IPv6 Addresses (1 of 2)

- An IPv6 address has 128 bits written as eight blocks of hexadecimal numbers separated by colons
    - Ex: 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 (this is the preferred method because it contains the fewest zeroes)

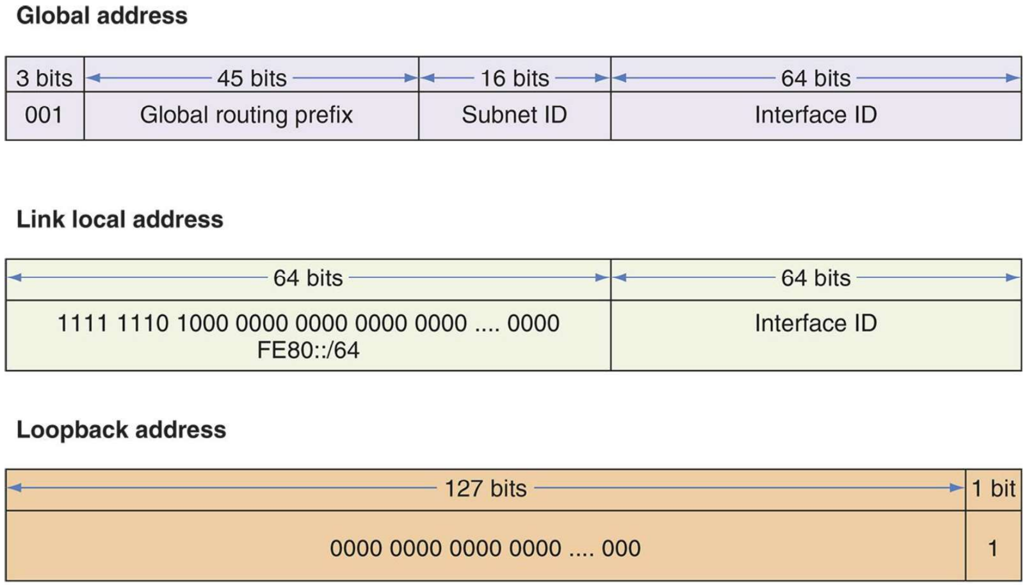
IPv6 Addresses (2 of 2)

- IPv6 terminology:
  - A **link** (sometimes called local link) is any LAN bounded by routers
  - **Neighbors** are two or more nodes on the same link
  - **Dual stacked** is when a network is configured to use both IPv4 and IPv6
  - **Tunneling** is a method used by IPv6 to transport IPv6 packets through or over an IPv4 network
  - **Interface ID** is the last 64 bits or four blocks of an IPv6 address that identify the interface

Types of IPv6 Addresses (1 of 4)

- **Unicast address** - specifies a single node on a network
  - **Global address** can be routed on the Internet
  - **Link local address** can be used for communicating with nodes in the same link
  - **Loopback address** can be used to test that an interface and supporting protocol stack are functioning properly
- **Multicast address –** delivers packets to all nodes on a network
- **Anycast address** - can identify multiple destinations, with packets delivered to the closest destination

Types of IPv6 Addresses (2 of 4)



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

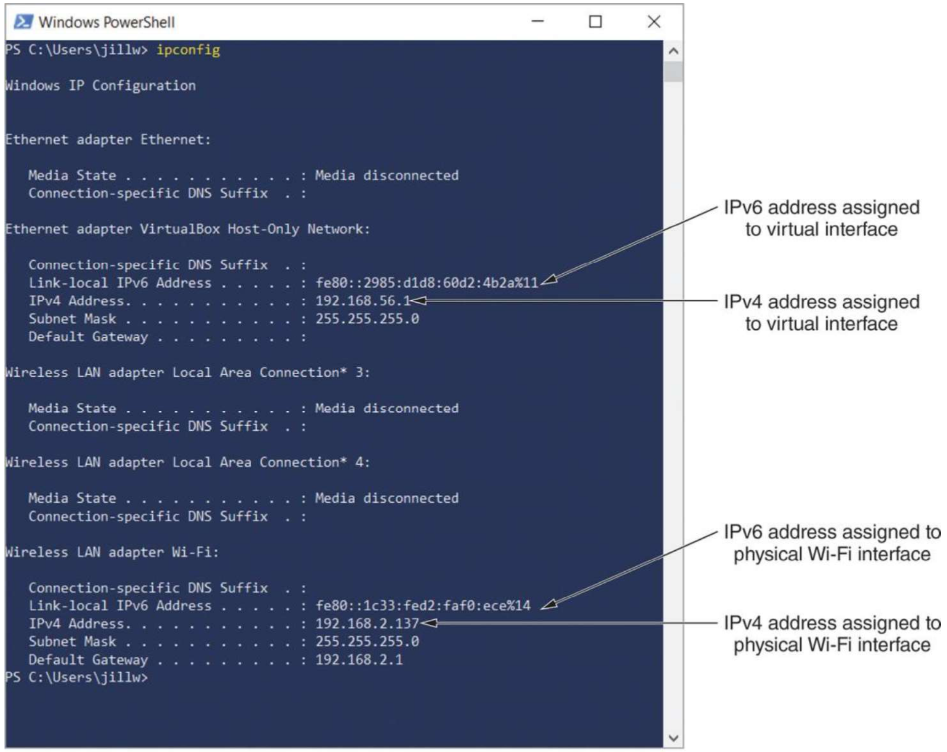
Loopback address

127 bits	1 bit
0000 0000 0000 0000 000	1

Figure 3-16 Three types of IPv6 addresses

Figure 3-16 Three types of IPv6 addresses

Types of IPv6 Addresses (3 of 4)



```
PS C:\Users\jillw> 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::2985:d1d8:60d2:4b2a%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 3:

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

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::1c33:fed2:faf0:ece%14
   IPv4 Address. . . . . . . . . . . : 192.168.2.137
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
PS C:\Users\jillw>
```

IPv6 address assigned to virtual interface

IPv4 address assigned to virtual interface

IPv6 address assigned to physical Wi-Fi interface

IPv4 address assigned to physical Wi-Fi interface

Figure 3-18 The `ipconfig` command shows IPv4 and IPv6 addresses assigned to this computer

Figure 3-18 The `ipconfig` command shows IPv4 and IPv6 addresses assigned to this computer

Types of IPv6 Addresses (4 of 4)

- IPv6 autoconfiguration
  - IPv6 addressing is designed so that a computer can autoconfigure its own link local IP address
  - This process is called **SLAAC (stateless address autoconfiguration)**
- Step 1 - The computer creates its IPv6 address
  - It uses FE80::/64 as the first 64 bits (called prefix)
  - The last 64 bits are generated from the network adapter's MAC address
- Step 2 - The computer checks to make sure its IP address is unique on the network
- Step 3 - The computer asks if a router on the network can provide configuration information
  - This message is called an **RS (router solicitation)** message

CENGAGE

Knowledge Check Activity 3-1

Which of the following IPv4 addresses is a public IP address?

a. 10.0.2.14

b. 172.16.156.254

c. 192.168.72.73

d. 64.233.177.189

Knowledge Check Activity 3-1: Answer

Which of the following IPv4 addresses is a public IP address?

Answer: d. 64.233.177.189

IP addresses within the ranges of 10.0.0.0 through 10.255.255.255, 172.16.0.0 through 172.31.255.255, and 192.168.0.0 through 192.168.255.255 are RFC1918, or private, IP addresses. The address 64.233.177.189 is a public IP address.

Ports and Sockets (1 of 2)

- A port is a number assigned to a process that can receive data
  - Port numbers ensure data is transmitted to the correct process among multiple processes running on a single device
- A socket consists of host’s IP address and the port number of an application running on the host
  - A 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

CENGAGE

Ports and Sockets (2 of 2)

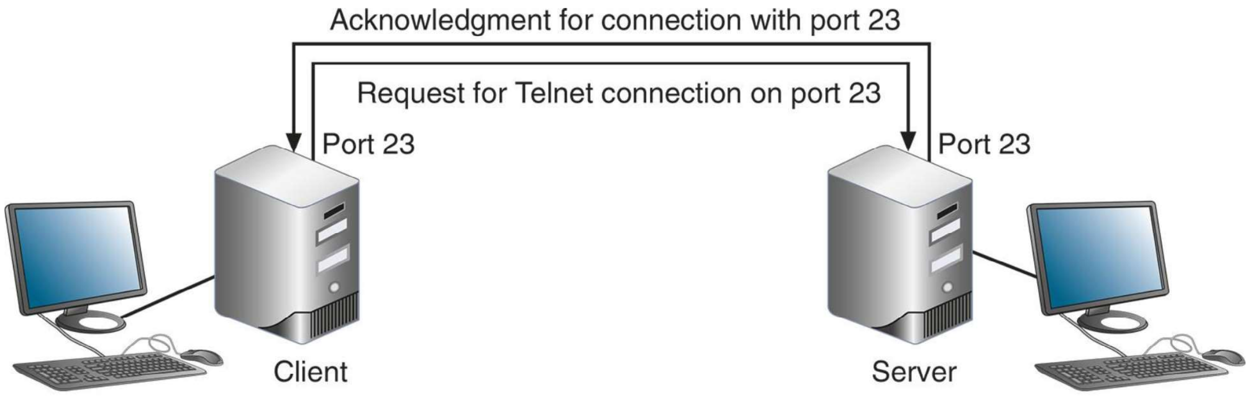

Acknowledgment for connection with port 23
Request for Telnet connection on port 23
Port 23
Port 23
Client
Server

Figure 3-19 A virtual connection for the Telnet service

Figure 3-19 A virtual connection for the Telnet service

Domain Names and DNS (1 of 2)

- Character-based names are easier to remember than numeric IP addresses
- A **URL (uniform resource locator)** is an addressing scheme that identifies where to find a particular resource on a network
- 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 2)

- 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
  - An **authoritative name 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**

CENGAGE

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 DNS server types can co-exist on the same machine
- DNS name servers are organized in a hierarchical structure
- At the root level, 13 clusters of **root DNS servers** hold information used to locate top-level domain (TLD) servers

Name Servers (2 of 4)

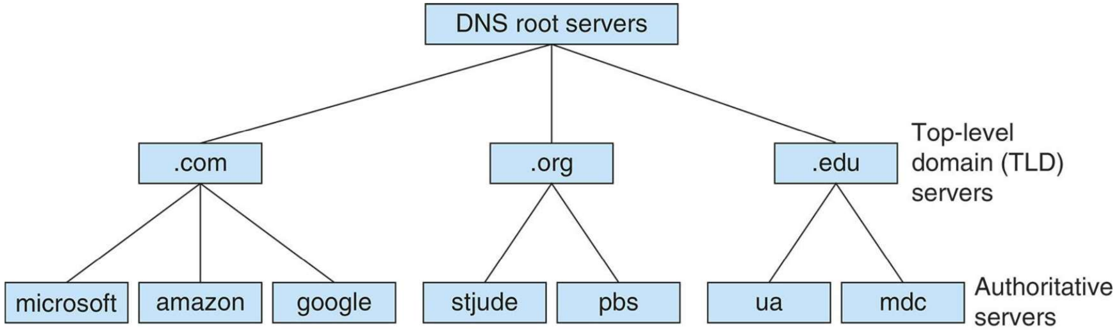


Figure 3-21 Hierarchy of name servers

Figure 3-21 Hierarchy of name servers

Name Servers (3 of 4)

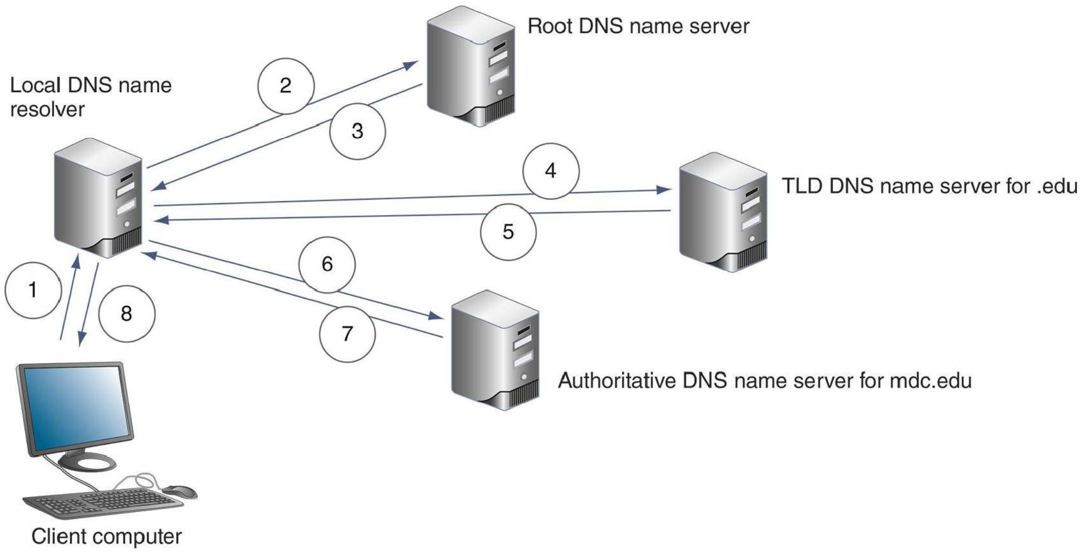

Root DNS name server
Local DNS name resolver
TLD DNS name server for .edu
Authoritative DNS name server for mdc.edu
Client computer
1
2
3
4
5
6
7
8

Figure 3-22 Queries for name resolution of *www.mdc.edu*

Figure 3-22 Queries for name resolution of *www.mdc.edu*

Name Servers (4 of 4)

- Ways the resolution process can get more complex:
  - A caching server typically is not the same machine as the authoritative server
    - The 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 lookup –** a query that demands a resolution or the answer “It can’t be found”
  - **Iterative lookup –** 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

CENGAGE

Resource Records in a DNS Database

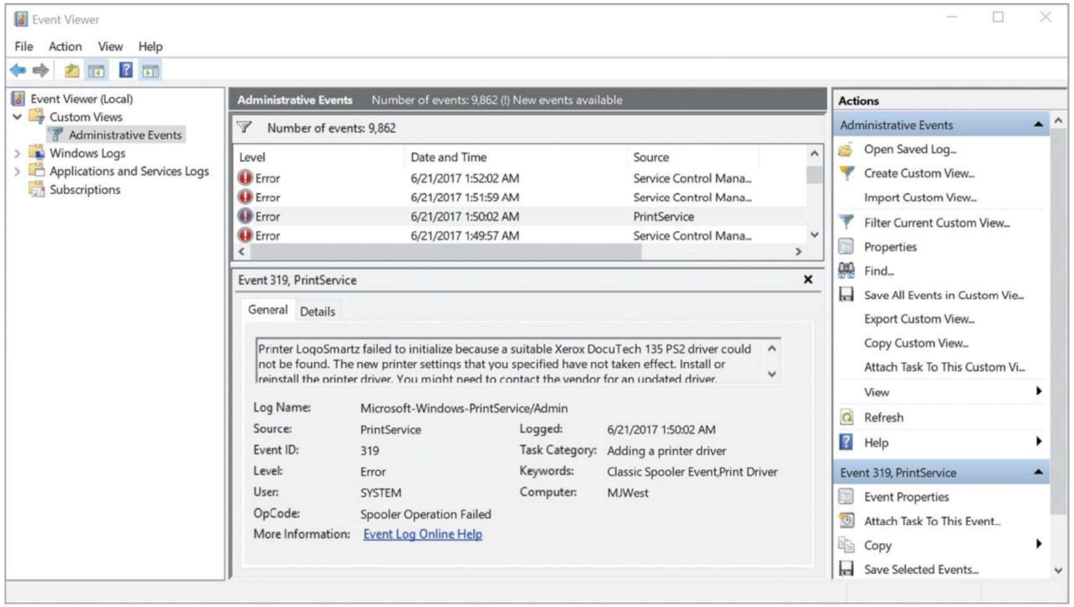
- Several types of records, called resource records are kept in a DNS database:
  - **SOA (start of authority) record** – gives information about the zone
  - **A (address) record** – stores the name-to-address mapping for a host
  - **AAAA (address) record** – holds the name-to-address mapping, the IP address is an IPv6 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

- BIND (Berkeley Internet Name Domain) is the most popular DNS server software
  - Open source - the term for software whose code is publicly available for use and modification
- Microsoft DNS Server is a built-in DNS service in the Windows Server OS
- Windows Server is capable of split-brain or split-horizon deployment, which is used to handle internal clients and external clients

CENGAGE

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 3-24 Event Viewer provided the diagnosis of a printer problem and recommended steps to fix the problem

Figure 3-24 Event Viewer provided the diagnosis of a printer problem and recommended steps to fix the problem

Troubleshooting Tools (1 of 8)

- Command-line tools are a great resource to troubleshoot network problems
- **ping (Packet Internet Groper)** utility is 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)
  - The other computer responds in the form of an echo reply
- **ICMP (Internet Control Message Protocol)** is the protocol used by the echo request/reply to carry error messages and information about the network

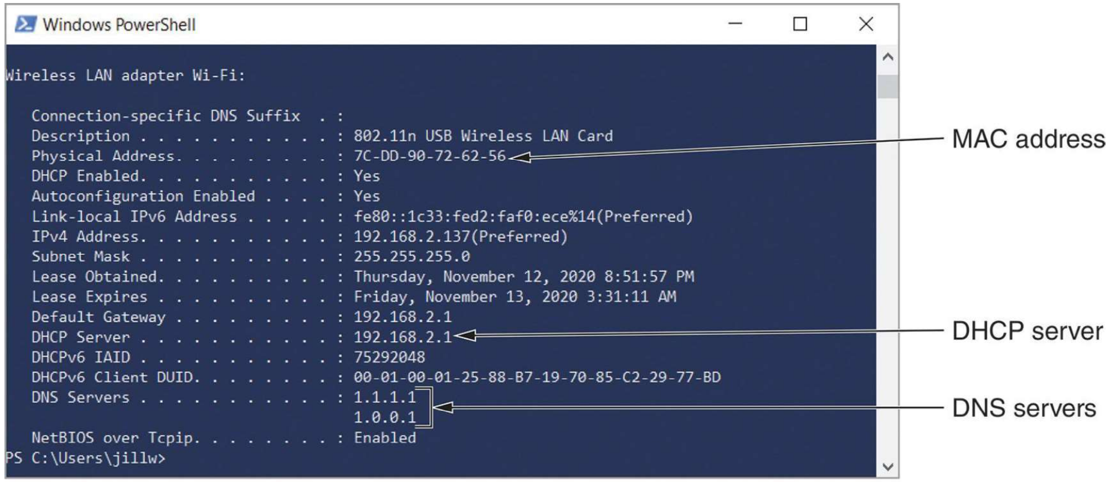
Troubleshooting Tools (2 of 8)

- 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 (3 of 8)

- The **`ipconfig`** command 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

Troubleshooting Tools (4 of 8)



Windows PowerShell

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 802.11n USB Wireless LAN Card
   Physical Address. . . . . . . . . : 7C-DD-90-72-62-56
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1c33:fed2:faf0:ece%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.137(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, November 12, 2020 8:51:57 PM
   Lease Expires . . . . . . . . . . : Friday, November 13, 2020 3:31:11 AM
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 75292048
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-88-B7-19-70-85-C2-29-77-BD
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       1.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\jillw>
```

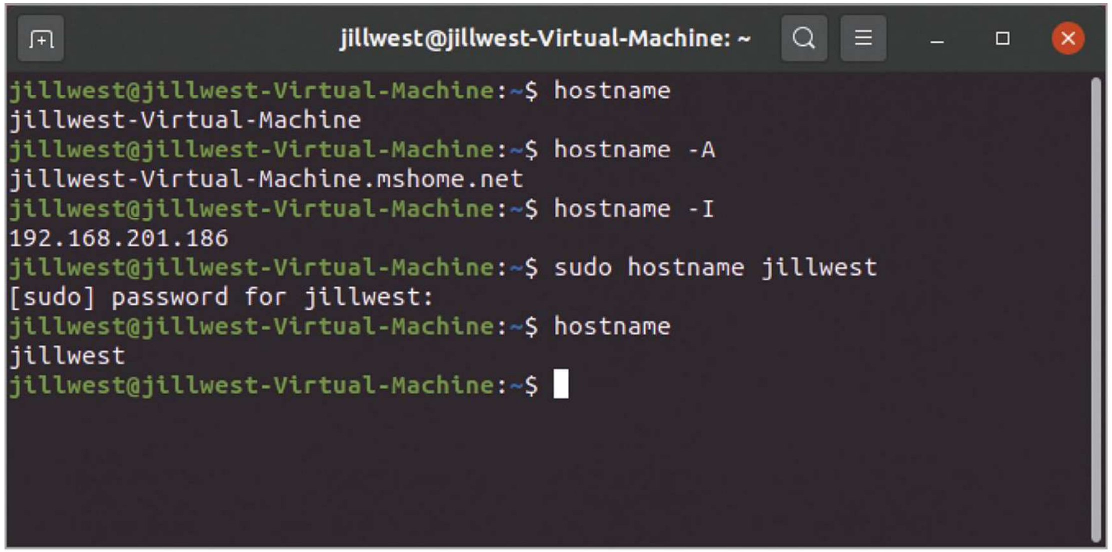
Figure 3-29 `ipconfig /all` gives more information than `ipconfig` by itself

Figure 3-29 `ipconfig /all` gives more information than ipconfig by itself

Troubleshooting Tools (5 of 8)

- Use the `ip` utility to view and manage TCP/IP settings
- The `ip` utility is only available on UNIX and Linux systems
- Any `ip` commands that change the state of a link require elevated privileges
  - This is accomplished by logging in as the root user or by temporarily elevating the current user's privileges with the `sudo` (superuser do) command
- `ifconfig` is a similar utility used to view and manage TCP/IP settings
- If your Linux or UNIX system provides a GUI
  - Open a shell prompt, then type `ifconfig`

Troubleshooting Tools (6 of 8)



```
jillwest@jillwest-Virtual-Machine:~$ hostname
jillwest-Virtual-Machine
jillwest@jillwest-Virtual-Machine:~$ hostname -A
jillwest-Virtual-Machine.mshome.net
jillwest@jillwest-Virtual-Machine:~$ hostname -I
192.168.201.186
jillwest@jillwest-Virtual-Machine:~$ sudo hostname jillwest
[sudo] password for jillwest:
jillwest@jillwest-Virtual-Machine:~$ hostname
jillwest
jillwest@jillwest-Virtual-Machine:~$
```

Source: The Linux Foundation

Figure 3-32 Use `hostname` to view or change a device's host name

Figure 3-32 Use `hostname` to view or change a device's host name

Troubleshooting Tools (7 of 8)

- The `nslookup` (name space lookup) utility 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
  - It is 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`
- The nslookup utility is available in two modes:
  - Interactive - to test multiple DNS servers at one time
  - Noninteractive - test a single DNS server
- 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`

Troubleshooting Tools (8 of 8)

- The **dig (domain information groper)** utility is available on Linux and macOS
  - Provides more detailed information than nslookup and uses more reliable sources of information to output its results
- Use dig to query DNS nameservers for information about host addresses and other DNS records
- An **IP scanner** can be used to gather information about all devices connected to a network

Common Network Issues (1 of 2)

- Incorrect time
  - Check a domain computer’s time source from a Command Prompt window by entering `w32tm /query /source`
- DHCP Issues
  - If you are getting DHCP errors or if multiple clients are having trouble connecting to the network, try the following:
    - 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 (2 of 2)

- Network Connection Configuration Issues
  - Common configuration errors:
    - Incorrect IP address
    - Duplicate IP address
    - Incorrect subnet mask
    - Incorrect gateway
    - Incorrect DNS or DNS issues
  - 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

Knowledge Check Activity 3-2

What protocol does ping use?

a. HTTP

b. ICMP

c. DHCP

d. FTP

Knowledge Check Activity 3-2: Answer

What protocol does ping use?

Answer: b. ICMP

The protocol used by the ping echo request and echo reply is ICMP (Internet Control Message Protocol), a lightweight protocol used to carry error messages and information about a network.

Summary

Now that the lesson has ended, you should be able to:

- Work with MAC addresses
- Configure TCP/IP settings on a computer, including IP address, subnet mask, default gateway, and DNS servers
- Identify the ports of several common network protocols
- Describe domain names and the name resolution process
- Use command-line tools to troubleshoot common network problems