconnect-retries:         -1 (default)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1630224329
connection.read-only:                   no
connection.permissions:                 --
connection.zone:                        --
connection.master:                      --
connection.slave-type:                  --
connection.autoconnect-slaves:          -1 (default)
connection.secondaries:                 --
connection.gateway-ping-timeout:        0
connection.metered:                     unknown
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
---------------------------------------------------------------------------
802-3-ethernet.port:                    --
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
802-3-ethernet.mac-address-blacklist:   --
802-3-ethernet.mtu:                     auto
802-3-ethernet.s390-subchannels:        --
802-3-ethernet.s390-nettype:            --
802-3-ethernet.s390-options:            --
```

```
802-3-ethernet.wake-on-lan:             default
802-3-ethernet.wake-on-lan-password:    --
------------------------------------------------------------------------------
ipv4.method:                            manual
ipv4.dns:                               --
ipv4.dns-search:                        --
ipv4.dns-options:                       --
ipv4.dns-priority:                      0
ipv4.addresses:                         10.0.2.46/24
ipv4.gateway:                           10.0.2.1
ipv4.routes:                            --
ipv4.route-metric:                      -1
ipv4.route-table:                       0 (unspec)
ipv4.routing-rules:                     --
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-iaid:                         --
ipv4.dhcp-timeout:                      0 (default)
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.dhcp-fqdn:                         --
ipv4.dhcp-hostname-flags:               0x0 (none)
ipv4.never-default:                     no
ipv4.may-fail:                          yes
ipv4.dad-timeout:                       -1 (default)
ipv4.dhcp-vendor-class-identifier:      --
ipv4.dhcp-reject-servers:               --
------------------------------------------------------------------------------
ipv6.method:                            auto
ipv6.dns:                               --
ipv6.dns-search:                        --
ipv6.dns-options:                       --
ipv6.dns-priority:                      0
```

```
ipv6.addresses:                         --
ipv6.gateway:                           --
ipv6.routes:                            --
ipv6.route-metric:                      -1
ipv6.route-table:                       0 (unspec)
ipv6.routing-rules:                     --
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       -1 (unknown)
ipv6.addr-gen-mode:                     stable-privacy
ipv6.ra-timeout:                        0 (default)
ipv6.dhcp-duid:                         --
ipv6.dhcp-iaid:                         --
ipv6.dhcp-timeout:                      0 (default)
ipv6.dhcp-send-hostname:                yes
ipv6.dhcp-hostname:                     --
ipv6.dhcp-hostname-flags:               0x0 (none)
ipv6.token:                             --
------------------------------------------------------------------------------
proxy.method:                           none
proxy.browser-only:                     no
proxy.pac-url:                          --
proxy.pac-script:                       --
------------------------------------------------------------------------------
==============================================================================
      Activate connection details (0f48c74d-5d16-4c37-8220-24644507b589)
==============================================================================
GENERAL.NAME:                           ip_fixed
GENERAL.UUID:                           0f48c74d-5d16-4c37-8220-24644507b589
GENERAL.DEVICES:                        ens18
GENERAL.IP-IFACE:                       ens18
GENERAL.STATE:                          activated
```

```
GENERAL.DEFAULT:                        yes
GENERAL.DEFAULT6:                       no
GENERAL.SPEC-OBJECT:                    --
GENERAL.VPN:                            no
GENERAL.DBUS-PATH:                      /org/freedesktop/NetworkManager/ActiveConnection/4
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/Settings/4
GENERAL.ZONE:                           --
GENERAL.MASTER-PATH:                    --
---------------------------------------------------------------------------
IP4.ADDRESS[1]:                         10.0.2.46/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
---------------------------------------------------------------------------
IP6.ADDRESS[1]:                         fe80::5223:aee1:998e:9f27/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255
---------------------------------------------------------------------------
lines 83-127/127 (END)
[q]
```

To see a list of the profiles associated with a device, use the following command:

```
[root@centos8 ~]# nmcli -f CONNECTIONS device show ens18
CONNECTIONS.AVAILABLE-CONNECTION-PATHS:
/org/freedesktop/NetworkManager/Settings/1,/org/freedesktop/NetworkManager/Settings/4
CONNECTIONS.AVAILABLE-CONNECTIONS[1]:   fc4a4d23-b15e-47a7-bcfa-b2e08f49553e | ens18
CONNECTIONS.AVAILABLE-CONNECTIONS[2]:   0f48c74d-5d16-4c37-8220-24644507b589 | ip_fixed
```

The configuration files for the **ens18** device can be found in the **/etc/sysconfig/network-scripts/** directory:

```
[root@centos8 ~]# ls -l /etc/sysconfig/network-scripts/ | grep ifcfg
-rw-r--r--. 1 root root 417 Jun 16 06:39 ifcfg-ens18
```

```
-rw-r--r--. 1 root root 326 Aug 29 03:58 ifcfg-ip_fixed
```

1.2 - Name Resolution

Looking at the **/etc/sysconfig/network-scripts/ifcfg-ip_fixed** file reveals that their is currently no DNS entry:

```
[root@centos8 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixed
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=10.0.2.46
PREFIX=24
GATEWAY=10.0.2.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ip_fixed
UUID=0f48c74d-5d16-4c37-8220-24644507b589
DEVICE=ens18
ONBOOT=yes
```

As a result there is currently no name resolution :

```
[root@centos8 ~]# ping www.free.fr
ping: www.free.fr: Name or service not known
```

Modify the **ip_fixed** profile to rectify this:

```
[root@centos8 ~]# nmcli connection mod ip_fixed ipv4.dns 8.8.8.8
```

Consulting the **/etc/sysconfig/network-scripts/ifcfg-ip_fixed** file shows that a DNS server has been added:

```
[root@centos8 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixed
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=10.0.2.46
PREFIX=24
GATEWAY=10.0.2.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ip_fixed
UUID=0f48c74d-5d16-4c37-8220-24644507b589
DEVICE=ens18
ONBOOT=yes
DNS1=8.8.8.8
```

Restart the NetworkManager service to apply this change:

```
root@centos8 ~]# systemctl restart NetworkManager.service
[root@centos8 ~]# systemctl status NetworkManager.service
● NetworkManager.service - Network Manager
   Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-08-29 04:15:11 EDT; 8s ago
     Docs: man:NetworkManager(8)
 Main PID: 973390 (NetworkManager)
```

```
    Tasks: 4 (limit: 23535)
   Memory: 4.6M
   CGroup: /system.slice/NetworkManager.service
           └─973390 /usr/sbin/NetworkManager --no-daemon

Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2235] device (ens18): state
change: ip-check -> secondaries (reas>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2237] device (virbr0): state
change: secondaries -> activated (re>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2241] manager: NetworkManager
state is now CONNECTED_LOCAL
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2251] policy: set 'ip_fixed'
(ens18) as default for IPv4 routing a>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3090] device (virbr0):
Activation: successful, device activated.
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3098] device (ens18): state
change: secondaries -> activated (rea>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3102] manager: NetworkManager
state is now CONNECTED_SITE
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3111] device (ens18):
Activation: successful, device activated.
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3116] manager: NetworkManager
state is now CONNECTED_GLOBAL
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3121] manager: startup
complete
lines 1-20/20 (END)
[q]
```

Now check that the **/etc/resolv.conf** file has been modified to check the change made:

```
[root@centos8 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ittraining.loc
```

```
nameserver 8.8.8.8
```

Lastly, check the name resolution:

```
[root@centos8 ~]# ping www.free.fr
PING www.free.fr (212.27.48.10) 56(84) bytes of data.
64 bytes from www.free.fr (212.27.48.10): icmp_seq=1 ttl=47 time=29.3 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=2 ttl=47 time=29.4 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=3 ttl=47 time=29.4 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=4 ttl=47 time=29.4 ms
^C
--- www.free.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 29.266/29.377/29.428/0.183 ms
```

Important : Notez qu'il existe un front-end graphique en mode texte, **nmtui**, pour configurer NetworkManager.

1.3 - Adding a Second IP Addresse to a Profile

To add a second IP address, use the following command:

```
[root@centos8 ~]# nmcli connection mod ip_fixed +ipv4.addresses 192.168.1.2/24
```

Reload the profile:

```
[root@centos8 ~]# nmcli con up ip_fixed
```

Check that the new IP address is visible:

```
[root@centos8 ~]# nmcli connection show ip_fixed
connection.id:                          ip_fixed
connection.uuid:                        0f48c74d-5d16-4c37-8220-24644507b589
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              ens18
connection.autoconnect:                 yes
connection.autoconnect-priority:        0
connection.autoconnect-retries:         -1 (default)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1630225792
connection.read-only:                   no
connection.permissions:                 --
connection.zone:                        --
connection.master:                      --
connection.slave-type:                  --
connection.autoconnect-slaves:          -1 (default)
connection.secondaries:                 --
connection.gateway-ping-timeout:        0
connection.metered:                     unknown
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
802-3-ethernet.port:                    --
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
802-3-ethernet.mac-address-blacklist:   --
802-3-ethernet.mtu:                     auto
```

```
802-3-ethernet.s390-subchannels:        --
802-3-ethernet.s390-nettype:            --
802-3-ethernet.s390-options:            --
802-3-ethernet.wake-on-lan:             default
802-3-ethernet.wake-on-lan-password:    --
ipv4.method:                            manual
ipv4.dns:                               8.8.8.8
ipv4.dns-search:                        --
ipv4.dns-options:                       --
ipv4.dns-priority:                      0
ipv4.addresses:                         10.0.2.46/24, 192.168.1.2/24
ipv4.gateway:                           10.0.2.1
ipv4.routes:                            --
ipv4.route-metric:                      -1
ipv4.route-table:                       0 (unspec)
ipv4.routing-rules:                     --
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-iaid:                         --
ipv4.dhcp-timeout:                      0 (default)
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.dhcp-fqdn:                         --
ipv4.dhcp-hostname-flags:               0x0 (none)
ipv4.never-default:                     no
ipv4.may-fail:                          yes
ipv4.dad-timeout:                       -1 (default)
ipv4.dhcp-vendor-class-identifier:      --
ipv4.dhcp-reject-servers:               --
ipv6.method:                            auto
ipv6.dns:                               --
ipv6.dns-search:                        --
ipv6.dns-options:                       --
```

```
ipv6.dns-priority:                      0
ipv6.addresses:                         --
ipv6.gateway:                           --
ipv6.routes:                            --
ipv6.route-metric:                      -1
ipv6.route-table:                       0 (unspec)
ipv6.routing-rules:                     --
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       -1 (unknown)
ipv6.addr-gen-mode:                     stable-privacy
ipv6.ra-timeout:                        0 (default)
ipv6.dhcp-duid:                         --
ipv6.dhcp-iaid:                         --
ipv6.dhcp-timeout:                      0 (default)
ipv6.dhcp-send-hostname:                yes
ipv6.dhcp-hostname:                     --
ipv6.dhcp-hostname-flags:               0x0 (none)
ipv6.token:                             --
proxy.method:                           none
proxy.browser-only:                     no
proxy.pac-url:                          --
proxy.pac-script:                       --
GENERAL.NAME:                           ip_fixed
GENERAL.UUID:                           0f48c74d-5d16-4c37-8220-24644507b589
GENERAL.DEVICES:                        ens18
GENERAL.IP-IFACE:                       ens18
GENERAL.STATE:                          activated
GENERAL.DEFAULT:                        yes
GENERAL.DEFAULT6:                       no
GENERAL.SPEC-OBJECT:                    --
GENERAL.VPN:                            no
```

```
GENERAL.DBUS-PATH:                      /org/freedesktop/NetworkManager/ActiveConnection/3
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/Settings/2
GENERAL.ZONE:                           --
GENERAL.MASTER-PATH:                    --
IP4.ADDRESS[1]:                         10.0.2.46/24
IP4.ADDRESS[2]:                         192.168.1.2/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 192.168.1.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[3]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
IP4.DNS[1]:                             8.8.8.8
IP6.ADDRESS[1]:                         fe80::5223:aee1:998e:9f27/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255
lines 72-116/116 (END)
[q]
```

Important : Note the second address on the **ipv4.addresses:** line and the addition of the **IP4.ADDRESS[2]:** line.

Now check the **/etc/sysconfig/network-scripts/ifcfg-ip_fixed** file:

```
[root@centos8 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixed
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=10.0.2.46
PREFIX=24
GATEWAY=10.0.2.1
```

```
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ip_fixed
UUID=0f48c74d-5d16-4c37-8220-24644507b589
DEVICE=ens18
ONBOOT=yes
DNS1=8.8.8.8
IPADDR1=192.168.1.2
PREFIX1=24
```

Important : Note the addition of the **IPADDR1=192.168.1.2** line.

1.4 - The hostname Command

Any change to the hostname is immediate and permanent:

```
[root@centos8 ~]# hostname
centos8.ittraining.loc

[root@centos8 ~]# nmcli general hostname centos.ittraining.loc

[root@centos8 ~]# cat /etc/hostname
centos.ittraining.loc

[root@centos8 ~]# hostname
```

```
centos.ittraining.loc

[root@centos8 ~]# nmcli general hostname centos8.ittraining.loc

[root@centos8 ~]# cat /etc/hostname
centos8.ittraining.loc

[root@centos8 ~]# hostname
centos8.ittraining.loc
```

1.5 - The ip Command

Use of the **ip** command is now preferred over the use of the ifconfig command:

```
[root@centos8 ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 4e:b1:31:bd:5d:b2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.46/24 brd 10.0.2.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet 192.168.1.2/24 brd 192.168.1.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::5223:aee1:998e:9f27/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:79:02:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
```

```
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:79:02:66 brd ff:ff:ff:ff:ff:ff
```

Command Line Switches

The command line switches of this command are:

```
[root@centos8 ~]# ip --help
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                   netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                   vrf | sr | nexthop | mptcp }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec | -j[son] | -p[retty] |
                    -f[amily] { inet | inet6 | mpls | bridge | link } |
                    -4 | -6 | -I | -D | -M | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                    -c[olor]}
```

1.6 - Manually Activating and Disactivating a Device

Two commands exist for this purpose:

```
# nmcli device disconnect enp0s3
# nmcli device connect enp0s3
```

Important : Do **NOT** execute these two commands.

1.7 - Static Routing

The ip Command

To delete the 192.168.1.0 route, use the following command:

```
[root@centos8 ~]# ip route
default via 10.0.2.1 dev ens18 proto static metric 100
10.0.2.0/24 dev ens18 proto kernel scope link src 10.0.2.46 metric 100
192.168.1.0/24 dev ens18 proto kernel scope link src 192.168.1.2 metric 100
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown

root@centos8 ~]# ip route del 192.168.1.0/24 via 0.0.0.0
[root@centos8 ~]# ip route
default via 10.0.2.1 dev ens18 proto static metric 100
10.0.2.0/24 dev ens18 proto kernel scope link src 10.0.2.46 metric 100
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

To add a route for the 192.168.1.0 network, use the following command:

```
[root@centos8 ~]# ip route add 192.168.1.0/24 via 10.0.2.1
[root@centos8 ~]# ip route
default via 10.0.2.1 dev ens18 proto static metric 100
10.0.2.0/24 dev ens18 proto kernel scope link src 10.0.2.46 metric 100
192.168.1.0/24 via 10.0.2.1 dev ens18
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

Important - The command used to add a default gateway is **ip route add default via *ip_address***.

Disactivating/Activating Internal Routing on a Server

To disactivate internal routing between interfaces, use the following command:

```
[root@centos8 ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@centos8 ~]# echo 0 > /proc/sys/net/ipv4/ip_forward
[root@centos8 ~]# cat /proc/sys/net/ipv4/ip_forward
0
```

To activate internal routing between interfaces, use the following command:

```
[root@centos8 ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@centos8 ~]# cat /proc/sys/net/ipv4/ip_forward
1
```

LAB #2 - Diagnostics

2.1 - ping

To test whether a destination can be reached, use the **ping** command:

```
[root@centos8 ~]# ping -c4 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_seq=1 ttl=64 time=0.104 ms
```

```
64 bytes from 10.0.2.1: icmp_seq=2 ttl=64 time=0.325 ms
64 bytes from 10.0.2.1: icmp_seq=3 ttl=64 time=0.250 ms
64 bytes from 10.0.2.1: icmp_seq=4 ttl=64 time=0.123 ms

--- 10.0.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3083ms
rtt min/avg/max/mdev = 0.104/0.200/0.325/0.092 ms
```

Command Line Switches

The command line switches of this command are:

```
[root@centos8 ~]# ping --help
ping: invalid option -- '-'
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
             [-W timeout] destination
```

2.2 - netstat -i

To see networking statistics, use the **netstat** command:

```
[root@centos8 ~]# netstat -i
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
```

```
ens18            1500   476056      0      0 0        363562      0      0      0 BMRU
lo              65536    10936      0      0 0         10936      0      0      0 LRU
virbr0           1500        0      0      0 0             0      0      0      0 BMU
```

Command Line Switches

The command line switches of this command are:

```
[root@centos8 ~]# netstat --help
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -I[<Iface>] | [-veenNac] -i | [-cnNe] -M | -s [-6tuw] } [delay]

        -r, --route              display routing table
        -I, --interfaces=<Iface> display interface table for <Iface>
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -W, --wide               don't truncate IP addresses
        -n, --numeric            don't resolve names
        --numeric-hosts          don't resolve host names
        --numeric-ports          don't resolve port names
        --numeric-users          don't resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -o, --timers             display timers
        -c, --continuous         continuous listing

        -l, --listening          display listening server sockets
```

```
       -a, --all                display all sockets (default: connected)
       -F, --fib                display Forwarding Information Base (default)
       -C, --cache              display routing cache instead of FIB
       -Z, --context            display SELinux security context for sockets

  <Socket>={-t|--tcp} {-u|--udp} {-U|--udplite} {-S|--sctp} {-w|--raw}
           {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
    x25 (CCITT X.25)
```

2.3 - traceroute

This command is used to discover the route taken to reach a specified destination:

```
[root@centos8 ~]# traceroute www.ittraining.network
bash: traceroute: command not found...
Install package 'traceroute' to provide command 'traceroute'? [N/y] y


 * Waiting in queue...
The following packages have to be installed:
 traceroute-3:2.1.0-6.el8.x86_64        Traces the route taken by packets over an IPv4/IPv6 network
Proceed with changes? [N/y] y


 * Waiting in queue...
 * Waiting for authentication...
 * Waiting in queue...
 * Downloading packages...
 * Requesting data...
```

```
 * Testing changes...
 * Installing packages...
traceroute to www.ittraining.network (109.228.56.52), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.1)  0.132 ms  0.101 ms  0.078 ms
 2  79.137.68.252 (79.137.68.252)  0.542 ms  0.656 ms  0.809 ms
 3  10.50.24.61 (10.50.24.61)  0.238 ms  0.219 ms 10.50.24.60 (10.50.24.60)  0.239 ms
 4  10.50.0.16 (10.50.0.16)  0.172 ms 10.50.0.22 (10.50.0.22)  0.194 ms  0.173 ms
 5  10.73.248.192 (10.73.248.192)  0.766 ms 10.73.248.194 (10.73.248.194)  0.730 ms 10.73.248.192 (10.73.248.192)
0.757 ms
 6  waw-wa2-sbb1-nc5.pl.eu (91.121.131.150)  1.102 ms  1.396 ms  1.099 ms
 7  fra-fr5-sbb1-nc5.de.eu (213.251.128.113)  18.309 ms fra-fr5-sbb2-nc5.de.eu (54.36.50.116)  21.881 ms fra-fr5-
sbb1-nc5.de.eu (213.251.128.113)  16.764 ms
 8  10.200.0.6 (10.200.0.6)  20.922 ms 10.200.0.0 (10.200.0.0)  16.959 ms 10.200.0.4 (10.200.0.4)  21.143 ms
 9  decix.bb-a.fra3.fra.de.oneandone.net (80.81.192.123)  18.789 ms decix.bb-c.act.fra.de.oneandone.net
(80.81.193.123)  20.310 ms decix.bb-a.fra3.fra.de.oneandone.net (80.81.192.123)  18.693 ms
10  ae-14.bb-b.fr7.fra.de.oneandone.net (212.227.120.149)  22.222 ms  22.206 ms  22.257 ms
11  port-channel-3.gw-ngcs-1.dc1.con.glo.gb.oneandone.net (88.208.255.131)  39.660 ms  39.679 ms ae-19.bb-
b.thn.lon.gb.oneandone.net (212.227.120.33)  33.973 ms
12  109.228.63.209 (109.228.63.209)  37.363 ms port-channel-3.gw-ngcs-1.dc1.con.glo.gb.oneandone.net
(88.208.255.131)  39.534 ms 109.228.63.209 (109.228.63.209)  37.901 ms
13  * 109.228.63.209 (109.228.63.209)  38.014 ms  37.991 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
```

```
27  * * *
28  * * *
29  * * *^C
```

Command Line Switches

The command line switches of this command are:

```
[root@centos8 ~]# traceroute --help
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -
p port ] [ -t tos ] [ -l flow_label ] [ -w MAX,HERE,NEAR ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --
fwmark=num ] host [ packetlen ]
Options:
  -4                          Use IPv4
  -6                          Use IPv6
  -d  --debug                 Enable socket level debugging
  -F  --dont-fragment         Do not fragment packets
  -f first_ttl  --first=first_ttl
                              Start from the first_ttl hop (instead from 1)
  -g gate,...  --gateway=gate,...
                              Route packets through the specified gateway
                              (maximum 8 for IPv4 and 127 for IPv6)
  -I  --icmp                  Use ICMP ECHO for tracerouting
  -T  --tcp                   Use TCP SYN for tracerouting (default port is 80)
  -i device  --interface=device
                              Specify a network interface to operate with
  -m max_ttl  --max-hops=max_ttl
                              Set the max number of hops (max TTL to be
                              reached). Default is 30
  -N squeries  --sim-queries=squeries
                              Set the number of probes to be tried
                              simultaneously (default is 16)
```

```
-n                           Do not resolve IP addresses to their domain names
-p port  --port=port         Set the destination port to use. It is either
                             initial udp port value for "default" method
                             (incremented by each probe, default is 33434), or
                             initial seq for "icmp" (incremented as well,
                             default from 1), or some constant destination
                             port for other methods (with default of 80 for
                             "tcp", 53 for "udp", etc.)
-t tos  --tos=tos            Set the TOS (IPv4 type of service) or TC (IPv6
                             traffic class) value for outgoing packets
-l flow_label  --flowlabel=flow_label
                             Use specified flow_label for IPv6 packets
-w MAX,HERE,NEAR  --wait=MAX,HERE,NEAR
                             Wait for a probe no more than HERE (default 3)
                             times longer than a response from the same hop,
                             or no more than NEAR (default 10) times than some
                             next hop, or MAX (default 5.0) seconds (float
                             point values allowed too)
-q nqueries  --queries=nqueries
                             Set the number of probes per each hop. Default is
                             3
-r                           Bypass the normal routing and send directly to a
                             host on an attached network
-s src_addr  --source=src_addr
                             Use source src_addr for outgoing packets
-z sendwait  --sendwait=sendwait
                             Minimal time interval between probes (default 0).
                             If the value is more than 10, then it specifies a
                             number in milliseconds, else it is a number of
                             seconds (float point values allowed too)
-e  --extensions             Show ICMP extensions (if present), including MPLS
-A  --as-path-lookups        Perform AS path lookups in routing registries and
                             print results directly after the corresponding
                             addresses
```

```
  -M name  --module=name      Use specified module (either builtin or external)
                              for traceroute operations. Most methods have
                              their shortcuts (`-I' means `-M icmp' etc.)
  -O OPTS,...  --options=OPTS,...
                              Use module-specific option OPTS for the
                              traceroute module. Several OPTS allowed,
                              separated by comma. If OPTS is "help", print info
                              about available options
  --sport=num                 Use source port num for outgoing packets. Implies
                              `-N 1'
  --fwmark=num                Set firewall mark for outgoing packets
  -U  --udp                   Use UDP to particular port for tracerouting
                              (instead of increasing the port per each probe),
                              default port is 53
  -UL                         Use UDPLITE for tracerouting (default dest port
                              is 53)
  -D  --dccp                  Use DCCP Request for tracerouting (default port
                              is 33434)
  -P prot  --protocol=prot    Use raw packet of protocol prot for tracerouting
  --mtu                       Discover MTU along the path being traced. Implies
                              `-F -N 1'
  --back                      Guess the number of hops in the backward path and
                              print if it differs
  -V  --version               Print version info and exit
  --help                      Read this help and exit

Arguments:
+     host          The host to traceroute to
      packetlen     The full packet length (default is the length of an IP
                    header plus 40). Can be ignored or increased to a minimal
                    allowed value
```

LAB #3 - SSH

3.1 - Presentation

There are two types of SSH.

SSH-1

To authenticate there are six possible methods:

- **Kerberos**,
- **Rhosts**,
- **RhostsRSA**,
- **Asymetric Keys**,
- **TIS**,
- **Password**.

SSH-2

To authenticate there are three possible methods:

- **Asymetric Keys**,
- **RhostsRSA**,
- **Password**

Command Line Switches

The command line switches of this command are:

```
[root@centos8 ~]# ssh --help
unknown option -- -
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

3.2 - Configuring the Server

The server is configured by editing the **/etc/ssh/sshd_config** file:

```
[root@centos8 ~]# cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
```

```
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# This system is following system-wide crypto policy. The changes to
# crypto properties (Ciphers, MACs, ...) will not have any effect here.
# They will be overridden by command-line options passed to the server
# on command line.
# Please, check manual pages for update-crypto-policies(8) and sshd_config(5).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
```

```
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
```

```
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnablek5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in Fedora and may cause several
# problems.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes

# It is recommended to use pam_motd in /etc/pam.d/sshd instead of PrintMotd,
# as it is more configurable and versatile than the built-in version.
PrintMotd no

#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
```

```
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
```

To remove all empty and comment lines, use the following command:

```
[root@centos8 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/ssh/sshd_config > sshd_config
[root@centos8 tmp]# cat sshd_config
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

```
SyslogFacility AUTHPRIV
PermitRootLogin yes
AuthorizedKeysFile      .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
X11Forwarding yes
PrintMotd no
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

This file now has to be hardened by adding/editing the following directives:

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
X11Forwarding no
```

The file should look like this:

```
[root@centos8 tmp]# vi sshd_config
```

```
[root@centos8 tmp]# cat sshd_config
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
X11Forwarding no
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
PermitRootLogin yes
AuthorizedKeysFile      .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
PrintMotd no
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

Rename the current **/etc/ssh/sshd_config** file as **/etc/ssh/sshd_config.old** :

```
[root@centos8 tmp]# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.old
```

Copy the **/tmp/sshd_config** file to **/etc/ssh/** :

```
[root@centos8 tmp]# cp /tmp/sshd_config /etc/ssh
cp: overwrite '/etc/ssh/sshd_config'? y
```

Restart the sshd service:

```
[root@centos8 tmp]# systemctl restart sshd
[root@centos8 tmp]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-08-30 02:17:00 EDT; 11s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1042039 (sshd)
    Tasks: 1 (limit: 23535)
   Memory: 1.1M
   CGroup: /system.slice/sshd.service
           └─1042039 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-
ctr,aes256-cbc,aes128-gcm@openssh.com,a>

Aug 30 02:17:00 centos8.ittraining.loc systemd[1]: Starting OpenSSH server daemon...
Aug 30 02:17:00 centos8.ittraining.loc sshd[1042039]: Server listening on 0.0.0.0 port 22.
Aug 30 02:17:00 centos8.ittraining.loc sshd[1042039]: Server listening on :: port 22.
Aug 30 02:17:00 centos8.ittraining.loc systemd[1]: Started OpenSSH server daemon.
[q]
```

Put **trainee** in the **adm** group:

```
[root@centos8 tmp]# groups trainee
trainee : trainee
[root@centos8 tmp]# usermod -aG adm trainee
[root@centos8 tmp]# groups trainee
```

```
trainee : trainee adm
```

To generate the server keys, execute the following commands as **root**. Note that the passphrase must be **empty**:

```
[root@centos8 tmp]# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa): /etc/ssh/ssh_host_dsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
SHA256:dywC6jKyIMaTxsaEamz1kmthEmuG18HxmS22qRICOYk root@centos8.ittraining.loc
The key's randomart image is:
+---[DSA 1024]----+
|                 |
|    .            |
|.o . o.+         |
|E.  o.*..  .     |
|+ooo.o +S o o    |
|X==++ o  o o     |
|B/=+oo           |
|Ooo++            |
|. .o             |
+----[SHA256]-----+
```

```
[root@centos8 tmp]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /etc/ssh/ssh_host_rsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
```

```
SHA256:8jXFK50NnoJCz9E7aPKpFYSYCstCPfRsdmlLBTNUnKg root@centos8.ittraining.loc
The key's randomart image is:
+---[RSA 3072]----+
|   .  .==o.      |
|  o oo o=+ .     |
|.. oo=+=o . +    |
|oo .+E++.+ = *   |
|o..   +.S B * .  |
|.      B + =     |
|        =        |
|       o         |
|      .          |
+----[SHA256]-----+
[root@centos8 tmp]# ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/root/.ssh/id_ecdsa): /etc/ssh/ssh_host_ecdsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_ecdsa_key.
Your public key has been saved in /etc/ssh/ssh_host_ecdsa_key.pub.
The key fingerprint is:
SHA256:AMqFUJKGqnUEPh/IYda0wnbW1kXK+lnprpHsOo4UMbI root@centos8.ittraining.loc
The key's randomart image is:
+---[ECDSA 256]---+
|++*=+    .o      |
|oX.=o+ o o       |
|o %.B + +        |
|...O.= o   .     |
|..E.o . S o      |
|.    . o =       |
|    .   * .      |
|   . ... o       |
|    ..ooo..      |
+----[SHA256]-----+
```

```
[root@centos8 tmp]# ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519): /etc/ssh/ssh_host_ed25519_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_ed25519_key.
Your public key has been saved in /etc/ssh/ssh_host_ed25519_key.pub.
The key fingerprint is:
SHA256:CtbcN9iXv00PfbHFGf2bEW7iRibOFwRctyqM5hmlhwE root@centos8.ittraining.loc
The key's randomart image is:
+--[ED25519 256]--+
|       E  .... . |
|        .  .. . o|
|         . . . +.|
|     o . oB ..o.=|
|    o o S*+=o* *+|
|   . . .o.*o*.+.B|
|      .  o o +o++|
|            o  =o|
|              . o|
+----[SHA256]-----+
```

Public keys have a **.pub** extension:

```
[root@centos8 tmp]# ls /etc/ssh
moduli      ssh_config.d  sshd_config.old     ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub
ssh_host_rsa_key.pub
ssh_config  sshd_config   ssh_host_ecdsa_key  ssh_host_ed25519_key    ssh_host_rsa_key
```

Restart the sshd service:

```
[root@centos8 tmp]# systemctl restart sshd.service
[root@centos8 tmp]# systemctl status sshd.service
● sshd.service - OpenSSH server daemon
```

```
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-08-30 02:24:57 EDT; 9s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1042204 (sshd)
    Tasks: 1 (limit: 23535)
   Memory: 1.1M
   CGroup: /system.slice/sshd.service
           └─1042204 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-
ctr,aes256-cbc,aes128-gcm@openssh.com,a>

Aug 30 02:24:57 centos8.ittraining.loc systemd[1]: Starting OpenSSH server daemon...
Aug 30 02:24:57 centos8.ittraining.loc sshd[1042204]: Server listening on 0.0.0.0 port 22.
Aug 30 02:24:57 centos8.ittraining.loc sshd[1042204]: Server listening on :: port 22.
Aug 30 02:24:57 centos8.ittraining.loc systemd[1]: Started OpenSSH server daemon.
[q]
```

3.3 - Configuring the Client

To generate the client keys, execute the following commands as **trainee**. Note that the passphrase must be **empty**:

```
[root@centos8 tmp]# exit
logout
[trainee@centos8 ~]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_dsa):
Created directory '/home/trainee/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_dsa.
Your public key has been saved in /home/trainee/.ssh/id_dsa.pub.
The key fingerprint is:
SHA256:Qd17X1iROjk5rLOQBbyVg1hNXkUdTeiFtEpn3rgPKc4 trainee@centos8.ittraining.loc
```

```
The key's randomart image is:
+---[DSA 1024]----+
|        =o+o.o+OB|
|       o +o=o oo=|
|        . +.+oB+ |
|         o o.&+o.|
|        S o o.*.o|
|         o o   o.|
|          . + +  |
|           + . o |
|            E   .|
+----[SHA256]-----+
[trainee@centos8 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.

Enter file in which to save the key (/home/trainee/.ssh/id_rsa): Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_rsa.
Your public key has been saved in /home/trainee/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:BgEjoWQrGCzdJfyZczVZYVoafiHsz9GK5PDWuywG/z0 trainee@centos8.ittraining.loc
The key's randomart image is:
+---[RSA 3072]----+
|o+o++oo  .oo*.   |
|=+o.oo . .=B .   |
|=.   ..o o+...   |
|.     =.o o.. .  |
|       oS= = o   |
|       .. = =    |
|         +   .   |
|          +...E  |
|         . o+... |
+----[SHA256]-----+
[trainee@centos8 ~]$ ssh-keygen -t ecdsa
```

```
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ecdsa.
Your public key has been saved in /home/trainee/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:mpBDgsCxP2DqRPkmGvXHpNnvm5B+Cl7MSiiZKfDjWLk trainee@centos8.ittraining.loc
The key's randomart image is:
+---[ECDSA 256]---+
|o..              |
|.oo              |
|.*o . .          |
|+.++ B           |
|+o =B + S        |
|=*oo.* =         |
|B.* o O .        |
|.= = = o..       |
|. E o oo+.       |
+----[SHA256]-----+
[trainee@centos8 ~]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ed25519.
Your public key has been saved in /home/trainee/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:JfFxG2mg9feAvFGxoxZ8uSsON3sXvtYQYYg5iVxzZS4 trainee@centos8.ittraining.loc
The key's randomart image is:
+--[ED25519 256]--+
|       ..o*=++=. |
|        o==O+Boo |
|        o ooE.O. |
```

```
|         o   O.= |
|        S   + ...|
|           .  .o |
|          . + o.o|
|           + +.oo|
|            o..o.|
+----[SHA256]-----+
```

The keys can be found in the **~/.ssh/** directory:

```
[trainee@centos8 ~]$ ls .ssh
id_dsa  id_dsa.pub  id_ecdsa  id_ecdsa.pub  id_ed25519  id_ed25519.pub  id_rsa  id_rsa.pub
```

3.4 - Authentication using Asymetric Keys

Connect to your own virtual machine as if it were the server:

```
[root@centos8 ~]# ssh -l trainee 127.0.0.1
\S
Kernel \r on an \m
trainee@127.0.0.1's password: trainee
Activate the web console with: systemctl enable --now cockpit.socket

[trainee@centos8 ~]$ ls -la | grep .ssh
drwx------.  2 trainee trainee      4096 Aug 30 02:26 .ssh
```

Now transfer the client's **.ssh/id_ecdsa.pub** key to the server and rename it **authorized_keys** :

```
[trainee@centos8 ~]$ exit
logout
Connection to 127.0.0.1 closed.
```

```
[root@centos8 ~]# exit
logout

[trainee@centos8 ~]$ scp .ssh/id_ecdsa.pub trainee@127.0.0.1:/home/trainee/.ssh/authorized_keys
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Q7T/CP0SLiMbMAIgVzTuEHegYS/spPE5zzQchCHD5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
\S
Kernel \r on an \m
trainee@127.0.0.1's password: trainee
id_ecdsa.pub
100%  192   497.6KB/s   00:00
```

Re-connect to your own virtual machine as if it were the server:

```
[trainee@centos8 ~]$ ssh -l trainee localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:Q7T/CP0SLiMbMAIgVzTuEHegYS/spPE5zzQchCHD5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
\S
Kernel \r on an \m
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Aug 30 03:57:14 2021 from 127.0.0.1
[trainee@centos8 ~]$
```

Important - Note that no password is required.