



# Networking Tools

CompTIA Network+ (N10-007)

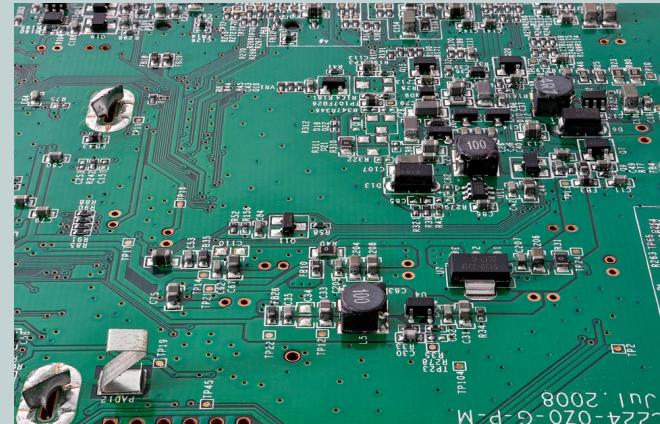
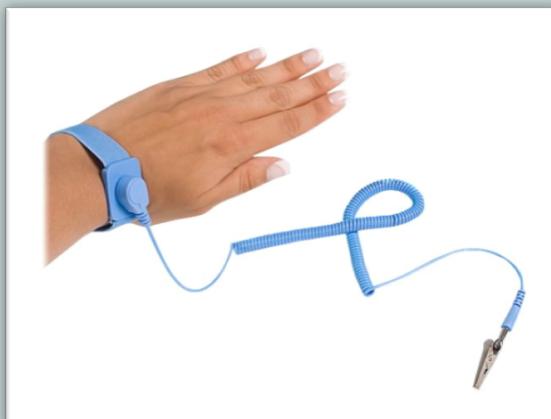
# Networking Tools

- Physical cabling still serves as the backbone of networks even with wireless networking
- Many network problems can be reduced through proper installation and configuration
- Multiple hardware and software tools are available to help diagnose, isolate, and resolve network issues
- It is important to understand the various tools, management devices, and protocols in use by network technicians



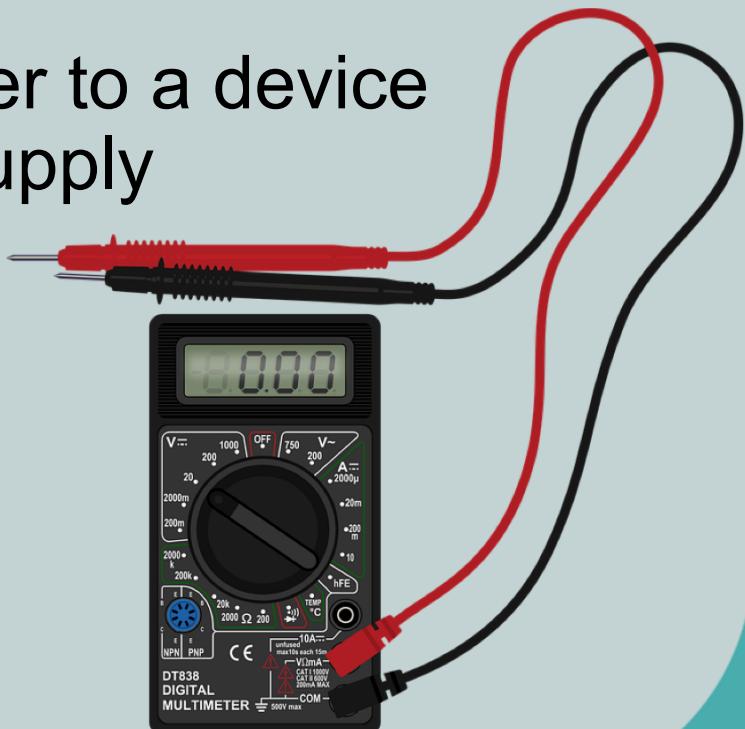
# Electrostatic Discharge (ESD) Strap

- Allows static buildup in your body to be discharged into a grounded object instead of damaging the electrical components
- Static discharge can be several thousands of volts but at low amperage
  - Humans aren't injured by the shock
  - Circuit boards and components can be destroyed



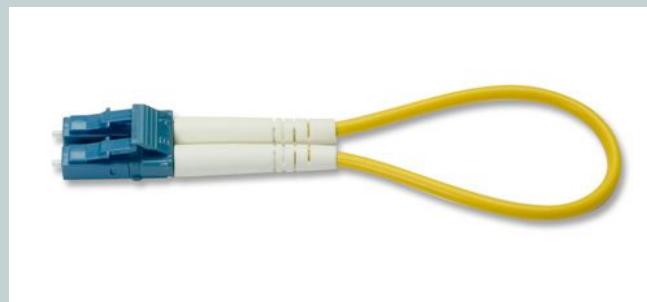
# Multimeter

- Used with copper cabling to verify continuity, resistance, amperage, or voltage
  - Can be used to verify a cable is broken or not by checking resistance
- Used to test source power to a device or device's own power supply
  - US (115-125 VAC)
  - Europe (230-240 VAC)



# Loopback

- Connects transmit pins (or fibers) to receive pins (or fiber) to test a network interfaces
  - Ethernet Pinout
    - Pins 1 to 3 (Tx+ to Rx+)
    - Pins 2 to 6 (Tx- to Rx-)
  - Fiber
    - Transmit fiber to Receive fiber
- Used with diagnostic software to test Ethernet connectivity of a client



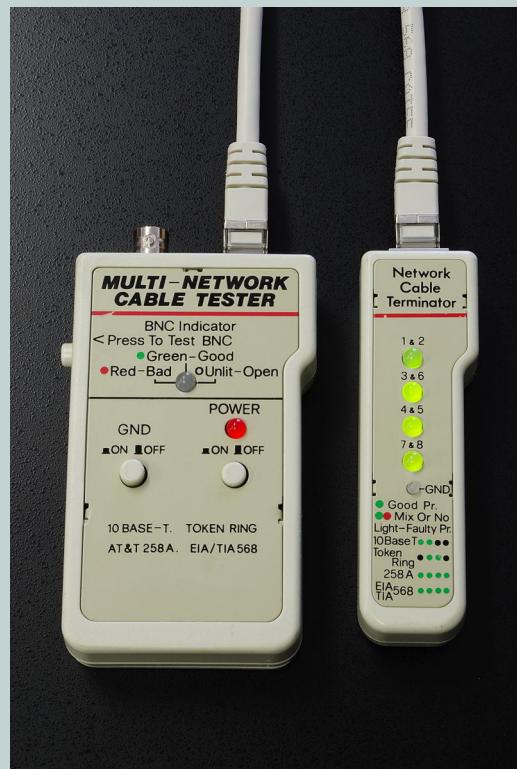
# Crimper

- Used to attach a connector to the cable's end
- Allows technicians to make cables of varying lengths instead of a standard size
- Physically crimps the plastic connector to a cable
  - RJ-45 for networks
  - RJ-11 for phones



# Cable Tester

- Verifies continuity for each wire in the cable to ensure there are no breaks
- Verifies the pinouts of the connectors
- Different testers for different cable types



# Cable Certifier

- Used with existing cable to determine its category or test data throughput
  - Cat 3, Cat 5, Cat5e, Cat 6, Cat 7, ...
- Identifies the frequency range supported by a cable to determine data throughput

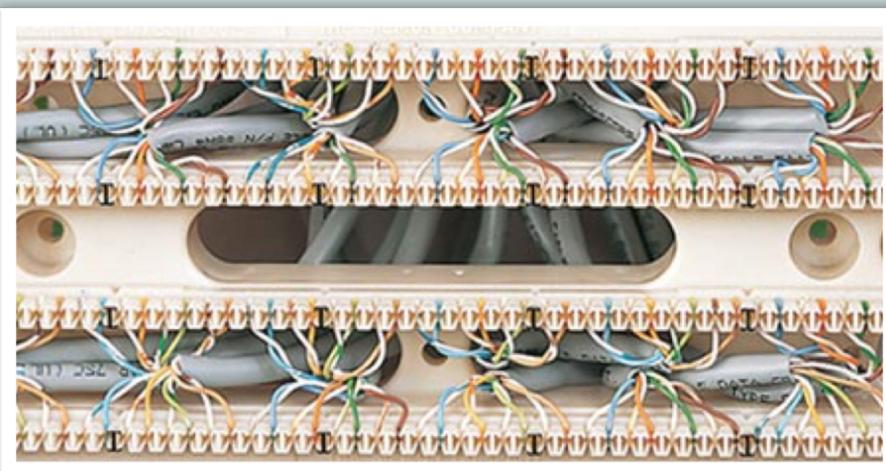
- Can be used to determine length of cable and if the cable is crimped properly

Wire Map	1	2	3	4	5	6	7	8
PASS								
(T568B)	1	2	3	4	5	6	7	8
Length (ft)				[Pair 78]		10		
Prop. Delay (ns)				[Pair 12]		16		
Delay Skew (ns)				[Pair 12]		1		
Resistance (ohms)				[Pair 36]		0.7		



# Punch-Down Tool

- Used to terminate wires on a punch-down block without stripping off the insulation
- Used with 66 block or 110 block, network jacks, and patch panels



# Butt Set

- Test equipment tools used by telephone technicians to check for dial tone or verify that a call can be placed from the line
- Limited use for network technicians unless you are working on DSL line
- Can connect to a punch-down block to connect to telephone line using alligator clips



# Toner Probe

- Allows technicians to generate a tone at one end of a connection and use the probe to audibly detect the wire pair connected to the tone generator
- Often called a “Fox and Hound”
  - Fox is a tone generator
  - Hound is a toner probe



# Time Domain Reflectometer (TDR)

- Locates breaks in copper cables and provide an estimate of severity and distance to break
- *Optical Time Domain Reflectometer (OTDR)* is used like a TDR, but for fiber-optic cables



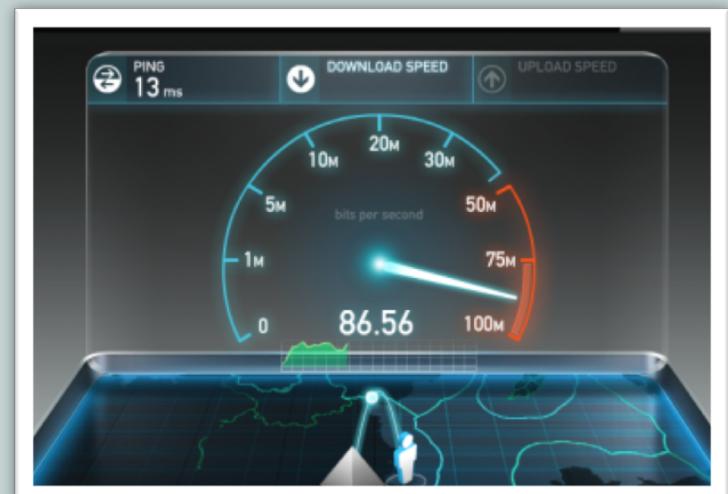


# Networking Tools (Part 2)

CompTIA Network+ (N10-007)

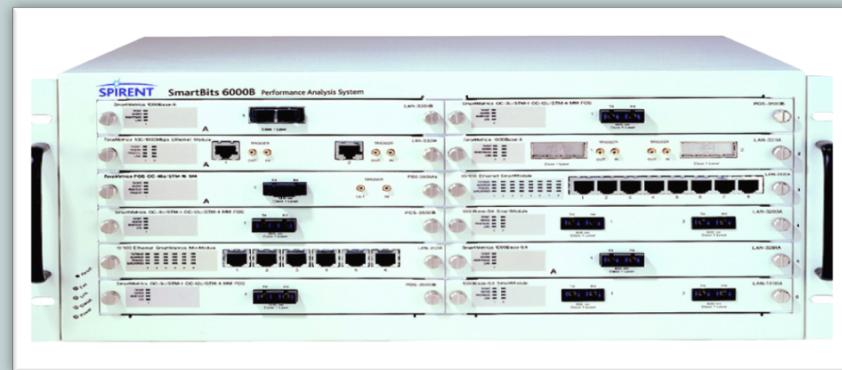
# Speed Test Sites

- Verifies throughput from client to Internet
- Downloads a random large file from the test server and uploads the file to server
  - Transfers are timed to determine connection speed
  - Uses Ping to determine latency
- Determines overall connection speed to the Internet



# Throughput Tester

- Network appliance that typically has multiple network interfaces and can generate high volumes of pseudo-random data for wired and wireless networks
- Used on prototype networks to observe how the network performs under heavy load
- Used on production networks to determine the actual throughput of the existing network



# Bit-Error Rate Tester (BERT)

- Generates patterns at one end of a link and analyzes the received patterns for errors
- Bit Error Rate (BER) is a common measurement to test networks

$$\text{BER} = \frac{\text{Bit Errors}}{\text{Bits Transferred}}$$

- Useful tool when troubleshooting interferences on a cable or fiber



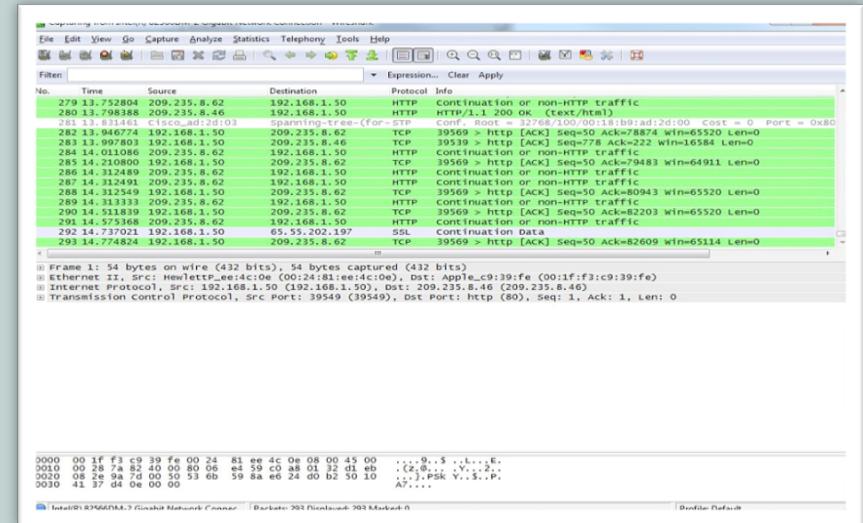
# Environmental Monitoring

- Send alerts if the temperature or humidity in a room changes above/below configured level
- Monitoring of
  - Temperature
  - Humidity
  - Power
  - Air Flow



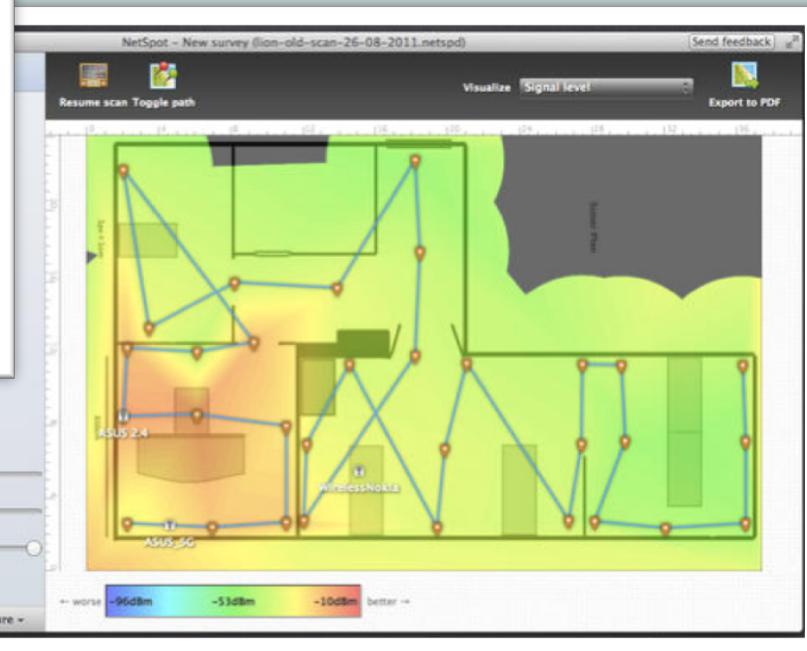
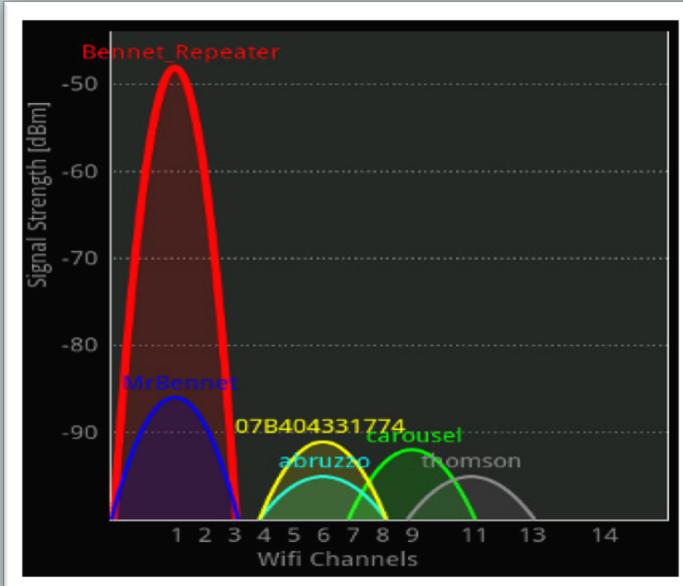
# Protocol Analyzer

- Traffic can be captured from the network and then reviewed for problems in the communication between devices
- Also known as a *network sniffer*
- Standalone device or simply software running on a laptop
  - Wireshark
  - Ethereal



# Wireless Analyzer

- Specialized software that can conduct wireless surveys to ensure proper coverage and prevent non-desired overlap



# Looking Glass Sites

- Allows users to connect to view the routing information from a server's perspective
  - Useful with BGP router configuration

**AS3327 Looking Glass**

Type of Query	Additional parameters	Node
<input type="radio"/> bgp		
<input type="radio"/> bgp advertised-routes		
<input checked="" type="radio"/> bgp summary		Tallinn (r9-Tin-Linx.EE.DataBone.net)
<input type="radio"/> ping		
<input type="radio"/> trace		
<input type="radio"/> IPv4		+ remote LG script

**Submit | Reset**

Disclaimer: All commands will be logged for possible later analysis and statistics. If you don't like this policy, please disconnect now!



# Remote Connectivity Software

- Enables you to access a network client via a PC that is located on a remote network
- Examples
  - Microsoft Remote Desktop Connection
  - RealVNC
  - GoToMyPC



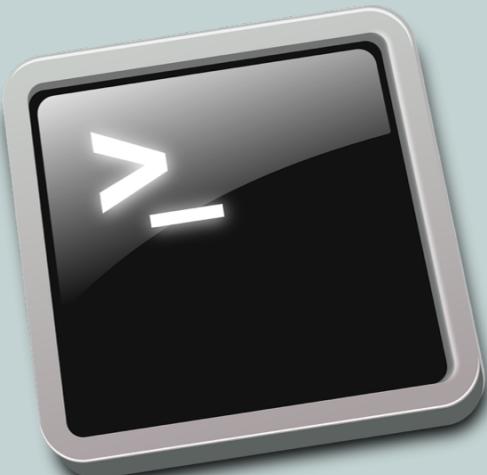


# Windows Command Line Tools

CompTIA Network+ (N10-007)

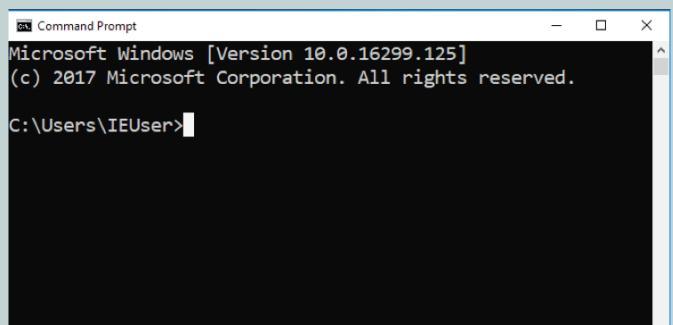
# Command Line Tools

- Used to configure and troubleshoot networks by issuing text-based commands at an operating system prompt
- Commands can be used on either clients or servers
- Commands can be specific to your version of the operating system (Windows 10, Server 2016, etc.)



# Accessing the Command Line

- Microsoft Windows Operating Systems allow you to quickly access the Command Prompt by pressing “Windows Key + R”.
- In Windows 7 or older, click START then Run, and type CMD <enter>
- In Windows 8 or newer, press your Windows key, then type CMD <enter>



# arp (Address Resolution Protocol)

- Shows the MAC address (Layer 2) for a known IP address (Layer 3)
  - **arp -a**
    - Displays the current ARP table on your computer
  - **arp -d 192.168.1.1**
    - Deletes the ARP mapping for 192.168.1.1 on all interfaces
  - **arp -s 192.168.1.1 00-AA-BB-4F-5C-23**
    - Adds a static ARP entry to force the IP provided to resolve to the MAC address provided



# arp (Address Resolution Protocol)

```
C:\ Command Prompt  
Microsoft Windows [Version 10.0.16299.125]  
(c) 2017 Microsoft Corporation. All rights reserved.  
  
C:\Users\IEUser>arp -a  
  
Interface: 10.0.2.15 --- 0x3  
Internet Address Physical Address Type  
10.0.2.2 52-54-00-12-35-02 dynamic  
10.0.2.3 52-54-00-12-35-03 dynamic  
10.0.2.255 ff-ff-ff-ff-ff-ff static  
224.0.0.22 01-00-5e-00-00-16 static  
224.0.0.252 01-00-5e-00-00-fc static  
239.255.255.250 01-00-5e-7f-ff-fa static  
255.255.255.255 ff-ff-ff-ff-ff-ff static  
  
C:\Users\IEUser>
```



# **ipconfig** **(IP Configuration)**

- Displays IP (Internet Protocol) address configuration parameters on a Windows PC
  - **ipconfig /all**
    - Provides additional configuration information
  - **ipconfig /release**
    - Releases a DHCP IP address from the PC
  - **ipconfig /renew**
    - Requests an IP address from DHCP server



# ipconfig (IP Configuration)

```
C:\ Command Prompt  
C:\Users\IEUser>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . : fios-router.home  
Link-local IPv6 Address . . . . . : fe80::c42a:e633:dbe5:1438%3  
IPv4 Address . . . . . : 10.0.2.15  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.2.2  
  
Tunnel adapter Teredo Tunneling Pseudo-Interface:  
  
Connection-specific DNS Suffix . :  
IPv6 Address . . . . . : 2001:0:9d38:953c:2451:30b9:b80b:151a  
Link-local IPv6 Address . . . . . : fe80::2451:30b9:b80b:151a%2  
Default Gateway . . . . . : ::  
  
C:\Users\IEUser>
```



# ipconfig (IP Configuration)

```
C:\ Command Prompt
C:\Users\IEUser>ipconfig /all

Windows IP Configuration

Host Name . . . . . : MSEDGEWIN10
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : fios-router.home

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : fios-router.home
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-70-92-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c42a:e633:dbe5:1438%3(Preferred)
IPv4 Address. . . . . : 10.0.2.15(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, January 24, 1882 5:17:50 AM
Lease Expires . . . . . : Saturday, March 3, 2018 11:03:30 AM
Default Gateway . . . . . : 10.0.2.2
DHCP Server . . . . . : 10.0.2.2
DHCPv6 IAID . . . . . : 34078759
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-7F-CA-39-08-00-27-70-92-1D
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
```



# ipconfig (IP Configuration)

```
C:\ Command Prompt
C:\Users\IEUser>ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::c42a:e633:dbe5:1438%3
  Default Gateway . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\IEUser>ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : fios-router.home
  Link-local IPv6 Address . . . . . : fe80::c42a:e633:dbe5:1438%3
  IPv4 Address. . . . . : 10.0.2.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.2.2

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  Connection-specific DNS Suffix . :
  IPv6 Address. . . . . : 2001:0:9d38:953c:2451:30b9:b80b:151a
  Link-local IPv6 Address . . . . . : fe80::2451:30b9:b80b:151a%2
  Default Gateway . . . . . : ::
```



# ping

- Used to check IP connectivity between two devices, most often for network troubleshooting
  - **ping www.jasondion.com**
    - Stops pinging after 4 pings (default)
  - **ping -n 10 www.jasondion.com**
    - Ping 10 times, then stop
  - **ping -t www.jasondion.com**
    - Ping forever (until user types CTRL+C)
  - **ping -6 www.jasondionping.com**
    - Ping using IPv6 addresses



# ping

```
C:\ Command Prompt  
C:\Users\IEUser>ping jasondion.com  
  
Pinging jasondion.com [50.87.237.193] with 32 bytes of data:  
Reply from 50.87.237.193: bytes=32 time=74ms TTL=127  
Reply from 50.87.237.193: bytes=32 time=74ms TTL=127  
Reply from 50.87.237.193: bytes=32 time=156ms TTL=127  
Reply from 50.87.237.193: bytes=32 time=71ms TTL=127  
  
Ping statistics for 50.87.237.193:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 71ms, Maximum = 156ms, Average = 93ms  
  
C:\Users\IEUser>
```



# tracert

- Displays the path between your device (the source) and the destination IP address, showing each route hop along the path
  - **tracert 209.85.135.99**
    - Displays the routers between your computer and the computer at 209.85.135.99
  - **tracert www.diontraining.com**
    - Displays the routers between your computer and the computer at www.google.com
  - **tracert -6 www.google.com**
    - Traces the route using IPv6



# tracert

```
C:\ Select Command Prompt
C:\Users\IEUser>tracert www.diontraining.com

Tracing route to diontraining.thinkific.com [54.221.229.100]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  10.0.2.2
 2  2 ms     1 ms     1 ms  192.168.1.1
 3  7 ms     7 ms     6 ms  lo0-100.BLTMMD-VFTTP-309.verizon-gni.net
 4  7 ms     2 ms     7 ms  B3309.BLTMMD-LCR-21.verizon-gni.net [REDACTED]
 5  *         *         * Request timed out.
 6  *         *         * Request timed out.
 7  8 ms     9 ms     9 ms  0.et-8-0-2.GW13.IAD8.ALTER.NET [140.222.0.185]
 8  8 ms     7 ms     6 ms  neustar-gw.customer.alter.net [152.179.50.58]
 9  38 ms    31 ms    31 ms  54.239.108.208
10  9 ms     12 ms   15 ms  54.239.110.138
11  24 ms    36 ms   32 ms  54.239.110.133
12  15 ms    12 ms   9 ms  54.239.108.131
13  27 ms    23 ms   19 ms  52.93.24.10
14  12 ms    10 ms   12 ms  52.93.24.1
15  *         *         * Request timed out.
16  *         *         * Request timed out.
17  *         *         * Request timed out.
18  *         *         * Request timed out.
19  *         *         * Request timed out.
20  *         *         * Request timed out.
21  *         *         * Request timed out.
22  *         *         * Request timed out.
23  *         *         * Request timed out.
24  *         *         * Request timed out.
25  *         *         * Request timed out.
26  *         *         * Request timed out.
27  *         *         * Request timed out.
28  *         *         * Request timed out.
29  *         *         * Request timed out.
30  *         *         * Request timed out.
```



# nbtstat

- Displays NetBIOS information for IP-based networks
- Displays a listing of the NetBIOS device names learned by the PC
  - **nbtstat -a <IP>**
    - Displays the NetBIOS table of the remote PC provided in <IP>
  - **nbtstat -c**
    - Displays a PC's NetBIOS name cache on the local computer



# nbtstat

```
C:\Users\ceh-student>nbtstat -A 10.3.1.6
```

```
Local Area Connection 5:
```

```
Node IpAddress: [10.3.0.6] Scope Id: []
```

## NetBIOS Remote Machine Name Table

Name	Type	Status
SERUER-PHILLY	<00>	UNIQUE
WORKGROUP	<00>	GROUP
SERUER-PHILLY	<20>	UNIQUE
WORKGROUP	<1E>	GROUP

```
MAC Address = 62-4E-5C-B3-A6-6B
```



# **netstat** **(Network Statistics)**

- Displays information for IP-based connections on a PC including current sessions, source and destination IP addresses, and port numbers
  - **netstat -a**
    - Displays all connections and listening ports
  - **netstat -n**
    - Displays addresses and port numbers in numerical form
  - **netstat -s**
    - Displays statistics for connections by protocol type (IPv4 and IPv6, TCP, UDP, and ICMP)



# `netstat -s` (Network Statistics)

```
C:\ Command Prompt
C:\Users\IEUser>netstat -s

IPv4 Statistics

Packets Received = 1714324
Received Header Errors = 0
Received Address Errors = 2
Datagrams Forwarded = 0
Unknown Protocols Received = 1
Received Packets Discarded = 217
Received Packets Delivered = 1714460
Output Requests = 453451
Routing Discards = 0
Discarded Output Packets = 2
Output Packet No Route = 49
Reassembly Required = 0
Reassembly Successful = 0
Reassembly Failures = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created = 0

IPv6 Statistics

Packets Received = 23
Received Header Errors = 0
Received Address Errors = 0
Datagrams Forwarded = 0
Unknown Protocols Received = 0
Received Packets Discarded = 90
Received Packets Delivered = 46
Output Requests = 614
Routing Discards = 0
Discarded Output Packets = 0
Output Packet No Route = 0
```



# netstat -ano (Network Statistics)

```
Command Prompt
C:\Users\IEUser>netstat -ano

Active Connections

Proto  Local Address          Foreign Address        State      PID
TCP    0.0.0.0:22              0.0.0.0:0            LISTENING  5720
TCP    0.0.0.0:135             0.0.0.0:0            LISTENING  776
TCP    0.0.0.0:445             0.0.0.0:0            LISTENING  4
TCP    0.0.0.0:5985            0.0.0.0:0            LISTENING  4
TCP    0.0.0.0:7680            0.0.0.0:0            LISTENING  6816
TCP    0.0.0.0:47001            0.0.0.0:0            LISTENING  4
TCP    0.0.0.0:49664            0.0.0.0:0            LISTENING  448
TCP    0.0.0.0:49665            0.0.0.0:0            LISTENING  1064
TCP    0.0.0.0:49666            0.0.0.0:0            LISTENING  604
TCP    0.0.0.0:49667            0.0.0.0:0            LISTENING  1832
TCP    0.0.0.0:49675            0.0.0.0:0            LISTENING  556
TCP    0.0.0.0:49676            0.0.0.0:0            LISTENING  544
TCP    10.0.2.15:139            0.0.0.0:0            LISTENING  4
TCP    10.0.2.15:5040           0.0.0.0:0            LISTENING  4084
TCP    10.0.2.15:51639          65.52.108.227:443  ESTABLISHED 2180
TCP    10.0.2.15:51646          204.79.197.200:443  ESTABLISHED 4516
TCP    10.0.2.15:51647          104.64.74.7:443   ESTABLISHED 4516
TCP    10.0.2.15:51648          72.21.91.29:80    CLOSE_WAIT  4516
TCP    10.0.2.15:51650          35.166.155.84:443  CLOSE_WAIT  4516
TCP    10.0.2.15:51653          204.79.197.222:443 ESTABLISHED 4516
TCP    10.0.2.15:51654          13.107.255.16:443  ESTABLISHED 4516
TCP    10.0.2.15:51655          72.21.81.200:443   ESTABLISHED 4516
TCP    10.0.2.15:51656          13.107.255.13:443  ESTABLISHED 4516
TCP    [::]:22                  [::]:0              LISTENING  5720
TCP    [::]:135                 [::]:0              LISTENING  776
TCP    [::]:445                 [::]:0              LISTENING  4
TCP    [::]:5985                [::]:0              LISTENING  4
TCP    [::]:7680                [::]:0              LISTENING  6816
TCP    [::]:47001               [::]:0              LISTENING  4
TCP    [::]:49664               [::]:0              LISTENING  448
```



# nslookup (Name Server Lookup)

- Resolves a fully qualified domain name (FQDN) to an IP address
  - **nslookup www.diontraining.com**
    - Non-interactive mode, provides IP address for a given domain name
  - **nslookup <enter>**
    - Loads interactive mode, allows for detailed control of the environment, including which name server to use for name resolution/lookup
    - Type **server <name>** to change which name server is used for lookup
    - Type **exit** to leave interactive mode



# nslookup (Name Server Lookup)

```
C:\ Command Prompt - nslookup
C:\Users\IEUser>nslookup diontraining.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: diontraining.com
Address: 184.168.221.2

C:\Users\IEUser>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> set q=MX
> diontraining.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
diontraining.com      MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
diontraining.com      MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
diontraining.com      MX preference = 1, mail exchanger = aspmx.l.google.com
diontraining.com      MX preference = 10, mail exchanger = aspmx2.googlemail.com
diontraining.com      MX preference = 10, mail exchanger = aspmx3.googlemail.com
> set q=CNAME
> diontraining.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

diontraining.com
    primary name server = ns37.domaincontrol.com
    responsible mail addr = dns.jomax.net
    serial = 2018022105
    refresh = 28800 (8 hours)
    retry = 7200 (2 hours)
```



# route

- Used to change or display the contents of the PC's current IP routing table
  - **route print**
    - Displays the contents of the IP routing table
  - **route delete 192.168.1.1**
    - Deletes an entry from the IP routing table with IP 192.168.1.1
  - **route add 192.168.1.1 192.168.2.1**
    - Adds a routing from 192.168.1.1 to 192.168.2.1



# route

```
C:\ Command Prompt
C:\Users\IEUser>route print
=====
Interface List
 3...08 00 27 70 92 1d ....Intel(R) PRO/1000 MT Desktop Adapter
 1........................Software Loopback Interface 1
 2...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask      Gateway      Interface Metric
          0.0.0.0        0.0.0.0    10.0.2.2    10.0.2.15     25
         10.0.2.0  255.255.255.0   On-link       10.0.2.15    281
        10.0.2.15  255.255.255.255  On-link       10.0.2.15    281
       10.0.2.255  255.255.255.255  On-link       10.0.2.15    281
         127.0.0.0    255.0.0.0   On-link      127.0.0.1    331
        127.0.0.1    255.255.255  On-link      127.0.0.1    331
 127.255.255.255  255.255.255.255  On-link      127.0.0.1    331
         224.0.0.0    240.0.0.0   On-link      127.0.0.1    331
        224.0.0.0    240.0.0.0   On-link      10.0.2.15    281
       255.255.255  255.255.255.255  On-link      127.0.0.1    331
       255.255.255  255.255.255.255  On-link      10.0.2.15    281
=====

Persistent Routes:
  None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
  2    331 ::/0        On-link
  1    331 ::1/128     On-link
  2    331 2001::/32    On-link
  2    331 2001:0:9d38:953c:309d:2207:b80b:151a/128
```



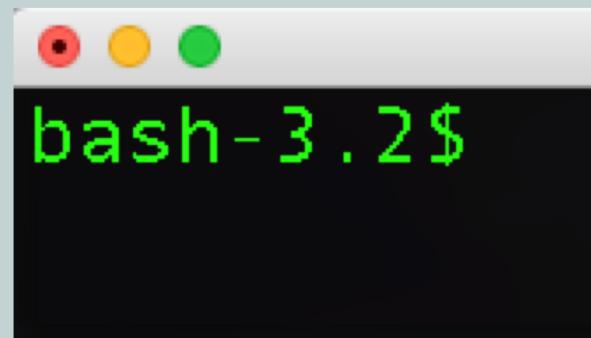


# UNIX Command Line Tools

CompTIA Network+ (N10-007)

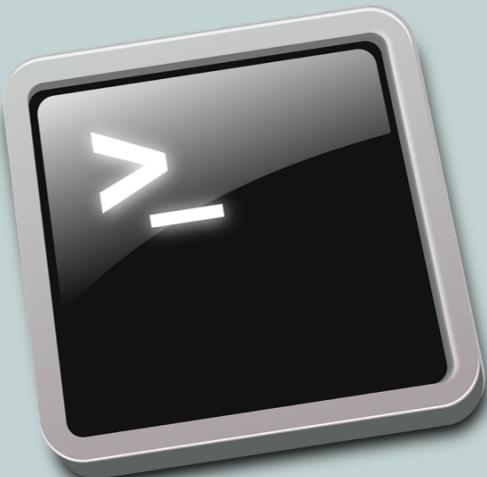
# What is UNIX?

- UNIX is implemented in various operating systems, including UNIX, BSD, Linux, and Macintosh OSX
- Command syntax between UNIX and Windows is often slightly different
- UNIX maintains manual pages in the OS, making it easy to get help from the terminal prompt (# or \$)
  - HOSTNAME# **man command**



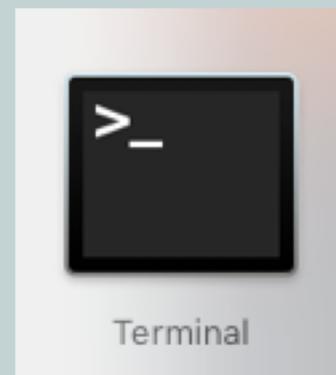
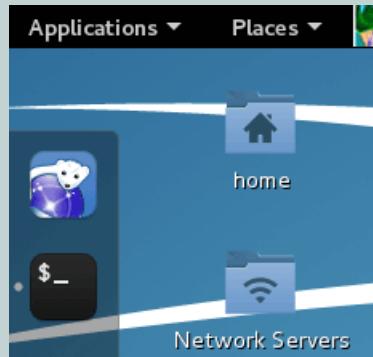
# Command Line Tools

- Used to configure and troubleshoot networks by issuing text-based commands at an operating system prompt
- Commands can be used on either clients or servers
- Commands can be specific to your version of the operating system (UNIX, BSD, OS X, or Linux variant)



# Accessing the Command Line

- In Linux or Unix, you often begin at the command line interface
- If you have a GUI, look for the terminal icon
- In OS X, open spotlight and type Terminal, or go to the Utilities folder under Applications and find Terminal



# arp (Address Resolution Protocol)

- Shows the MAC address (Layer 2) for a known IP address (Layer 3)

Same As Windows

- **arp -a**
  - Displays the current ARP table on your computer
- **arp -d 192.168.1.1**
  - Deletes the ARP mapping for 192.168.1.1 on all interfaces
- **arp -s 192.168.1.1 00-AA-BB-4F-5C-23**
  - Adds a static ARP entry to force the IP provided to resolve to the MAC address provided



# **ifconfig (Interface Configuration)**

- Displays IP (Internet Protocol) address configuration parameters on a UNIX machine
  - **ifconfig -a**
    - Provides additional configuration information
  - **ipconfig down**
    - Turn off the network adapter
  - **ipconfig up**
    - Turn on the network adapter



# ifconfig (Interface Configuration)

```
bash-3.2$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
      options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
      inet 127.0.0.1 netmask 0xff000000
      inet6 ::1 prefixlen 128
      inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
          nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      ether 78:4f:43:50:ce:6d
      inet6 fe80::45d:3f33:eb10:eeef%en0 prefixlen 64 secured scopeid 0x5
      inet 192.168.1.54 netmask 0xffffffff broadcast 192.168.1.255
          nd6 options=201<PERFORMNUD,DAD>
          media: autoselect
          status: active
en2: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
      options=60<TS04,TS06>
      ether a6:00:14:e0:31:04
      media: autoselect <full-duplex>
      status: inactive
en4: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
      options=60<TS04,TS06>
      ether a6:00:14:e0:31:05
```



# ping

- Used to check IP connectivity between two devices, most often for network troubleshooting
- Similar to Windows version, except it runs forever by default (like `-t` in Windows)
  - **ping www.jasondion.com**
    - Ping forever (until user types CTRL+C)
  - **ping -c 10 www.jasondion.com**
    - Ping 10 times, then stops automatically
  - **ping -6 www.jasondion.com**
    - Ping using IPv6 addresses



# ping

```
bash-3.2$ ping www.jasondion.com
PING jasondion.com (50.87.237.193): 56 data bytes
64 bytes from 50.87.237.193: icmp_seq=0 ttl=56 time=71.238 ms
64 bytes from 50.87.237.193: icmp_seq=1 ttl=56 time=70.550 ms
64 bytes from 50.87.237.193: icmp_seq=2 ttl=56 time=74.735 ms
64 bytes from 50.87.237.193: icmp_seq=3 ttl=56 time=74.658 ms
64 bytes from 50.87.237.193: icmp_seq=4 ttl=56 time=70.946 ms
64 bytes from 50.87.237.193: icmp_seq=5 ttl=56 time=72.342 ms
64 bytes from 50.87.237.193: icmp_seq=6 ttl=56 time=74.241 ms
64 bytes from 50.87.237.193: icmp_seq=7 ttl=56 time=73.773 ms
64 bytes from 50.87.237.193: icmp_seq=8 ttl=56 time=71.857 ms
64 bytes from 50.87.237.193: icmp_seq=9 ttl=56 time=75.165 ms
64 bytes from 50.87.237.193: icmp_seq=10 ttl=56 time=70.765 ms
64 bytes from 50.87.237.193: icmp_seq=11 ttl=56 time=70.338 ms
64 bytes from 50.87.237.193: icmp_seq=12 ttl=56 time=72.443 ms
64 bytes from 50.87.237.193: icmp_seq=13 ttl=56 time=71.671 ms
64 bytes from 50.87.237.193: icmp_seq=14 ttl=56 time=70.313 ms
64 bytes from 50.87.237.193: icmp_seq=15 ttl=56 time=74.017 ms
64 bytes from 50.87.237.193: icmp_seq=16 ttl=56 time=71.655 ms
64 bytes from 50.87.237.193: icmp_seq=17 ttl=56 time=71.072 ms
64 bytes from 50.87.237.193: icmp_seq=18 ttl=56 time=73.649 ms
64 bytes from 50.87.237.193: icmp_seq=19 ttl=56 time=71.477 ms
64 bytes from 50.87.237.193: icmp_seq=20 ttl=56 time=72.978 ms
^C
```



# traceroute

- Displays the path between your device (the source) and the destination IP address, showing each route hop along the path
  - **traceroute 209.85.135.99**
    - Displays the routers between your computer and the computer at 209.85.135.99
  - **traceroute www.diontraining.com**
    - Displays the routers between your computer and the computer at www.google.com
  - **traceroute -6 www.google.com**
    - Traces the route using IPv6



# traceroute

```
bash-3.2$ traceroute www.google.com
traceroute to www.google.com (172.217.12.228), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  1.304 ms  0.988 ms  0.950 ms
 2  lo0-100.bltmmd-vfttp-309.verizon-gni.net [REDACTED]  4.111 ms  5.528 ms
 5.803 ms
 3  b3309.bltmmd-lcr-22.verizon-gni.net (130.81.175.156)  10.426 ms
    b3309.bltmmd-lcr-21.verizon-gni.net (130.81.175.154)  7.495 ms  7.292 ms
 4  * * *
 5  * * *
 6  0.et-8-0-2.gw13.iad8.alter.net (140.222.0.185)  12.247 ms  9.213 ms
    0.et-11-1-2.gw13.iad8.alter.net (140.222.225.219)  7.146 ms
 7  204.148.79.46 (204.148.79.46)  9.878 ms  14.206 ms  8.349 ms
 8  108.170.246.1 (108.170.246.1)  10.953 ms  * *
 9  108.170.232.19 (108.170.232.19)  9.099 ms
    72.14.234.135 (72.14.234.135)  13.443 ms  8.590 ms
10  iad30s15-in-f4.1e100.net (172.217.12.228)  11.704 ms  6.916 ms  10.529 ms
bash-3.2$
```



# **netstat** **(Network Statistics)**

- Displays information for IP-based connections on a PC including current sessions, source and destination IP addresses, and port numbers

Same As Windows

- **netstat -a**
  - Displays all connections and listening ports
- **netstat -n**
  - Displays addresses and port numbers in numerical form
- **netstat -s**
  - Displays statistics for connections by protocol type (IPv4 and IPv6, TCP, UDP, and ICMP)



# netstat -an (Network Statistics)

```
bash-3.2$ netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 192.168.1.54.59622    52.86.150.190.443  ESTABLISHED
tcp4       0      0 192.168.1.54.59621    40.69.216.251.443  ESTABLISHED
tcp4       0      0 127.0.0.1.6234        *.*                  LISTEN
tcp4       0      0 192.168.1.54.59614    52.109.12.24.443  ESTABLISHED
tcp4       0      0 192.168.1.54.59571    40.97.139.114.443  ESTABLISHED
tcp4      31      0 192.168.1.54.59568    162.125.6.3.443   CLOSE_WAIT
tcp4       0      0 192.168.1.54.59559    131.253.34.238.443 ESTABLISHED
tcp4       0      0 192.168.1.54.59507    199.16.156.52.443  ESTABLISHED
tcp4      31      0 192.168.1.54.59449    162.125.34.6.443   CLOSE_WAIT
tcp4       0      0 192.168.1.54.59414    35.153.45.34.443  ESTABLISHED
tcp4       0      0 192.168.1.54.59325    52.201.32.182.443  CLOSE_WAIT
tcp4      31      0 192.168.1.54.59273    162.125.6.5.443   CLOSE_WAIT
tcp4       0      0 192.168.1.54.59134    162.125.18.133.443 ESTABLISHED
tcp4       0      0 192.168.1.54.58872    50.87.237.193.143  ESTABLISHED
tcp4       0      0 192.168.1.54.58550    50.17.178.82.443  ESTABLISHED
tcp4       0      0 192.168.1.54.58525    40.97.24.2.443   ESTABLISHED
tcp4       0      0 192.168.1.54.58524    173.194.68.125.5222 ESTABLISHED
tcp4       0      0 192.168.1.54.58523    17.36.205.4.993   ESTABLISHED
tcp4       0      0 192.168.1.54.58513    173.194.68.188.5228 ESTABLISHED
tcp4       0      0 192.168.1.54.58498    50.87.237.193.143  ESTABLISHED
tcp4       0      0 192.168.1.54.58497    17.249.172.15.5223 ESTABLISHED
```



# **nslookup and host (Name Server Lookup)**

- Resolves a fully qualified domain name (FQDN) to an IP address

**Same As Windows**

- **nslookup www.diontraining.com**
  - Non-interactive mode, provides IP address for a given domain name
- **host www.diontraining.com**
  - Host works like nslookup, except it only provides a single line response with the address



# host

```
konsole — bash — 80x24
bash-3.2$ host www.diontraining.com
www.diontraining.com is an alias for diontraining.thinkific.com.
diontraining.thinkific.com has address 54.221.229.100
diontraining.thinkific.com has address 54.225.68.244
diontraining.thinkific.com has address 23.21.157.83
diontraining.thinkific.com has address 107.21.123.200
bash-3.2$
```



# Dig (Name Server Lookup)

- Resolves a fully qualified domain name (FQDN) to an IP address and provides even more detailed information than nslookup
- **dig** has no interactive mode
  - **Dig –t mx google.com**
    - Looks up the mail records (mx) for google.com



# Dig (Name Server Lookup)

```
konsole — bash — 80x24
bash-3.2$ dig -t mx diontraining.com

; <>> DiG 9.8.3-P1 <>> -t mx diontraining.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61753
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;diontraining.com.           IN      MX

;; ANSWER SECTION:
diontraining.com.    2154    IN      MX      5 alt1.aspmx.l.google.com.
diontraining.com.    2154    IN      MX      5 alt2.aspmx.l.google.com.
diontraining.com.    2154    IN      MX      1 aspmx.l.google.com.
diontraining.com.    2154    IN      MX      10 aspmx2.googlemail.com.
diontraining.com.    2154    IN      MX      10 aspmx3.googlemail.com.

;; Query time: 21 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Mar  2 15:18:03 2018
;; MSG SIZE  rcvd: 164

bash-3.2$
```



# route

- Used to change or display the contents of the PC's current IP routing table
  - **route**
    - Displays the contents of the IP routing table
  - **route -n**
    - Displays the content of the IP routing table, including the default gateway



# route

```
root@backup2:~# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
default         5.153.23.97-sta 0.0.0.0      UG    100    0        0 eth1
5.153.23.96   *               255.255.255.248 U      0    0        0 eth1
10.0.0.0       10.70.203.65   255.0.0.0      UG    0    0        0 eth0
10.70.203.64  *               255.255.255.192 U      0    0        0 eth0
root@backup2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         5.153.23.97   0.0.0.0      UG    100    0        0 eth1
5.153.23.96   0.0.0.0        255.255.255.248 U      0    0        0 eth1
10.0.0.0       10.70.203.65   255.0.0.0      UG    0    0        0 eth0
10.70.203.64  0.0.0.0        255.255.255.192 U      0    0        0 eth0
root@backup2:~#
```

