Chapter 3

Addressing on Networks

Abdoul Rassaki

arassaki@iie.ac.za

Objectives

- Find the MAC address of a computer and explain its function in network communications
- Configure TCP/IP settings on a computer, including IP address, subnet mask, default gateway, and DNS servers
- Explain the purpose of ports and sockets, and identify the ports of several common, network protocols
- Describe domain names and the name resolution process
- Use command-line tools to troubleshoot problems with network addresses

Addressing Overview

- Four addressing methods:
  - ***Data Link layer MAC address***
    - 48 bits, written as six hex numbers separated by colons
    - Also called physical address
  - ***Network layer IP address***
    - IPv4 addresses have 32 bits and are written as four decimal numbers called octets
    - IPv6 addresses have 128 bits and are written as eight blocks of hexadecimal number
  - ***Transport layer port numbers***
    - It identifies an application that might be running on a host
  - ***Application layer FQDNs***, computer names, and host names
    - Fully qualified domain name (FQDN)—A unique character-based name

MAC Addresses

- Traditional MAC addresses contain two parts:
  - Example: 48 bits long, 00:60:8C:00:54:99
  - First 24 bits are known as the **OUI (Organizationally Unique Identifier**) or manufacturer-ID
    - Assigned by the IEEE (Institute of Electrical and Electronics Engineers)
  - Last 24 bits make up the **extension identifier or device ID**
    - Manufacturers assign each NIC a unique device ID

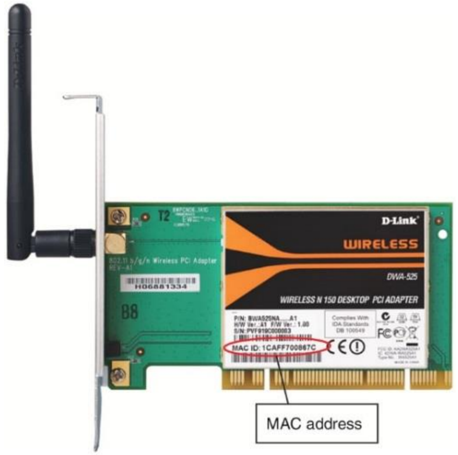


Figure 3-1 NIC with MAC address

Source: D-Link of North America

IP Addresses (1 of 2)

- **Static IP addresses** are assigned manually by the network administrator
- **Dynamic IP addresses** are automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server
    - You’ll learn more about DHCP later in the chapter
- To view TCP/IP settings on a Windows 10 computer:
    - In Control Panel, open the Network and Sharing Center. Click Change adapter settings
- Brief explanation of settings:
    - **Gateway**—Device that nodes use for access to the outside world
    - **Subnet mask**—Used to indicate what portion of an IP address is the network portion (network ID) and what part is the host portion (host ID)
    - **DNS server**—Server responsible for tracking computer names and their IP addresses

IP Addresses (2 of 2)

- You can use the **ipconfig** utility in a Command Prompt to find out current TCP/IP settings
- Two types of IP addresses:
    - IPv4—A 32-bit address
    - IPv6—A 128-bit address

IPv4 Addresses (1 of 7)

- **IPv4 addresses**
  - 32-bit address organized into four groups of 8 bits each (known as octets)
  - Each of the four octets can be any number from 0 to 255
  - Some IP addresses are reserved
- Example of an IPv4 address: 72.56.105.12

IPv4 Addresses (2 of 7)

- **Classful addressing**
  - The dividing line between the network and host portions is determined by the numerical range the IP address falls in
- Classful IPv4 addresses are divided into five classes:
  - Class A, Class B, Class C, Class D, and Class E
- Classes A, B, and C licensed IP addresses are available for use on the Internet
  - Called **public IP addresses**
- A company can use **private IP addresses** on its private networks
- IEEE recommends the following IP addresses be used for private networks:
  - 10.0.0.0 through 10.255.255.255
  - 172.16.0.0 through 172.31.255.255
  - 192.168.0.0 through 192.168.255.255

IPv4 Addresses (3 of 7)

- Table 3-1 IP address classes
  - Class A begin with octets 1–126
  - Class B begin with octets 128–191
  - Class C begins with octets 192-223

Classa	Network Octets	Approximate Number of possible networks	Approximate Number of IP addresses in each network
A	1.x.y.z to 126.x.y.z	126	16 million
B	128.0.x.y to 191.255.x.y	16 000	65 000
C	192.0.0.x to 223.255.255.x	2 million	254

IPv4 Addresses (4 of 7)

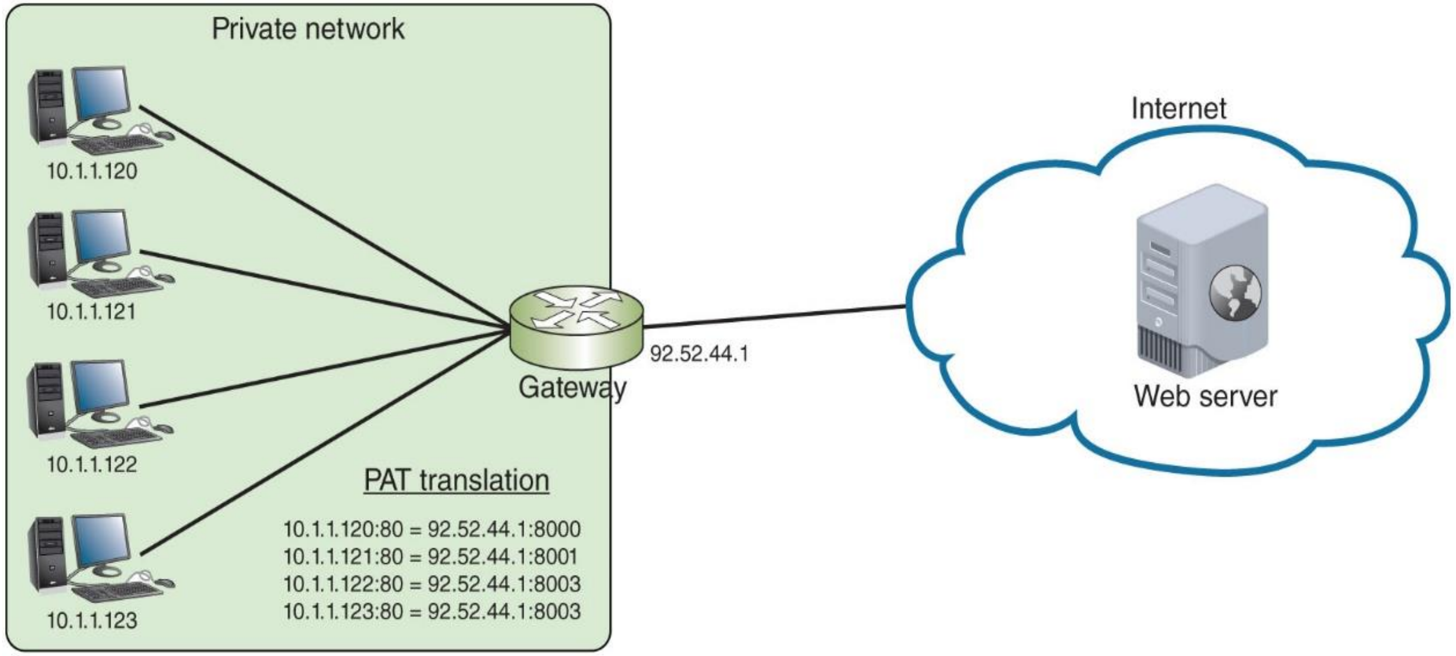
- Classes D and E addresses were not available for general use:
  - Class D begin with octets 224–239 and are used for **multicasting**
  - Class E begin with octets 240–254 and are used for research
- Table 3-2 Reserved IP addresses

IP addresses	Function
255.255.255.255	Used for **broadcast messages** by TCP/IP background processes. Broadcast message is read by every node on the net
0.0.0.0	Currently unassigned
127.0.0.1 through 127.255.255.254	Used for research and can indicate your own PC, in which case it is **loopback address**
169.254.0.1 through 169.254.255.254	Used to create an **APIPA (Automatic Private IP Addressing)** address when a computer configured for DH CP first connects to the network and is unable to lease an IPv4 address from the DHCP server

IPv4 Addresses (5 of 7)

- **Network Address Translation (NAT**)—A technique designed to conserve public IP addresses needed by a network
- **Address translation**—Process where a gateway device substitutes the private IP addresses with its own public address
  - When these computers need access to other networks or Internet
- **Port Address Translation (PAT**)—Process of assigning a TCP port number to each ongoing session between a local host and Internet host

IPv4 Addresses (6 of 7)



10.1.1.120:80 = 92.52.44.1:8000
10.1.1.121:80 = 92.52.44.1:8001
10.1.1.122:80 = 92.52.44.1:8003
10.1.1.123:80 = 92.52.44.1:8003

Figure 3-9 PAT (Port Address Translation)

IPv4 Addresses (7 of 7)

- Two variations of NAT to be aware of:
  - **SNAT (Static (or Source) Network Address Translation**)—The gateway assigns the same public IP address to a host each time it makes a request to access the Internet
  - **DNAT (Dynamic (or Destination) Network Address Translation**)—The gateway has a pool of public address that it is free to assign to a local host when it makes a request to access the Internet

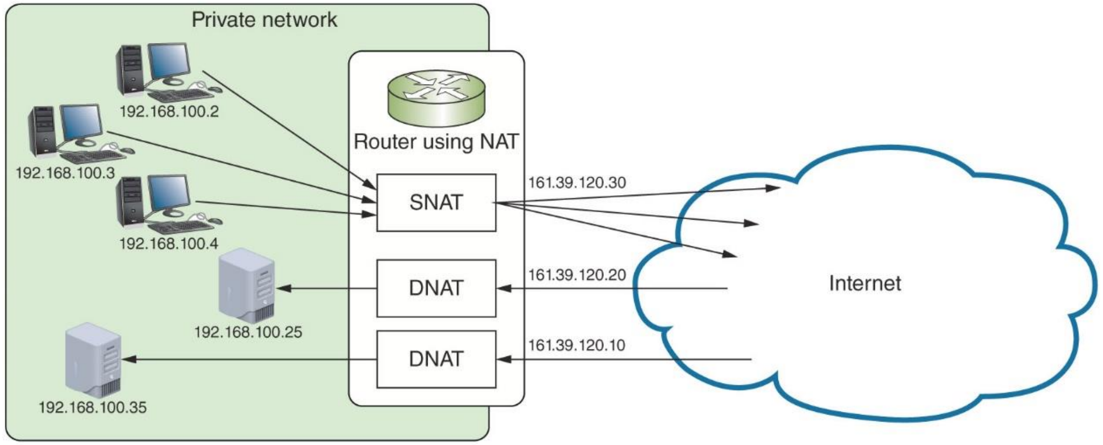


Figure 3-10 SNAT for outgoing messages, and DNAT for incoming messages

IPv6 Addresses (1 of 7)

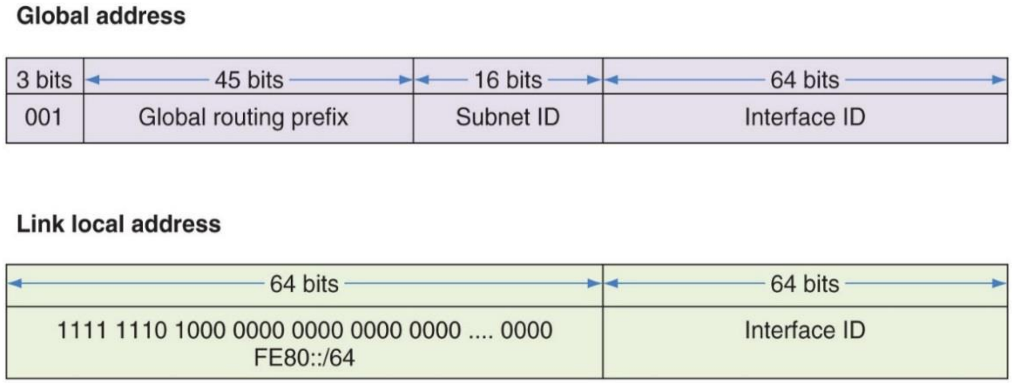
- An IPv6 address has 128 bits written as eight blocks of hexadecimal numbers separated by colons:
  - For example, 2001:0000:0B80:0000:0000:00D3:9C5A:00CC
  - Each block is 16 bits
  - Leading zeros in a four-character hex block can be eliminated
  - If blocks contain all zeroes, they can be written as **double colons (::),** only one set of double colons is used in an IP address
  - Therefore, above example can be written two ways:
    - 2001::B80:0000:0000:D3:9C5A:CC
    - 2001:0000:B80::D3:9C5A:CC (preferred method because it contains fewest zeroes)

IPv6 Addresses (2 of 7)

- IPv6 terminology:
  - **Link** (sometimes called local link)—Any LAN bounded by routers
  - An **interface** is a node’s attachment to a link
  - **Dual stacked**—When a network is configured to use both IPv4 and IPv6
    - Tunneling—A method used by IPv6 to transport IPv6 packets through or over an IPv4 network
  - **Interface ID**—The last 64 bits or four blocks of an IPv6 address that identify the interface
  - **Neighbors**—Two or more nodes on the same link

IPv6 Addresses (3 of 7)

- Types of IPv6 addresses:
  - **Unicast address**—Specifies a single node on a network
    - Global unicast address—Can be routed on the Internet
    - Link local unicast address—Can be used for communicating with nodes in the same link
  - **Multicast address**—Packets are delivered to all nodes on a network
  - **Anycast address**—Can identify multiple destinations, with packets delivered to the closest destination



Global address

3 bits	45 bits	16 bits	64 bits
001	Global routing prefix	Subnet ID	Interface ID

Link local address

64 bits	64 bits
1111 1110 1000 0000 0000 0000 0000 .... 0000 FE80::/64	Interface ID

Figure 3-13 Two types of IPv6 addresses

IPv6 Addresses (4 of 7)

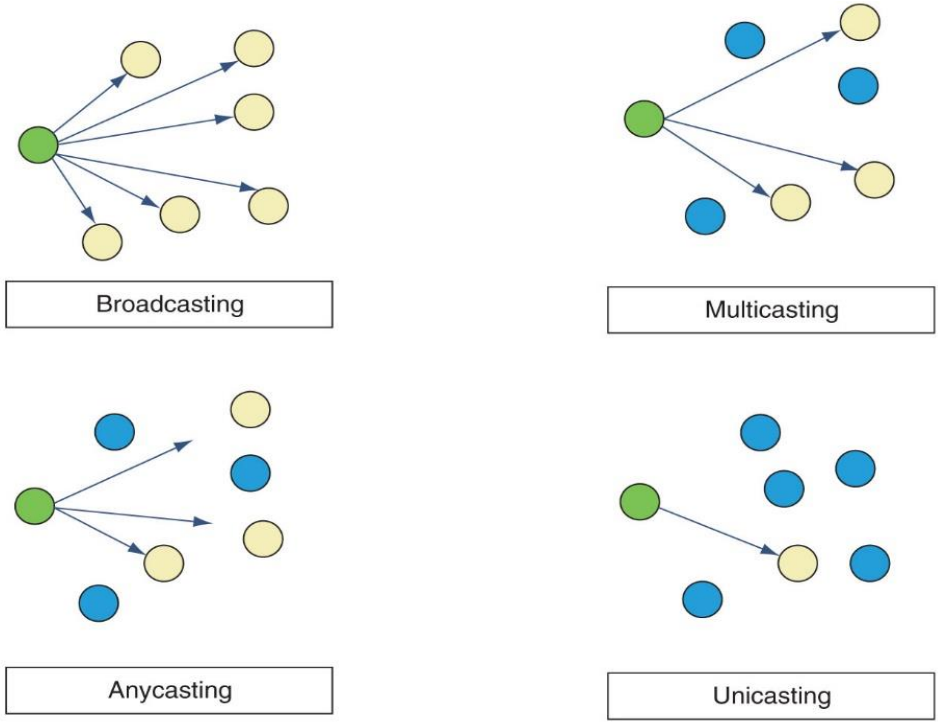


Figure 3-14 Concepts of broadcasting, multicasting, anycasting, and unicasting

IPv6 Addresses (5 of 7)

- Table 3-3 Address prefixes for types of IPv6 addresses

IP address type	Address prefix	Notes
Global Unicast	2000::/3	First 3 bits are always 001
Link local Unicast	FE80::/64	First 64 bits are always 1111 1110 1000 0000 0000 0000 …. 0000
Unique local Unicast	FC00::/7	First 7 bits are always 1111 110
	FD00::/8	First 8 bits are always 1111 1101
Multicast	FF00::/8	First 8 bits are always 1111 1111

IPv6 Addresses (6 of 7)

- **IPV6 Auto configuration**:
  - IPv6 addressing is designed so that a computer can autoconfigure its own link local IP address
  - Similar to how IPv4 uses an APIPA address
- Step 1—The computer creates its IPv6 address:
  - Uses FE80::/64 as the first 64 bits (called prefix)
  - Last 64 bits can be generated in two ways:
    - Randomly generated
    - Generated from the network adapter’s MAC address
- Step 2—The computer checks to make sure its IP address is unique on the network

IPv6 Addresses (7 of 7)

- Step 3—The computer asks if a router on the network can provide configuration information (message is called a **RS or router solicitation)**
  - If a router responds with DHCP information, the computer uses whatever information this might be (called a **RA or router advertisement)**
    - Such as the IP addresses of DNS server or the network prefix
  - Process is called prefix discovery
    - The computer uses the prefix to generate its own link local or global IPv6 address by appending its interface ID to the prefix

Ports and Sockets (1 of 3)

- **Port numbers**—Ensure data is transmitted to the correct **process** among multiple processes running on the computer
- **Socket**—Consists of host’s IP address and the port number of an application running on the host:
  - Colon separates the two values
  - Example—10.43.3.87:23
- Port numbers are divided into three types:
  - Well-known ports—0 to 1023
  - Registered ports—1024 to 49151
  - Dynamic and private ports—49152 to 65535

Ports and Sockets (2 of 3)

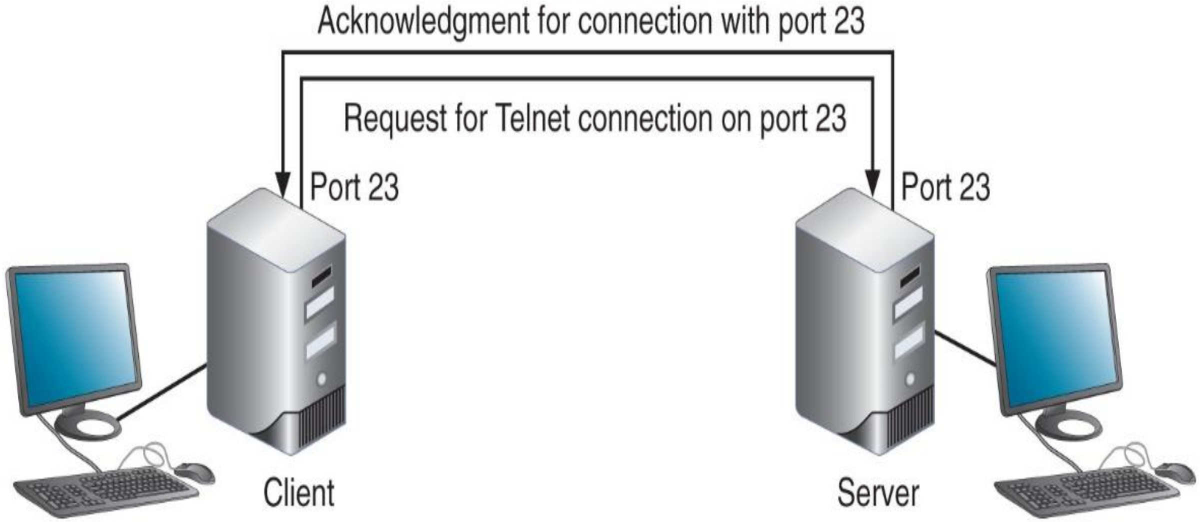

Acknowledgment for connection with port 23
Request for Telnet connection on port 23
Port 23
Port 23
Client
Server

Figure 3-16 A virtual connection for the Telnet service

Ports and Sockets (3 of 3)

- Protocols not yet covered:
  - TFTP (Trivial File Transfer Protocol)
  - NTP (Network Time Protocol)
  - LDAP (Lightweight Directory Access Protocol)
  - SMB (Server Message Block)
  - SIP (Session Initiation Protocol)
  - H.323 (Signaling protocol used to make connections between hosts)

Domain Names and DNS (1 of 3)

- Character-based names are easier to remember than numeric IP addresses
- Last part of an FQDN is called the **top-level domain (TLD)**
- Domain names must be registered with an Internet naming authority that works on behalf of ICANN
  - ICANN restricts what type of hosts can be associated with .arpa, .mil, .int, .edu, and .gov
- **Name resolution** is the process of discovering the IP address of a host when you know the FQDN

Domain Names and DNS (2 of 3)

- Table 3-5 Some well-known top-level domains

Domain suffix	Type of organization
ARPA	Reverse lookup (Special Internet function)
COM	Commercial
EDU	Educational
GOV	Government
ORG	Non commercial organization (Non profit agency)
NET	Network such as ISP
MIL	Military organization
BIZ	Businesses
INFO	Unrestricted use

Domain Names and DNS (3 of 3)

- DNS is an Application layer client-server system of computers and databases made up of these elements:
  - **namespace**—The entire collection of computer names and their associated IP addresses stored in databases on DNS name servers around the globe
  - **name servers**—Hold databases, which are organized in a hierarchical structure
  - **resolvers**—A DNS client that requests information from DNS name servers

Namespace Databases

- Each organization that provides host services is responsible for providing and maintaining its own DNS authoritative servers for public access
  - **Authoritative server** is the authority on computer names and their IP addresses for computers in their domains
- The domains that the organization is responsible for managing are called a **DNS zone**

Name Servers (1 of 4)

- Four common types of DNS servers:
  - *Primary DNS server*—The authoritative name server for the organization
    - Holds the authoritative DNS database for the organization’s zones
  - *Secondary DNS server*—Backup authoritative name server for the organization
  - *Caching DNS server*—Accesses the public DNS data and caches the DNS information it collects
  - *Forwarding DNS server*—Receives queries from local clients but doesn’t work to resolve the queries
- Any of these server types can co-exist on the same machine

Name Servers (2 of 4)

- DNS name servers are organized in a hierarchical structure
- At the root level, 13 clusters of root server hold information used to locate top-level domain (TLD) servers
- TLD servers hold information about authoritative servers owned by various organizations

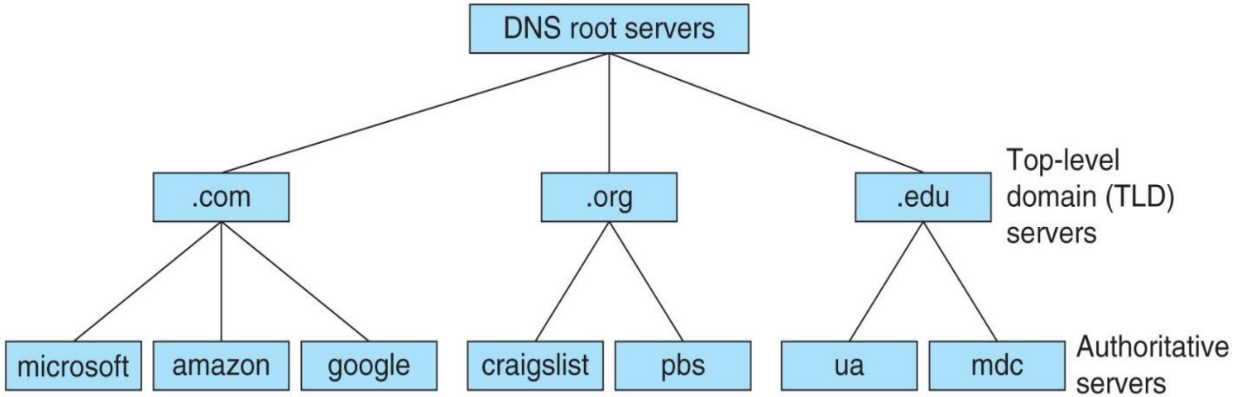


Figure 3-17 Hierarchy of name servers

Name Servers (3 of 4)

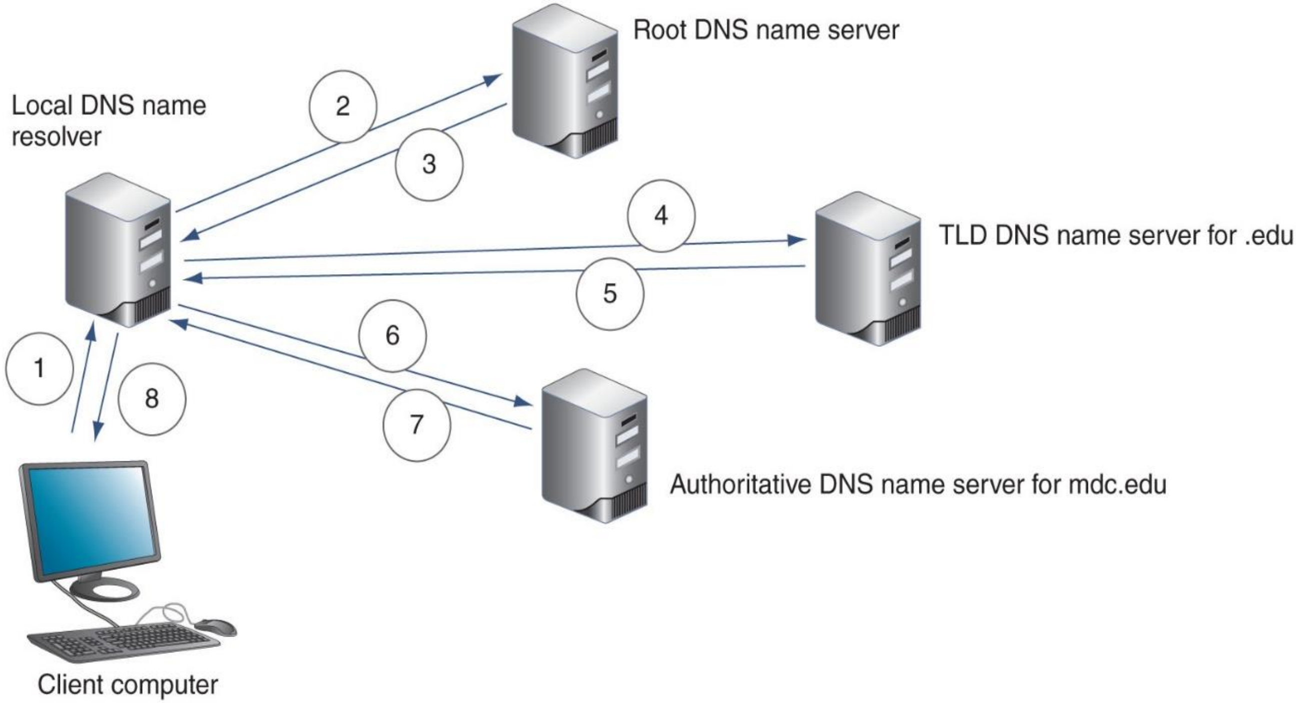

Root DNS name server
Local DNS name resolver
2
3
4
TLD DNS name server for .edu
5
6
1
8
7
Authoritative DNS name server for mdc.edu
Client computer

Figure 3-18 Queries for name resolution of *www.mdc.edu*

Name Servers (4 of 4)

- Ways the resolution process can get more complex:
  - Caching server typically is not the same machine as the authoritative server
    - Caching server exists only to resolve names for its own local clients
  - Name servers within a company might not have access to root servers
  - A TLD name server might be aware of an intermediate name server rather than the authoritative name server
- Two types of DNS requests:
  - **Recursive**—A query that demands a resolution or the answer “It can’t be found”
  - **Iterative**—A query where the local server issues queries to other servers
    - Other servers only provide information if they have it
    - Do not demand a resolution

Resource Records in a DNS Database

- Several types of records, called resource records are kept in a DNS database:
  - A (Address) record—Stores the name-to-address mapping for a host
  - AAAA (Address) record—Holds the name-to-address mapping, the IP address is an IP v6 type IP address
  - CNAME (Canonical Name) record—Holds alternative names for a host
  - PTR (Pointer) record—Used for reverse lookups
  - NS (Name Server) record—Indicates the authoritative name server for a domain
  - MX (Mail Exchanger) record—Identifies a mail server and is used for email traffic
  - SRV (Service) record—Identifies the hostname and port of a computer that hosts a specific network services besides email
  - TXT (Text) record—Holds any type of free-form text

DNS Server Software (1 of 2)

- BIND (Berkeley Internet Name Domain)—Most popular DNS server software
  - Open source—The term for software whose code is publicly available for use and modification
- Microsoft DNS Server—Built-in DNS service in the Windows Server OS
- For a more secure network:
  - Internal and external DNS queries should be handled by different DNS servers
  - Can use a firewall to filter or block traffic between networks
- DMZ or demilitarized zone
  - Area between two firewalls

DNS Server Software (2 of 2)

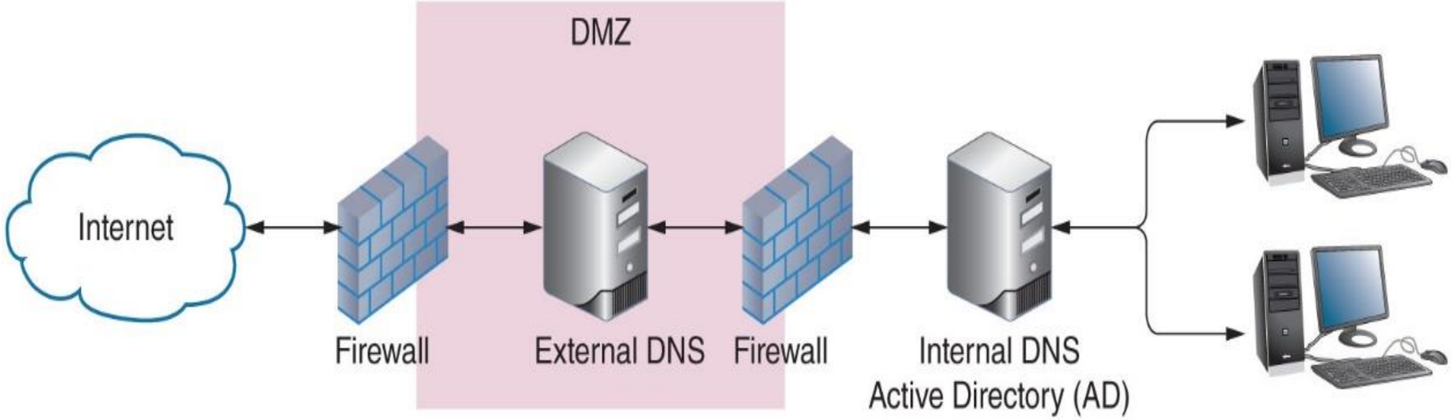
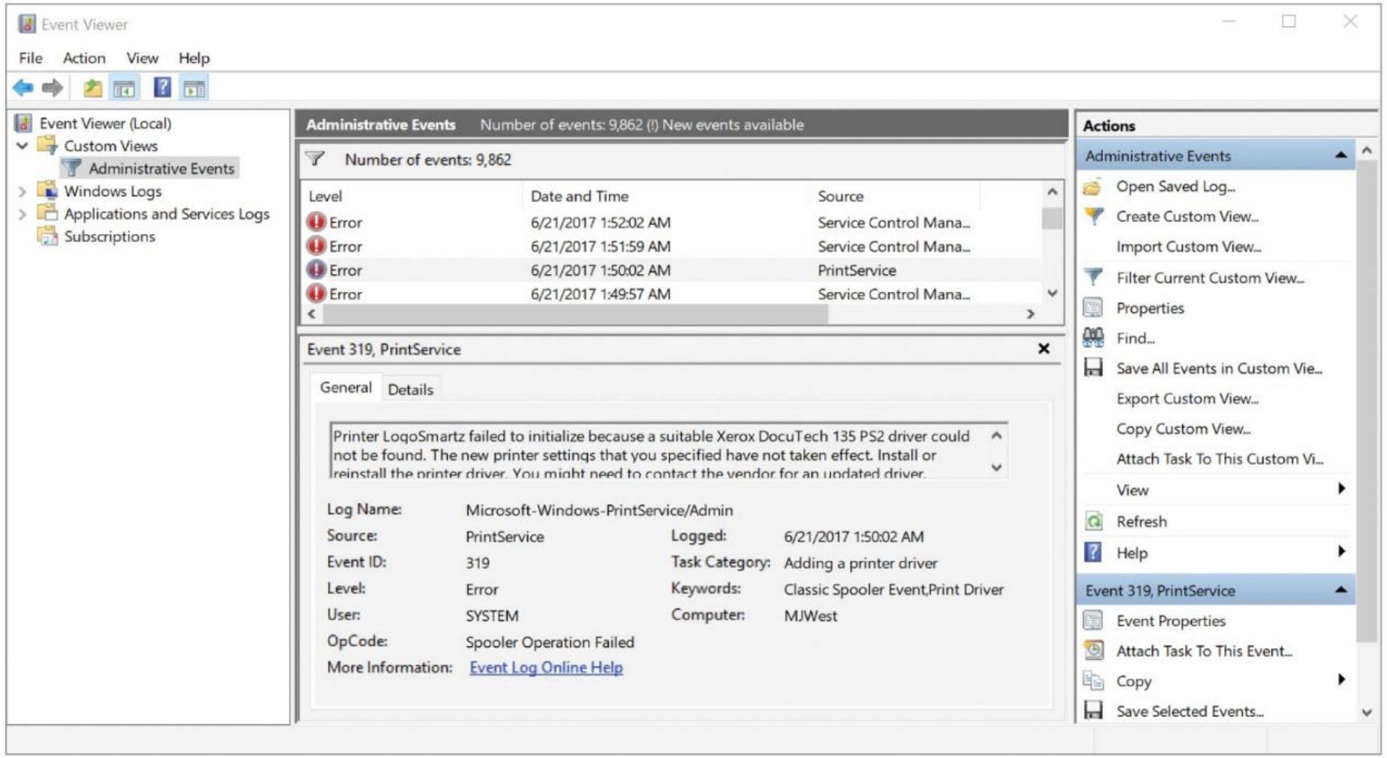


Figure 3-19 DNS services handled by two different servers so that the internal network remains protected

Troubleshooting Address Problems



Administrative Events Number of events: 9,862 (!) New events available

Number of events: 9,862

Level	Date and Time	Source
Error	6/21/2017 1:52:02 AM	Service Control Mana...
Error	6/21/2017 1:51:59 AM	Service Control Mana...
Error	6/21/2017 1:50:02 AM	PrintService
Error	6/21/2017 1:49:57 AM	Service Control Mana...

Event 319, PrintService

Printer LogoSmartz failed to initialize because a suitable Xerox DocuTech 135 PS2 driver could not be found. The new printer settings that you specified have not taken effect. Install or reinstall the printer driver. You might need to contact the vendor for an updated driver.

Log Name:	Microsoft-Windows-PrintService/Admin		
Source:	PrintService	Logged:	6/21/2017 1:50:02 AM
Event ID:	319	Task Category:	Adding a printer driver
Level:	Error	Keywords:	Classic Spooler Event,Print Driver
User:	SYSTEM	Computer:	MJWest
OpCode:	Spooler Operation Failed		
More Information:	Event Log Online Help		

Figure 3-20 Event Viewer provided the diagnosis of a problem and recommended steps to fix the problem

Troubleshooting Tools (1 of 12)

- Command-link tools are a great resource to troubleshoot network problems
- Some of the most helpful tools:
  - **ping**
  - **ipconfig** (Windows only)
  - **ifconfig** (Linux only)
  - **nslookup**
  - **dig** (Linux only)

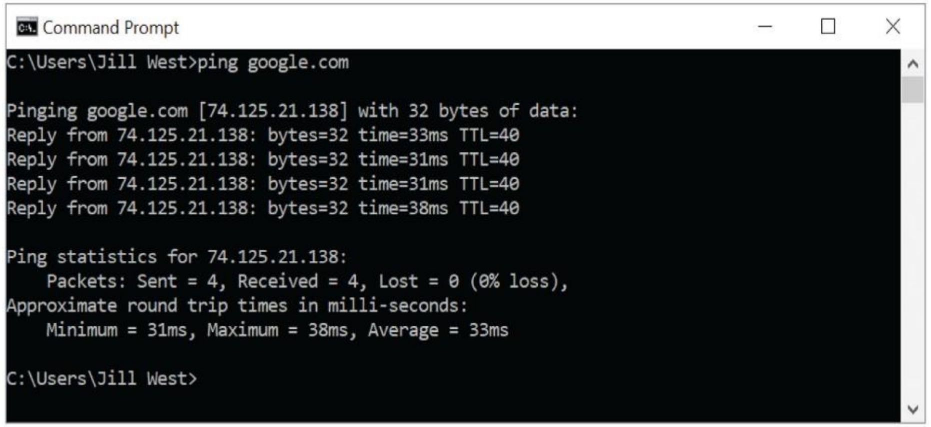
Troubleshooting Tools (2 of 12)

- **ping (Packet Internet Groper)**—Used to verify that TCP/IP is:
  - Installed
  - Bound to the NIC
  - Configured correctly
  - Communicating with the network
- The ping utility sends out a signal called an echo request to another device (request for a response)
  - Other computer responds in the form of an echo reply
- **ICMP (Internet Control Message Protocol**)—Protocol used by the echo request/reply to carry error messages and information about the network

Troubleshooting Tools (3 of 12)

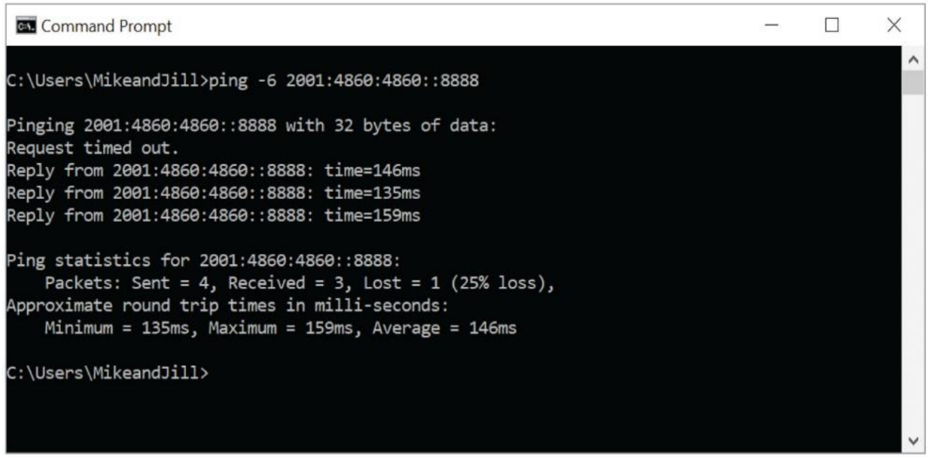
- IPv6 networks use a version of ICMP called ICMPv6:
  - ping6—On Linux computers running IPv6, use **ping6** to verify whether an IPv6 host is available
  - ping -6—On Windows computers, use **ping** with the **-6** switch to verify connectivity on IPv6 networks
- For the **ping6** and **ping -6** commands to work over the Internet, you must have access to the IPv6 Internet

Troubleshooting Tools (4 of 12)



```
C:\Users\Jill West>ping google.com

Pinging google.com [74.125.21.138] with 32 bytes of data:
Reply from 74.125.21.138: bytes=32 time=33ms TTL=40
Reply from 74.125.21.138: bytes=32 time=31ms TTL=40
Reply from 74.125.21.138: bytes=32 time=31ms TTL=40
Reply from 74.125.21.138: bytes=32 time=38ms TTL=40

Ping statistics for 74.125.21.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 38ms, Average = 33ms

C:\Users\Jill West>
```

Figure 3-22 Results of a successful `ping`

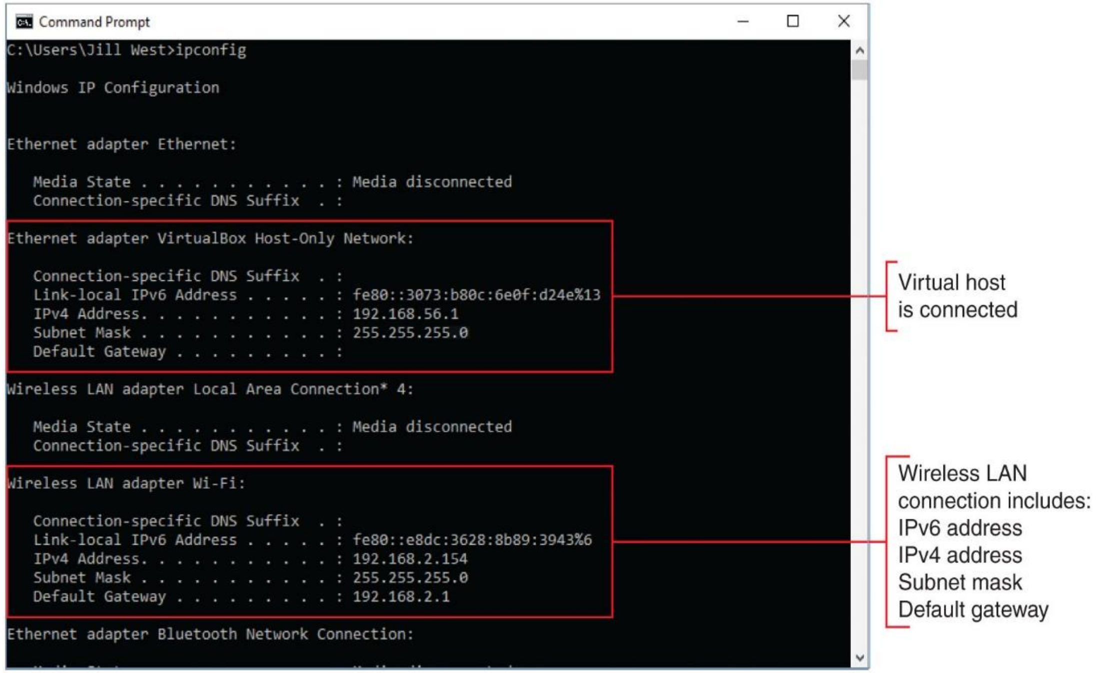


```
C:\Users\MikeandJill>ping -6 2001:4860:4860::8888

Pinging 2001:4860:4860::8888 with 32 bytes of data:
Request timed out.
Reply from 2001:4860:4860::8888: time=146ms
Reply from 2001:4860:4860::8888: time=135ms
Reply from 2001:4860:4860::8888: time=159ms

Ping statistics for 2001:4860:4860::8888:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 135ms, Maximum = 159ms, Average = 146ms

C:\Users\MikeandJill>
```

Figure 3-23 After an initial delay, the `ping -6` was successful

Troubleshooting Tools (5 of 12)

- **ipconfig**—Shows current TCP/IP addressing and domain name information on a Windows computer
  - Use ipconfig/all to see a more complete summary of TCP/IP addressing information

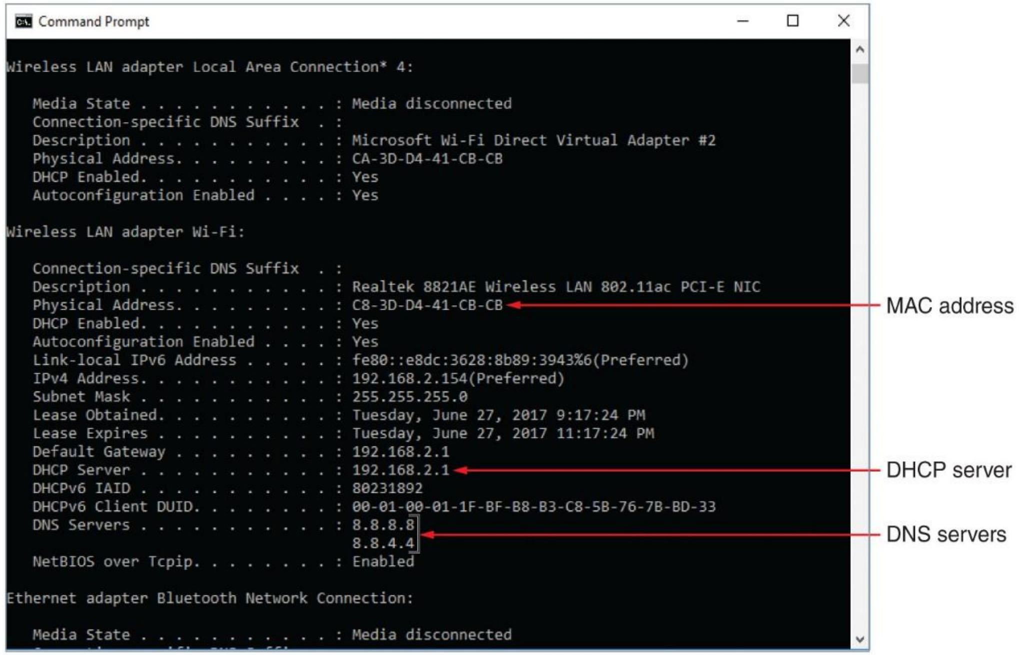


```
C:\Users\Jill West>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3073:b80c:6e0f:d24e%13
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e8dc:3628:8b89:3943%6
   IPv4 Address. . . . . . . . . . . : 192.168.2.154
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Ethernet adapter Bluetooth Network Connection:
```

Figure 3-24 This computer is connected to two different network interfaces, one of which is a virtual network inside VirtualBox

Troubleshooting Tools (6 of 12)

- **ipconfig**—Shows current TCP/IP addressing and domain name information on a Windows computer
    - Use ipconfig/all to see a more complete summary of TCP/IP addressing information



```
Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : CA-3D-D4-41-CB-CB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
   Physical Address. . . . . . . . . : C8-3D-D4-41-CB-CB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e8dc:3628:8b89:3943%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.154(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, June 27, 2017 9:17:24 PM
   Lease Expires . . . . . . . . . . : Tuesday, June 27, 2017 11:17:24 PM
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 80231892
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1F-BF-B8-B3-C8-5B-76-7B-BD-33
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
```

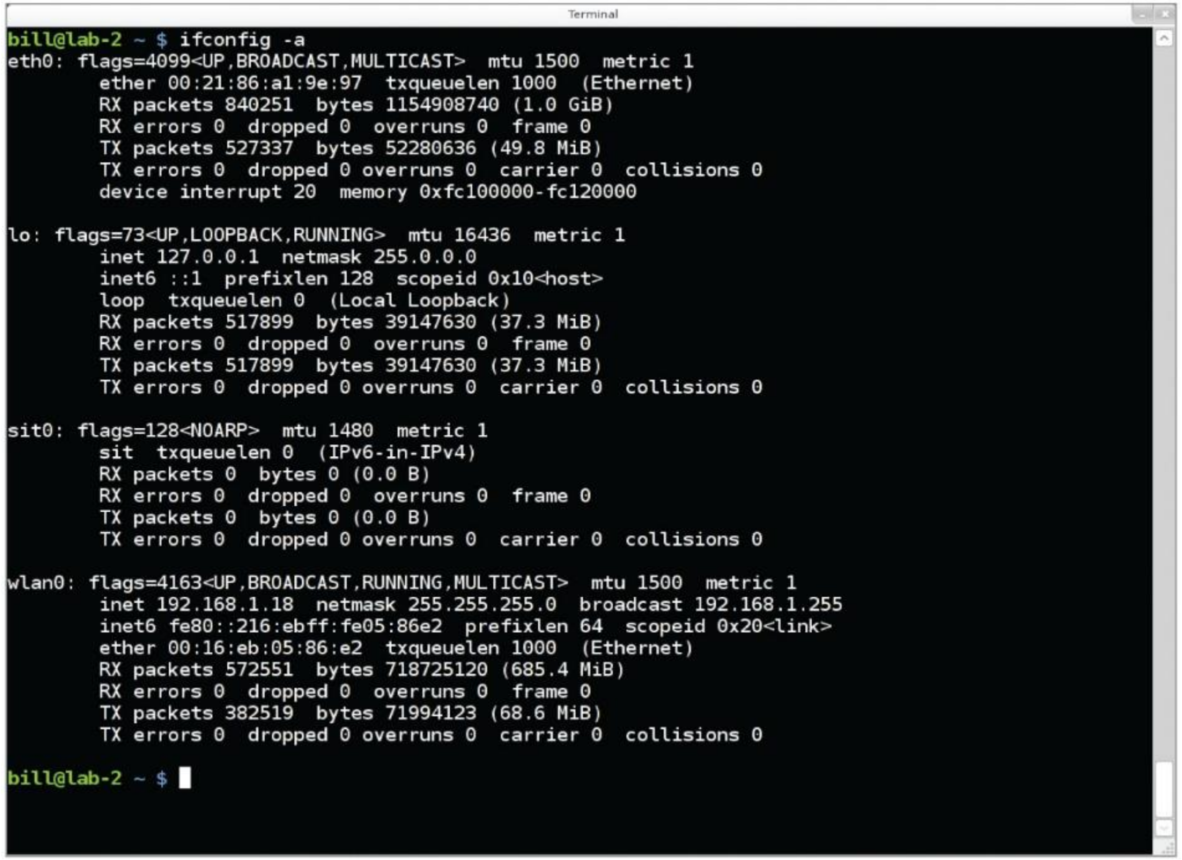
Figure 3-25 `ipconfig /all` gives a great deal more information than `ipconfig` by itself

Troubleshooting Tools (7 of 12)

- **ifconfig**—Utility to view and manage TCP/IP settings
- If your Linux or UNIX system provides a GUI
  - Open a shell prompt, then type **ifconfig**

Ifconfig command	**Description**
ifconfig	Displays basic TCP/IP information and network information, including MAC address of the NIC
Ifconfig -a	Displays TCP/IP information associated with every interface on a Linux device; can be used with other parameters (see Figure 3-26)
Ifconfig down	Marks the interface, or network connection, as unavailable to the network
Ifconfig up	Reinitializes the interface after it has been taken down (via the ifconfig down command), so that it is once again available to the network
man ifconfig	Displays the manual pages, called man pages, for the ifconfig command, which tells you how to use the command and about command parameters (similar to the ipconfig /? command in Windows)

Troubleshooting Tools (8 of 12)



```
bill@lab-2 ~ $ ifconfig -a
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500  metric 1
        ether 00:21:86:a1:9e:97  txqueuelen 1000  (Ethernet)
        RX packets 840251  bytes 1154908740 (1.0 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 527337  bytes 52280636 (49.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xfc100000-fc120000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 16436  metric 1
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 517899  bytes 39147630 (37.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 517899  bytes 39147630 (37.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sit0: flags=128<NOARP>  mtu 1480  metric 1
        sit  txqueuelen 0  (IPv6-in-IPv4)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
        inet 192.168.1.18  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::216:ebff:fe05:86e2  prefixlen 64  scopeid 0x20<link>
        ether 00:16:eb:05:86:e2  txqueuelen 1000  (Ethernet)
        RX packets 572551  bytes 718725120 (685.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 382519  bytes 71994123 (68.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

bill@lab-2 ~ $ 
```

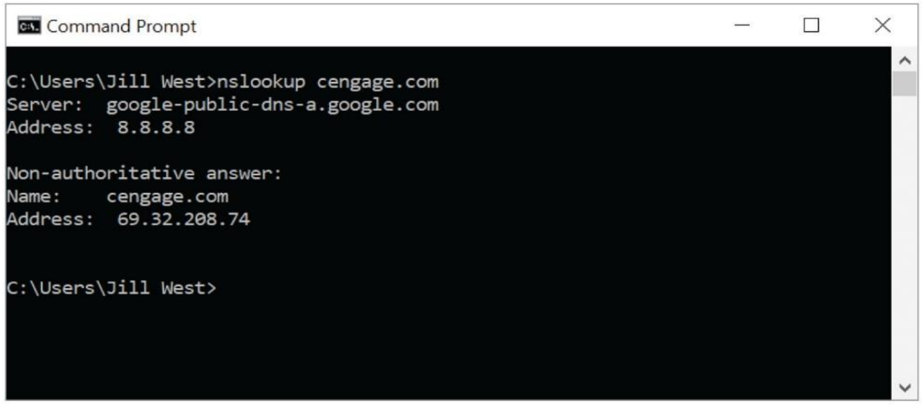
Figure 3-26 Detailed information available through `ifconfig -a`

Source: The Linux Foundation

Troubleshooting Tools (9 of 12)

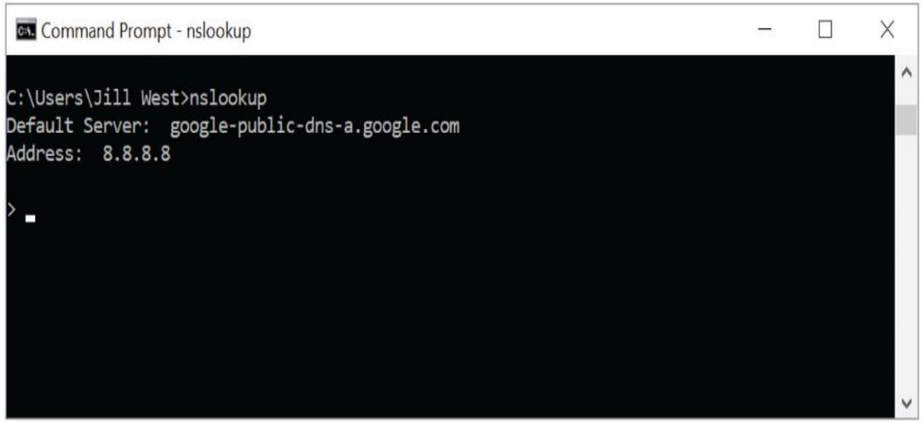
- **nslookup** (name space lookup)—Allows you to query the DNS database from any computer on a network:
  - To find the host name of a device by specifying its IP address, or vice versa
  - Useful for verifying a host is configured correctly or for troubleshooting DNS resolution problems
- Reverse DNS lookup—To find the host name of a device whose IP address you know
  - **nslookup 69.23.208.74**
- Two modes:
  - Interactive—To test multiple DNS servers at one time
  - Noninteractive—Test a single DNS server

Troubleshooting Tools (10 of 12)



```
C:\Users\Jill West>nslookup cengage.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    cengage.com
Address:  69.32.208.74


C:\Users\Jill West>
```

Figure 3-27 `nslookup` **shows DNS server and web host information**

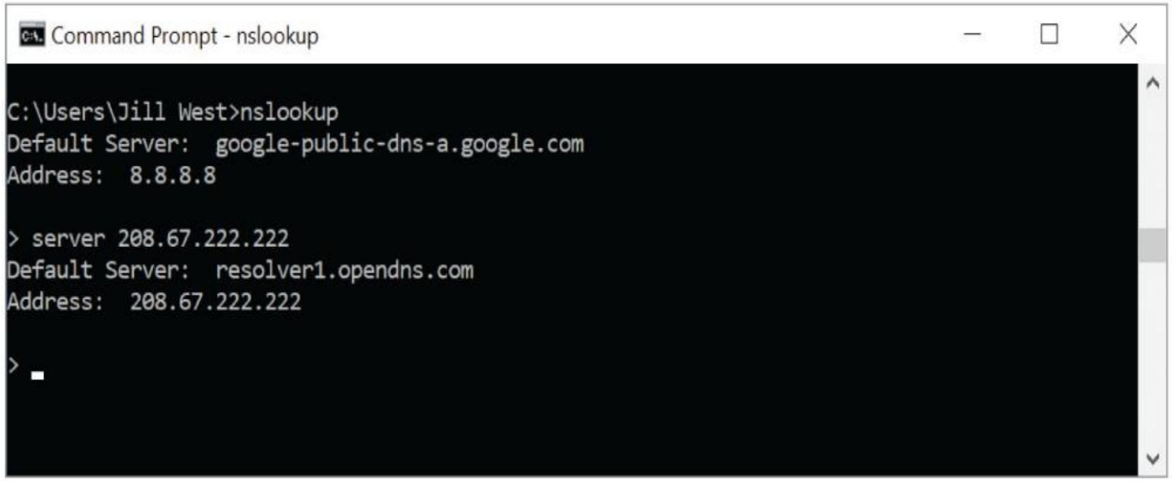


```
C:\Users\Jill West>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

>
```

Figure 3-28 Interactive mode of the nslookup utility

Troubleshooting Tools (11 of 12)

- You can change DNS servers from within interactive mode with the server subcommand and specifying the IP address of the new DNS server
- To exit nslookup’s interactive mode, enter **exit**



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

> server 208.67.222.222
Default Server:  resolver1.opendns.com
Address:  208.67.222.222

> _
```

Figure 3-29 The `server` subcommand can be used to change DNS servers

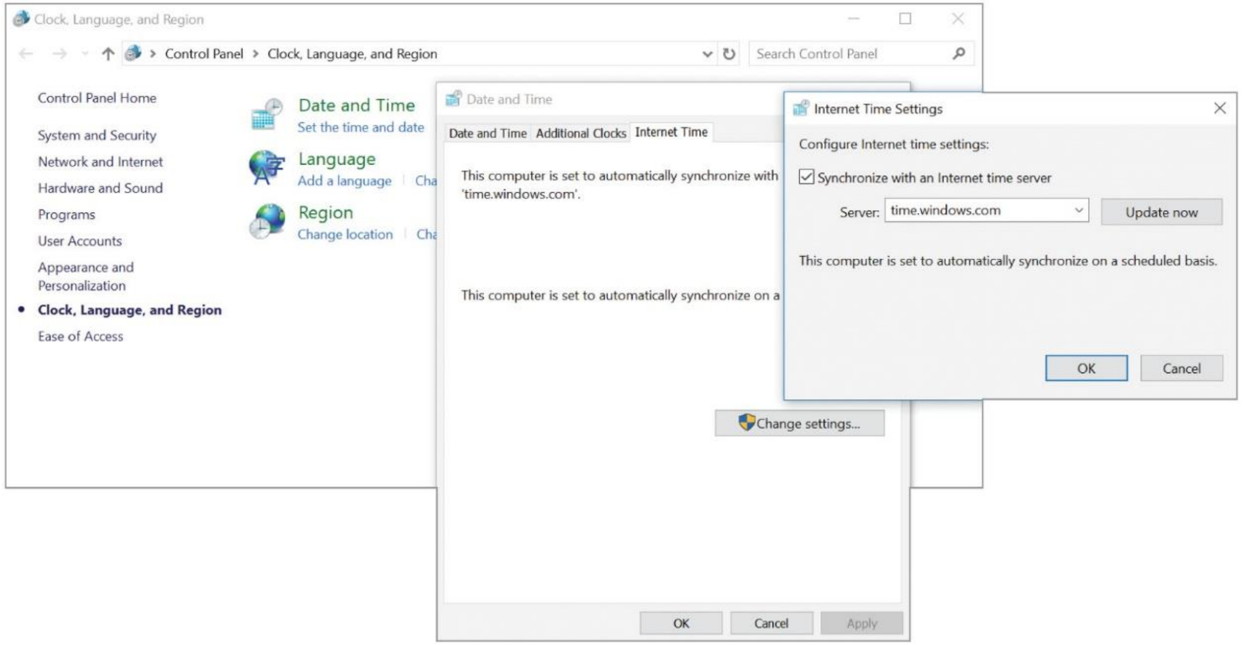
Troubleshooting Tools (12 of 12)

- **dig (domain information groper)**—Available on Linux and macOS
  - Provides more detailed information than nslookup and uses more reliable sources of information to output its results
  - Table 3-10 Sample dig commands

Sample dig commands	Description
dig google.com	Performs a DNS lookup on a domain name
dig @8.8.8.8 google.com	Specifies a name server in the google.com domain
dig @8.8.8.8 google.com MX	Requests a list of all A records in the google.com domain on a specific name server
dig google.com ANY	Requests a list of all record types in the google.com domain
dig –x 74.125.21.102	Performs a reverse lookup on a Google IP address
man dig	Displays the man page for the dig command

Common Network Issues (1 of 3)

- **Incorrect time**
  - Check a domain computer’s time source from a Command Prompt window by entering **w32tm /query /source**



This computer is set to automatically synchronize with 'time.windows.com'.

This computer is set to automatically synchronize on a

Configure Internet time settings:

☑ Synchronize with an Internet time server

Server: time.windows.com

This computer is set to automatically synchronize on a scheduled basis.

Figure 3-30 Change the time server your computer uses to synchronize its system time

Common Network Issues (2 of 3)

- **DHCP issues**:
  - If you are getting DHCP errors or if multiple clients are having trouble connecting to the network
    - Check the settings on your DHCP server
    - Make sure the DHCP scope is large enough to account for the number of clients the network must support
  - Consider implementing a shorter lease time on larger networks

Common Network Issues (3 of 3)

- **Network connection configuration issues**
    - Common configuration errors:
        - Incorrect netmask
        - Incorrect gateway
        - Duplicate IP address
    - When a computer is struggling to establish a network connection
        - Check its TCP/IP configuration settings
    - If the computer is not obtaining an IP address and related information from a DHCP server
        - Static settings might be using the wrong information
        - Try switching to DHCP

Summary

- The IANA is an organization responsible for tracking the assignments of domain names, port numbers, and IP addresses
- MAC addresses contain two parts, are 48 bits long, and are written in hexadecimal numbers separated by colons
- IP addresses identify nodes at the Network layer
- The first part of an IPv4 address identifies the network and the last part identifies the host
- A DHCP scope is a range of addresses to be assigned to clients when they request an IPv4 address
- A gateway device that stands between a private network and other networks substitutes the private IP address with its own public address when computers need access to other networks or the Internet

Summary

- IPv6 standards were developed to improve routing capabilities and speed communication over the established IPv4 standards
- IPv6 addressing is designed so that a computer can autoconfigure its own link local IP address
- A port number is a number, assigned to a process:
  - TCP and UDP ports ensure that data is transmitted to the correct process among multiple process running on the computer
- Name resolution is the process of discovering the IP address of a host when its FQDN is known
- Namespace databases are stored in DNS zone files
- The most popular DNS server software is BIND

Summary

- Troubleshooting utilities and tools:
  - Event Viewer, ping, ipconfig, ifconfig (Linux only), nslookup, and dig (Linux only)
- If your computer is not a member of a domain, you can determine and adjust the time server your computer syncs to when it connects to the Internet
- Make sure the DHCP scope is large enough to account for the number of clients the network must support
- If the computer is not obtaining an IP address and related information from a DHCP server:
  - Static settings might be using the wrong information
  - Try switching to DHCP