Module 14
Network Configuration

Exam Objective

4.4 Your Computer on the Network

Objective Description

Querying vital networking configuration and determining the basic requirements for a computer on a Local Area Network (LAN).

Introduction

Introduction

- Linux provides several tools to configure your network and monitor how it is performing.
- This module will cover how to use both GUI-based tools as well as command line tools.

Network Terminology

Network Terminology

- **Host** - A computer or device
- **Network** - Two or more computers that communicate
- **Internet** - Publicly accessible network
- **Wi-Fi** - A wireless network
- **Server** - A host that provides a service to another host.
- **Service** - A feature being provided from a host
- **Client** - A host that is accessing a server
- **Router** - A machine that connects hosts from one network to another network

Networking Features

- **Network packet** - A data delivery method used to send network communication between hosts
- **IP address** - An *Internet Protocol* address is a unique number assigned to a host on a network
- **Network mask** - A numbering system that defines which IP addresses are part of a network
- **Hostnames** - A name given to a host on a network
- **DHCP** - The *Dynamic Host Configuration Protocol* assigns hosts hostnames, IP addresses and other network-related information

Networking Features

- **DNS** - A *Domain Name Server* translates domain names into IP addresses
- **Ethernet** - Common method of physically connecting hosts into a network by using cables and devices
- **TCP/IP** - *Transmission Control Protocol/Internet Protocol* is a collection of protocols that are used to define how network communication should take place between hosts.

IP Addresses

- Hosts use IP addresses to send and receive network packets from other hosts.
- There are two types of IP addresses:
  - IPv4 - Uses four 8-bit numbers. For example, `192.168.10.120`.
    - Size limits number of addresses that are available for everyone on the internet.
  - IPv6 - 128-bit address. For example, `2001:0db8:85a3:0042:1000:8a2e:0370:7334`
    - Much larger address size result in more addresses available

Network Configuration

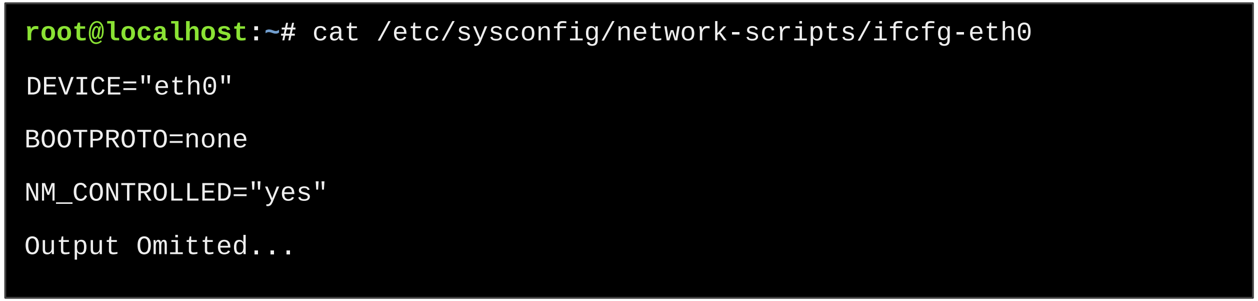
Configuring Network Devices

- Two important questions to consider when configuring network devices:
    - Wired or wireless?
        - Wireless includes additional security features
    - DHCP or static?
        - DHCP will provide an IP address and subnet mask (a number used to identify what subnetwork an IP address belongs to).
        - Static means to manually provide network information to the host.
        - Wireless uses DHCP

Using Configuration Files to Configure the Network

- There will be times when no GUI-based tool will be available. In those cases, it is helpful to know the configuration files that are used to store and modify network data.

- Primary IPv4 Configuration File: `/etc/sysconfig/network-scripts/ifcfg-eth0`
  - To configure as DHCP, change `BOOTPROTO` value to `dhcp`.



```
root@localhost:~# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO=none
NM_CONTROLLED="yes"
Output Omitted...
```

Using Configuration Files to Configure the Network

- Primary IPv6 Configuration File: `/etc/sysconfig/network-scripts/ifcfg-eth0`
    - Same file as IPv4 on CentOS
    - To configure IPv6 on your system the following would need to be added to the file:

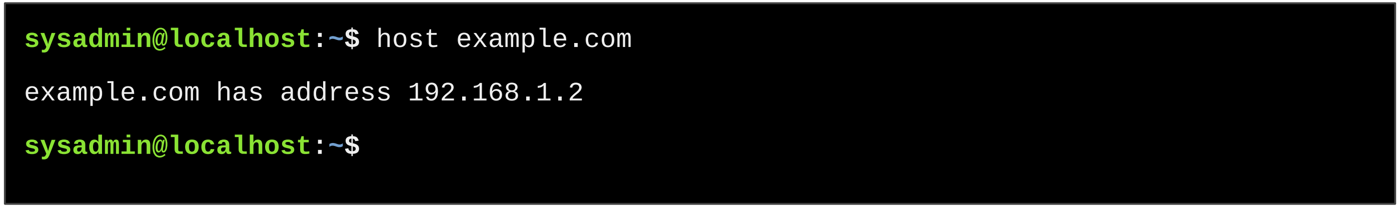
```
IPV6INIT=yes

IPV6ADDR=<IPv6 IP Address>

IPV6_DEFAULTGW=<IPv6 IP Gateway Address>
```

Domain Name Service (DNS)

- In order for the computer to associate an IP address with the URL or hostname request, the computer relies upon the DNS service of another computer.

- The address of the DNS server is stored in the `/etc/resolv.conf` file.

- For example this server is associated with the IP address 192.168.1.2 by the DNS server:



```
sysadmin@localhost:~$ host example.com
example.com has address 192.168.1.2
sysadmin@localhost:~$
```

Domain Name Service (DNS)

- Name resolution on a Linux host is accomplished by 3 critical files:
  - `/etc/hosts` - Contains a table of hostnames to IP addresses
  - `/etc/resolv.conf` - Contains the IP addresses of the name servers the system uses to resolve names to IP addresses
  - `/etc/nsswitch.conf` - Used to modify where hostname lookups occur
- Commands or programs on the system, (i.e., browser) will request a connection with a remote computer by DNS name.
- The system will consult various files in a particular order to attempt to resolve that name into a usable IP address.

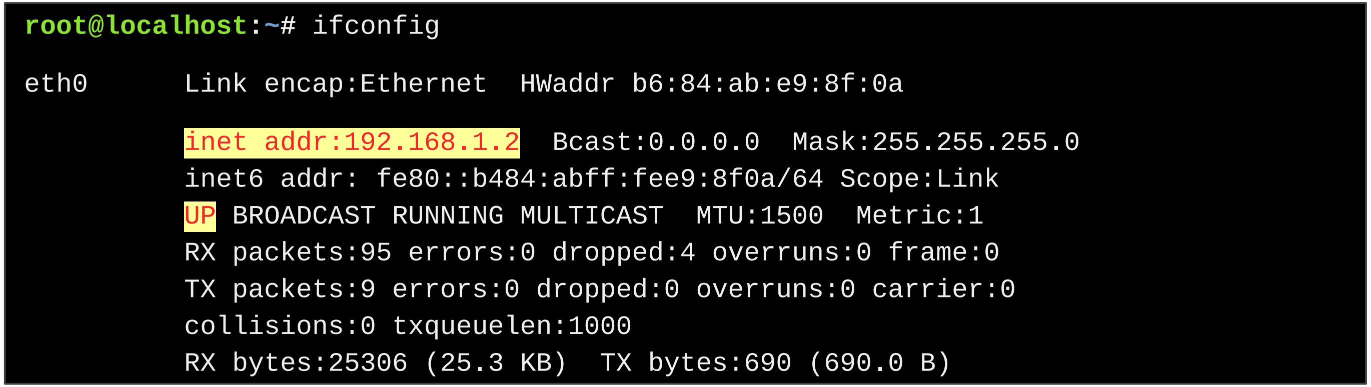
Network Tools

Network Tools

- There are several commands that you can use to view network information and troubleshoot network issues:
    - ifconfig
    - ip
    - route
    - ping
    - netstat
    - ss
    - dig
    - host
    - ssh

The ifconfig Command

- The `ifconfig` command stands for "interface configuration".
- Used to display network configuration information:



```
root@localhost:~# ifconfig

eth0      Link encap:Ethernet  HWaddr b6:84:ab:e9:8f:0a

          inet addr:192.168.1.2  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::b484:abff:fee9:8f0a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:95 errors:0 dropped:4 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25306 (25.3 KB)  TX bytes:690 (690.0 B)
```

  - In the output above, the IP address of the primary network device (`eth0`) is `192.168.1.2` and the device is currently active (UP).

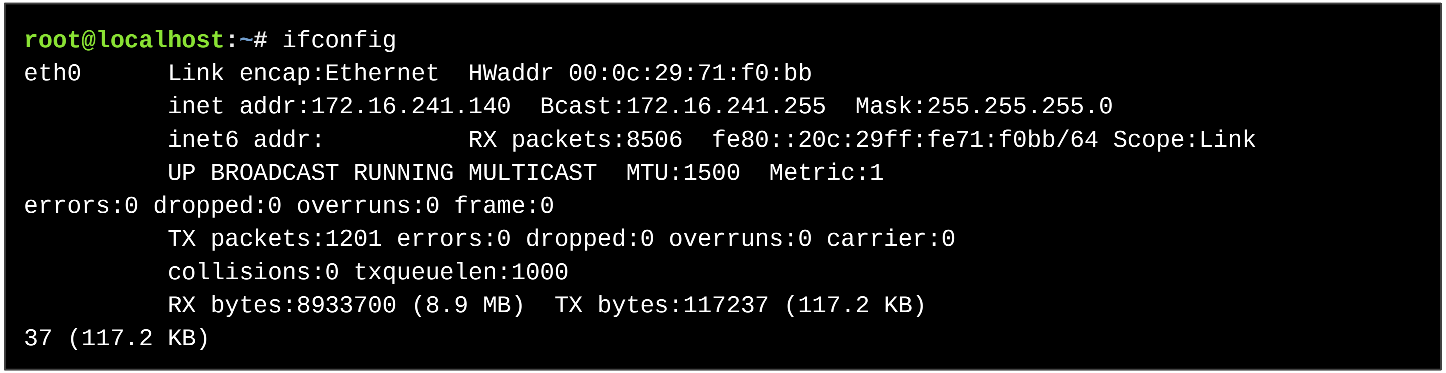
The ip Command

- The `ip` command is replacing the `ifconfig` command.
- The `ip` command has increased functionality and set of options.
- The format for the `ip` command is as follows:

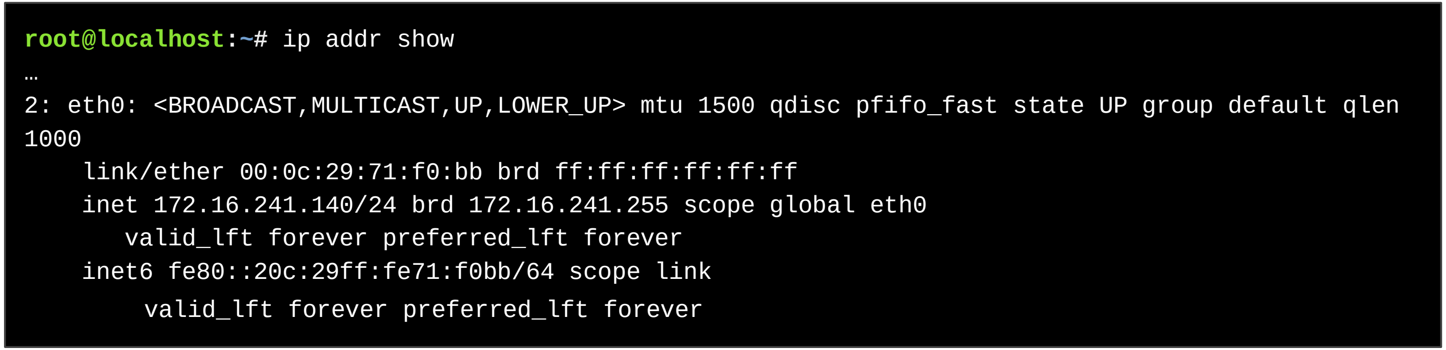
```
ip [OPTIONS] OBJECT COMMAND
```

- Both (`ip` and `ifconfig`) show the type of interface, protocols, hardware and IP addresses, network masks and other various information about each of the active interfaces on the system.

The ifconfig v.s. ip Commands



```
root@localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:71:f0:bb
          inet addr:172.16.241.140  Bcast:172.16.241.255  Mask:255.255.255.0
          inet6 addr:          RX packets:8506  fe80::20c:29ff:fe71:f0bb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
errors:0 dropped:0 overruns:0 frame:0
          TX packets:1201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8933700 (8.9 MB)  TX bytes:117237 (117.2 KB)
37 (117.2 KB)
```

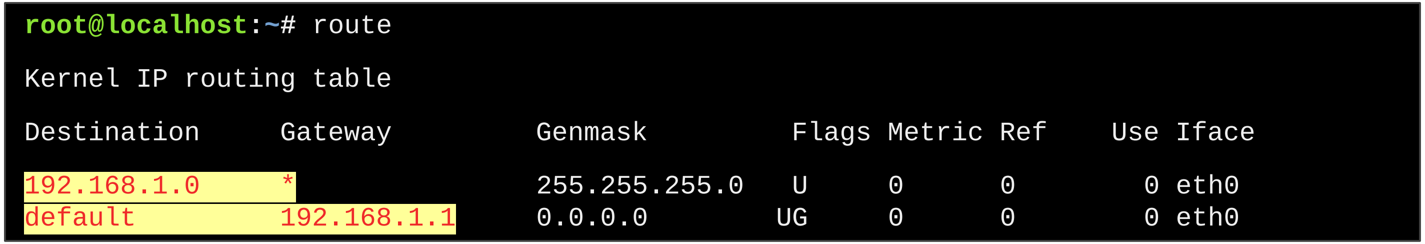


```
root@localhost:~# ip addr show
…
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
1000
    link/ether 00:0c:29:71:f0:bb brd ff:ff:ff:ff:ff:ff
    inet 172.16.241.140/24 brd 172.16.241.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe71:f0bb/64 scope link
        valid_lft forever preferred_lft forever
```

The route Command

Remember: A router (or gateway) is a machine that will allow hosts from one network to communicate with another network.

- The `route` command can be used to view a table that describes where network packages are sent.



```
root@localhost:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
default         192.168.1.1     0.0.0.0        UG     0      0        0 eth0
```

  - Any network package sent to a machine in the `192.168.1` network is not sent to a gateway machine (the `*` indicates "no gateway").
  - All other network packets are sent to the host with the IP address of `192.168.1.1` (the router).

The ping Command

- The `ping` command can be used to determine if another machine is "reachable".
- By default, the `ping` command will continue sending packages endlessly.
- Use the `-c` option followed by a number to limit how many pings to send.
- A successful ping looks like:

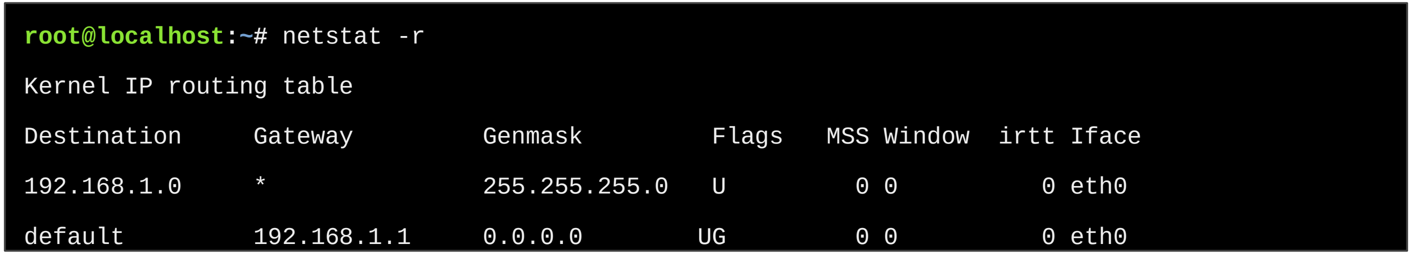
```
64 bytes from 192.168.1.2: icmp_req=1 ttl=64 time=0.051 ms
```

- If the `ping` command fails, a message stating, `Destination Host Unreachable` will display:

```
From 192.168.1.2 icmp_seq=1 Destination Host Unreachable
```

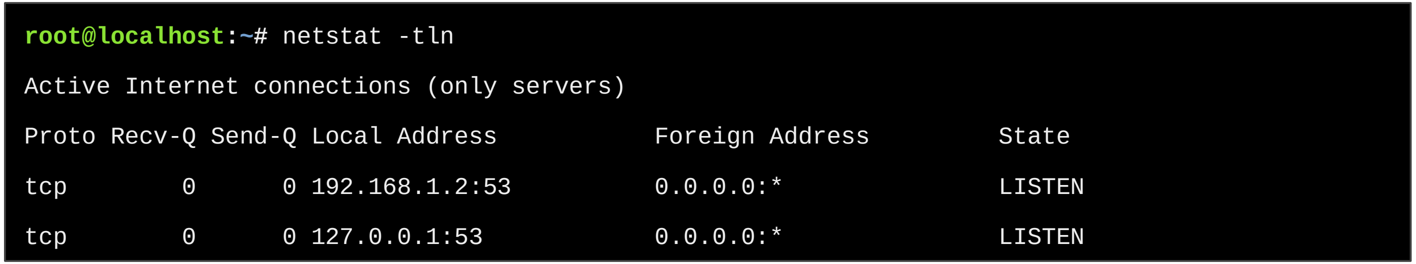
The netstat Command

- The `netstat` command is used to display information about network connections as well as display the routing table similar to the `route` command:



```
root@localhost:~# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     *               255.255.255.0   U         0 0          0 eth0
default         192.168.1.1     0.0.0.0        UG         0 0          0 eth0
```

- The `netstat` command is also commonly used to display open *ports*:

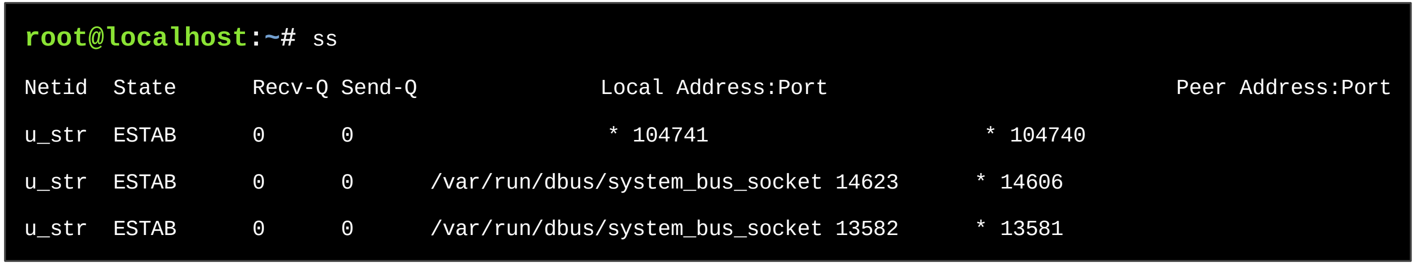


```
root@localhost:~# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.2:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
```

The ss Command

- The `ss` command is designed to show socket statistics and supports all the major packet and socket types.

- Used to view connections currently established between their local machine and remote machines, as well as statistics about those connections.



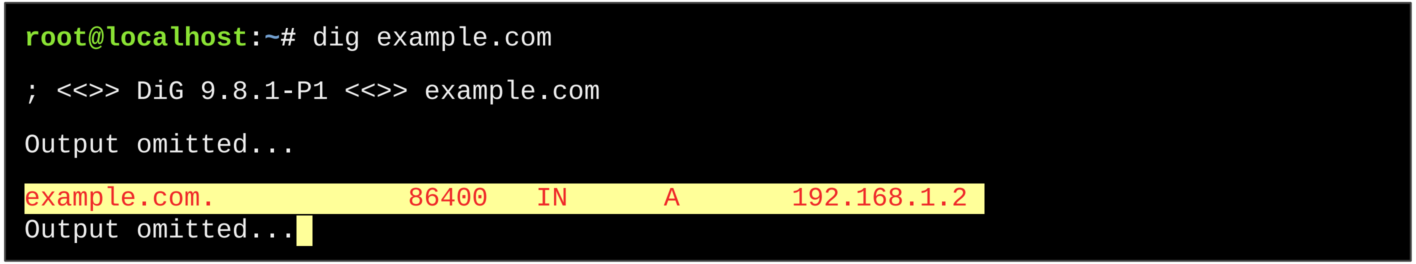
```
root@localhost:~# ss
Netid  State      Recv-Q Send-Q               Local Address:Port                             Peer Address:Port
u_str  ESTAB      0      0                     * 104741                       * 104740
u_str  ESTAB      0      0      /var/run/dbus/system_bus_socket 14623      * 14606
u_str  ESTAB      0      0      /var/run/dbus/system_bus_socket 13582      * 13581
```

- This output is very similar to the output of the `netstat` command with no options.

The dig Command

- The `dig` command will perform queries on the DNS server to determine if the information needed is available on the server.

- For example, the `dig` command is used to determine the IP address of the example.com host:



```
root@localhost:~# dig example.com

; <<>> DiG 9.8.1-P1 <<>> example.com

Output omitted...

example.com.            86400   IN      A       192.168.1.2
Output omitted...
```

- The DNS server has the IP address (`192.168.1.2`) to hostname (`example.com`) translation information in its database.

The host Command

- The `host` command works with DNS to associate a hostname with an IP address:

```
root@localhost:~# host example.com

example.com has address 192.168.1.2
```

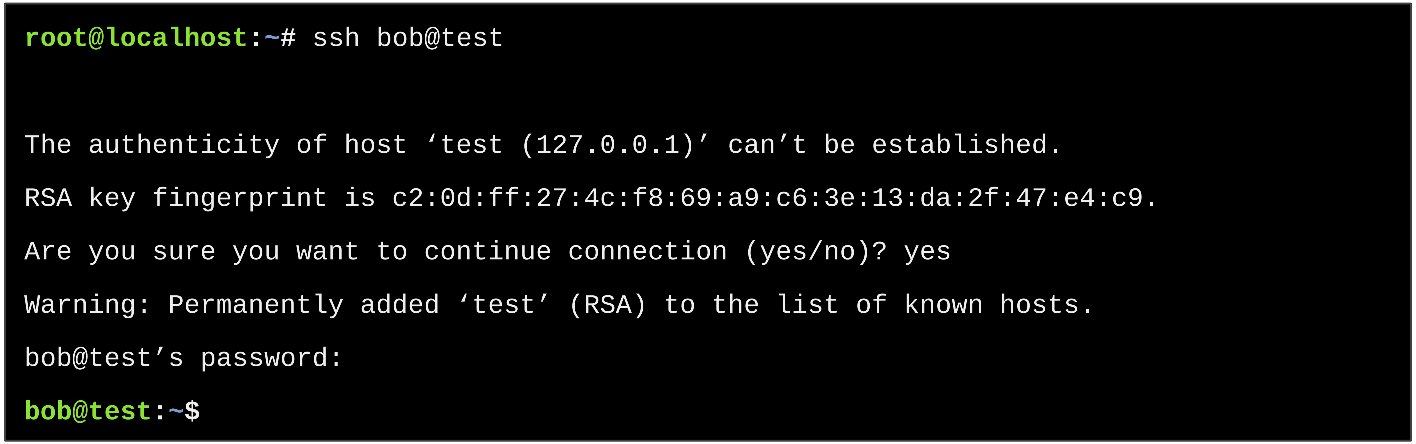
- The `host` command can also be used in reverse if an IP address is known, but the domain name is not:

```
root@localhost:~# host 192.168.1.2

2.1.168.192.in-addr.arpa domain name pointer example.com.

2.1.168.192.in-addr.arpa domain name pointer cserver.example.com.
```

- Other options exist to query the various aspects of a DNS such as CNAME (canonical name) and SOA (Start of Authority).

The ssh Command

- The `ssh` command will allow you to connect to another machine across the network, log in and then perform tasks on the remote machine:



```
root@localhost:~# ssh bob@test


The authenticity of host ‘test (127.0.0.1)’ can’t be established.

RSA key fingerprint is c2:0d:ff:27:4c:f8:69:a9:c6:3e:13:da:2f:47:e4:c9.

Are you sure you want to continue connection (yes/no)? yes

Warning: Permanently added ‘test’ (RSA) to the list of known hosts.

bob@test’s password:

bob@test:~$
```

- To return back to the local machine, use the `exit` command.

The ssh Command

- RSA key fingerprint
  - If you answer yes at the prompt (asking to verify the machine’s identity), the *RSA key fingerprint* of the remote machine will be stored on your local system:

```
RSA key fingerprint is c2:0d:ff:27:4c:f8:69:a9:c6:3e:13:da:2f:47:e4:c9.

Are you sure you want to continue connection (yes/no)? yes

Warning: Permanently added ‘test’ (RSA) to the list of known hosts.
```

  - When you attempt to `ssh` to the same machine in the future, the RSA key fingerprint provided by the remote machine is compared to the copy stored on the local machine.
  - If they don't match, you will see an error message.