MCSE MCSA MCSA Guide to Networking with Windows Server 2016 Exam 70-741 1st edition Tomsho Solutions Manual

SKU: 9781337400787-SOLUTIONS

Chapter 1 Solutions

Review Questions

1. Which of the following is needed if a computer with the IP address 172.31.210.10/24 wants to communicate with a computer with the IP address 172.31.209.122/24?
   a. Hub
   b. Router
   c. Switch
   d. Server

References: IP Operation

2. You have just typed the commands `ipconfig /flushdns` and `ping server1`. Which of the following protocols is used first as a result of these commands?
   a. TCP
   b. DNS
   c. ICMP
   d. DHCP

References: TCP/IP Components

3. Which command should you use with a dual-homed server to make sure the server sends packets out to the correct interface?
   a. `ipconfig`
   b. `ping`
   c. `tracert`
   d. `route`

References: Configuring the Default Gateway

4. Which command should you use to determine whether there's a bottleneck between your computer and a computer on another network?
   a. `ipconfig`
   b. `ping`
   c. `tracert`
   d. `route`

References: IP Configuration Command-Line Tools

5. Which command should you use to configure the primary DNS server on your computer?
   a. `ipconfig`
   b. `netsh`
   c. `nslookup`
   d. `arp`

References: IP Configuration Command-Line Tools

6. Which IP address expressed in CIDR notation has the subnet mask 255.255.255.0?

   a. 10.100.44.123/24

   b. 172.16.88.222/16

   c. 192.168.100.1/26

   d. 172.29.111.201/18

References: Classless Interdomain Routing

7. Which IP network address expressed in CIDR notation can support a maximum of 1022 hosts?

   a. 10.100.44.0/24

   b. 172.16.4.0/22

   c. 192.168.100.64/26

   d. 172.29.128.0/18

References: Classless Interdomain Routing

8. You have just finished a default installation of Windows Server 2016. You know that TCP/IP is installed. How does your new server receive an assigned an IP address?

   a. TCP

   b. DNS

   c. ARP

   d. DHCP

References: TCP/IP Components

9. Your DNS server is on the same network as the computer where you enter the following commands:

```
arp -d
ipconfig /flushdns
nslookup server1
```

   Which of the following protocols is used first as a result of these commands?

   a. TCP

   b. DNS

   c. ARP

   d. DHCP

References: IP Configuration Command-Line Tools

10. Which of the following IP addresses will be delivered to all the computers on the local network?

    a. 10.255.150.255/8

    b. 10.1.254.255/16

    c. 10.1.240.255/24

    d. 175.16.1.1/16

References: Classless Interdomain Routing

11. Which of the following is a good reason to subnet an IPv4 network? (Choose all that apply.)

    a. Eliminate the need for ARP requests.

b. Decrease the size of the broadcast domain.

c. Allow broadcasts to reach more computers.

d. Conserve IP addresses.

References: Subnetting

12. Which of the following IP addresses has 12 bits in the host ID?

a. 172.31.21.12/16

b. 172.31.89.100/12

c. 12.49.127.88/8

d. 12.156.109.252/20

References: Subnetting

13. You have set up an e-mail server that needs to respond to e-mail requests by~~by~~ using mail.coolgadgets.com and mail.niftytools.com in the request URL. How can you do this?

a. Install two NICs, and assign the same IP address to both NICs. Configure DNS to map one MAC address to mail.coolgadgets.com and the other MAC address to mail.niftytools.com.

b. Configure two IP addresses on one NIC. Configure DNS to map one IP address to mail.coolgadgets.com and the other IP address to mail.niftytools.com.

c. Install two NICs, and connect each one to a different network. Set up the router on each network to forward mail packets to the NIC bound to the correct URL.

d. Install two NICs, and assign different IP addresses to each NIC, but make sure both IP addresses use the same network ID. Configure the NICs to use default gateways on different networks.

References: Configuring Multiple IP Addresses

14. You have a server with two NICs, each attached to a different IP network. You're having problems communicating with devices on remote networks that send packets to one of the interfaces. The server receives the packets fine, but the server's replies never reach the intended destination network. Replies to packets that come in through the other interface seem to reach their destination without any problems. What can you do that will most likely solve the problem?

a. Configure a second default gateway on the interface exhibiting problems.

b. Change the default gateway to use the router that's on the network of the interface exhibiting problems.

c. Use the `route` command to add routes to the networks that aren't receiving replies.

d. Replace the NIC that's having problems replying to packets.

References: Configuring the Default Gateway

15. You have just changed the IP address on a computer named computer5 in your domain from 172.31.1.10/24 to 172.31.1.110/24. You were communicating with this computer from your workstation with no problems~~fine~~ right before you changed the address. Now when you try the command `ping computer5` from your workstation, you don't get a successful reply. Other computers on the network aren't having a problem communicating with the computer. Which command might help solve the problem?

a. `arp -d`

b. `ipconfig /flushdns`

c. `tracert computer5`

d. `ping -6 172.31.1.110`

References: IP Configuration Command-Line Tools

16. Which command can cause an address of 0.0.0.0 to be assigned to a host?

a. `nslookup 0.0.0.0`

b. `netsh set IPv4 address=Null`

c. `Set-NetIPInterface -InterfaceAlias Ethernet -DHCP enabled`

d. `ipconfig /release`

References: IP Configuration Command-Line Tools

17. Which IP address can't be assigned to a host computer?

a. 10.100.44.16/24

b. 172.16.7.255/22

c. 192.168.100.66/26

d. 172.29.132.0/18

References: Configuring IPv4 Addresses

18. Which of the following is a benefit of using IPv6 rather than IPv4? (Choose all that apply.)

a. You can assign four times the number of addresses in IPv6.

b. **Subnetting to conserve IP addresses is less of a concern.**

c. **Features to improve communication security and quality are built into IPv6.**

d. IPv6 addresses are expressed as 16 8-bit numbers separated by colons, which are easier to read than dotted decimal notation.

References: IPv6 Overview

19. Which of the following is a valid IPv6 address? (Choose all that apply.)

a. `fe80:0:0:FEED::1`

b. `2001:DB8:00AB:11:3344`

c. `fe80:DB8::EE::8901`

d. `2001:DB8:BAD:F00D:0020:3344:0:e4`

References: IPv6 Address Structure

20. Which IPv6 transition technology can be used with NAT routers and has the address prefix `2001::/32`?

a. Teredo

b. ISATAP

c. 6to4

d. IPv6-over-IPv4

References: Teredo Tunneling

21. Which IPv6 transition technology requires the `netsh` command to manually create the tunnel to carry IPv6 traffic over the IPv4 Internet?

a. Teredo

b. ISATAP

c. IPv6-over-IPv4

d. 6to4

References: IPv6-over-IPv4 Tunneling

22. Which of the following IPv6 transition technologies is enabled by default in Windows Server 2016 and embeds an IPv4 address in a link-local IPv6 address?

a. Teredo

b. ISATAP

c. IPv6-over-IPv4

d. 6to4

References: Intra-Site Automatic Tunnel Addressing Protocol

23. How many bits are in the interface ID of an IPv6 address?

a. 32

b. 64

c. 16

d. 48

References: IPv6 Address Structure

24. What type of IPv6 address should you use when you have multiple routers on a subnet and want hosts to use the nearest router for packets that should be delivered to remote networks?

a. Multicast

b. Broadcast

c. Anycast

d. Unicast

References: Anycast Addresses

25. What address should you ping if you want to test local IPv6 operation but don't want to actually send any packets on the network?

a. `1::f`

b. `2001::db8`

c. `fe80::ffff`

d. `::1`

References: IPv6 Unicast Addresses

26. Which of the following IPv6 autoconfiguration methods utilizes an autoconfiguration protocol, such as DHCPv6, to acquire an IPv6 address?

a. Static IPv6 configuration

b. Stateful autoconfiguration

c. Prefixed IPv6 autoconfiguration

d. Stateless autoconfiguration

References: IPv6 Autoconfiguration

Activities

Activity 1-1: Converting Decimal Numbers to Binary

Decimal number	Binary number
167	**10100111**
149	**10010101**
252	**11111100**
128	**10000000**
64	**01000000**
240	**11110000**
255	**11111111**
14	**00001110**
15	**00001111**
63	**00111111**
188	**10111100**
224	**11100000**

Activity 1-2: Converting Binary Numbers to Decimal

Binary number	Decimal number
00110101	**53**
11111000	**248**
00011111	**31**
10101010	**170**
01010101	**85**
11111110	**254**
11111100	**252**
00111011	**59**
11001100	**204**
00110011	**51**
00000111	**7**
00111100	**60**

Activity 1-3: Working with CIDR Notation

Network/prefix	Subnet mask	Host bits	Number of hosts
172.16.1.0/24	**255.255.255.0**	**8**	**254**
10.1.100.128/26	**255.255.255.192**	**6**	**62**

10.1.96.0/19	**255.255.224**	**13**	**8190**
192.168.1.0/24	**255.255.255.0**	**8**	**254**
172.31.0.0/16	**255.255.0.0**	**16**	**65534**
10.255.255.252/30	**255.255.255.252**	**2**	**2**
172.28.240.0/20	**255.255.240.0**	**12**	**4094**
10.44.108.0/22	**255.255.252.0**	**10**	**1022**
192.168.100.24/21	**255.255.248.0**	**11**	**2046**
172.23.64.0/18	**255.255.192.0**	**14**	**16382**
192.168.5.128/25	**255.255.255.128**	**7**	**126**

Activity 1-4: Determining the Correct Prefix

Network ID	Required hosts	Host bits needed	Network ID/prefix
172.16.1.0	254	**8**	**172.16.1.0/24**
10.1.100.128	62	**6**	**10.1.100.128/26**
10.1.96.0	8190	**13**	**10.1.96.0/19**
192.168.1.0	200	**8**	**192.168.1.0/24**
172.31.0.0	65000	**16**	**172.31.0.0/16**
10.255.255.252	2	**2**	**10.255.255.252/30**
172.28.240.0	4000	**12**	**172.28.240.0/20**
10.44.108.0	900	**10**	**10.44.108.0/22**
192.168.240.0	2200	**12**	**192.168.240.0/20**
172.23.64.0	16000	**14**	**172.23.64.0/18**
192.168.5.128	110	**7**	**192.168.5.128/25**

Critical Thinking

Case Project 1-1: Creating a List of MAC Addresses

There are a few possibilities. The manual method is using `ipconfig /all` at each computer to display the necessary information and writing it down. A more automated method is having each computer run a startup script containing `ipconfig /all > \\server\Share\%computername%.txt`, which creates a text file with the required information on a share on the server. The information then has to be extracted from each file. (The script could also use the command `ipconfig /all >>\\serverXX\Share\IPconfigs.txt`, which has the advantage of sending output to a single file because >> appends output to a file.)

Another possibility is pinging all the IP addresses in the range of IP addresses you're using. Using the `-a` option, you can get the computer name, and then use ARP to display the MAC address. However, this method has the drawback of being labor intensive, and the computers would have to be on at the time you pinged them.

Case Project 1-2: Calculating a Subnet Mask

Subnet mask: 255.255.255.240

First four subnets: 198.60.123.0/28, 198.60.123.16/28, 198.60.123.32/28, 198.60.123.48/28

Subnet Mask: 255.255.255.240	
Subnetwork	**Range of host addresses**
198.60.123.0/28	**198.60.123.1 - 14**
198.60.123.16/28	**198.60.123.17 - 30**
198.60.123.32/28	**198.60.123.33 - 46**
198.60.123.48/28	**198.60.123.49 - 62**
198.60.123.64/28	**198.60.123.65 - 78**
198.60.123.80/28	**198.60.123.81 - 94**
198.60.123.96/28	**198.60.123.97 - 110**
198.60.123.112/28	**198.60.123.113 - 126**
198.60.123.128/28	**198.60.123.129 - 142**
198.60.123.144/28	**198.60.123.145 - 158**
198.60.123.160/28	**198.60.123.161 - 174**
198.60.123.176/28	**198.60.123.177 -190**
198.60.123.192/28	**198.60.123.193 - 206**
198.60.123.208/28	**198.60.123.209 - 222**
198.60.123.224/28	**198.60.123.225 - 238**
198.60.123.240/28	**198.60.123.241 - 254**

Case Project 1-3: Using IPv6 Subnetting

Answers will vary. In this sample answer, each location has the first 56 bits assigned. Students create up to 256 subnets because they have 8 bits they can use to create subnets. For example, Location 1 can have subnets `2001:DB8:FAB:0100`, `2001:DB8:FAB:0101`, `2001:DB8:FAB:0102`, and so forth, up to `2001:DB8:FAB:01FF`.

Location 1: `2001:DB8:FAB:0100/56`

Location 2: `2001:DB8:FAB:0200/56`

Location 3: `2001:DB8:FAB:0300/56`

Location 4: `2001:DB8:FAB:0400/56`

Location 5: `2001:DB8:FAB:0500/56`

Location 6: `2001:DB8:FAB:0600/56`

Chapter 1

Configuring TCP/IP

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms

Lecture Notes

Overview

This chapter explains some of the components of the TCP/IP protocol suite. Your students will learn how to subnet, IPv4 addresses and how to configure IPv4 addresses on Windows computers with both GUI and command-line tools. They will also be introduced to IPv6 and will learn about the structure of IPv6 addresses as well as a variety of methods for configuring IPv6 addresses on host computers. Your students will also discover ways to transition from an IPv4 network to an IPv6 network.

Chapter Objectives

After reading this chapter and completing the exercises, the student will be able to:

- Describe the TCP/IP protocol and its components
- Define IPv4 addressing and calculate subnet masks
- Configure IPv4 addresses
- Describe IPv6
- Define IPv6 address types
- Autoconfigure IPv6 addresses
- Transition from IPv4 to IPv6

Teaching Tips

An Overview of TCP/IP

1. Introduce the TCP/IP protocol.

2. Describe the two TCP/IP protocol versions included with Windows Server 2016:
   a. TCP/IPv4
   b. TCP/IPv6

3. Mention that the differences between TCP/IPv4 and TCP/IPv6 are limited to the IP part of the protocol.

4. Explain the TCP/IP is a suite of protocols and discuss the many tasks a suite of protocols can handle.

TCP/IP Components

1. Describe the protocols that are usually installed with TCP/IP:
   a. Domain Name System (DNS)
   b. Dynamic Host Configuration Protocol (DHCP)
   c. Transmission Control Protocol (TCP

d. User Datagram Protocol (UDP)
e. Internet Protocol version 4 (IPv4)
f. Internet Protocol version 6 (IPv6)
g. Address Resolution Protocol (ARP)
h. Internet Control Message Protocol (ICMP)
i. Internet Control Message Protocol version 6 (ICMPv6)

TCP/IP Communication

1. Discuss communication between two computers using TCP/IP.

2. Explain how a client determines whether it is on the same network or a different network as the Web server.

3. Review general network terms:
   a. MAC address
   b. Frame
   c. Packet
   d. Segment

4. Provide an overview of the roles of TCP and UDP:
   a. Explain that the TCP or UDP header provides information to determine which application received data should be sent to.
   b. Explain to students that the transport layer works with units of data called segments. These segments are then passed down to an internetwork layer protocol, such as IP.
   c. Describe how port numbers identify application destinations for TCP and UDP protocols, and how these port numbers can be used to identify what services might be running on a computer. For example, the HTTP protocol used by Web servers is assigned port 80. Refer students to commonly used port numbers presented in Table 1-2.

Teaching Tip	Students can learn more How TCP/IP Works by visiting: http://technet.microsoft.com/en-us/library/cc786128%28v=WS.10%29.aspx

IP Operation

1. Discuss the three main functions of Internet Protocol (IP):
   a. Logical addressing:
      i. Explain the purpose of a logical address and how it is used to identify both a computer/device and the network the device belongs to.

ii. Discuss the difference between a source IP address and a destination IP address. Also point out what the term "unicast address" refers to.

b. Efficient packet delivery: Use the mail delivery analogy to discuss the responsibility of IP in efficient delivery of packets.

c. Packet routing: Describe to students the process by which IP is responsible for routing packets from network to network until they reach their destination.

IPv4 Addresses

1. Describe an IP address.

2. Define an octet.

3. Describe a network ID and explain how it is used.

4. Define a subnet mask and explain how it is used.

5. Explain how IP addresses are formatted and how the network address for a given IP address is determined.

Binary Math

1. Explain to students how computers use a logical AND operation between two binary values.

2. Review with your students how the decimal system works.

3. Compare how the binary system works versus the decimal system.

4. Converting Decimal to Binary: Use Table 1-3 to show students how to convert a decimal number to a binary number. Explain the sequence of steps necessary to complete the calculation.

5. Converting Binary to Decimal: Use Table 1-4 to show students how to convert a binary number to a decimal number.

IP Address Classes

1. Show students the different classes of IP addresses, and describe how to determine what class an IP address is. Reference Table 1-5.
   a. Class A: 1 – 127
   b. Class B: 128 – 191
   c. Class C: 192 – 223
   d. Class D: 224 – 239
   e. Class E: 240 – 255

2. Explain the use of the entire 127.0.0.0 A class network for loopback purposes.

Private IP Addresses

1. Explain the need for private IP addresses, and discuss how IPv4's addressing limitations have affected the use of private IP addressing.

2. Define and describe Automatic Private IP addressing (APIPA). Point out that computers that are assigned a link-local address can communicate only on the local LAN.

Network Address Translation

1. Explain how Network Address Translation allows the deployment of private IP addressing behind a public IP address or addresses.
    a. Port Address Translation extends NAT by allowing many private IP addressed machines to use a single public IP address, or several IP addresses from a pool.

Classless Interdomain Routing

1. Discuss how Classless Interdomain Routing has improved the flexibility of IPv4 addressing versus the use of classful addressing.

2. Introduce students to the concept of Classless Interdomain Routing (CIDR). Discuss how CIDR allows subnet masks to be configured regardless of their address class.

3. Explain why there may be a need to assign a subnet mask different from the default.

4. Explain the use of an IP prefix in CIDR notation.

5. Define and describe a broadcast domain.
    a. Point out that a broadcast is a packet addressed to all computers on the network.
    b. Explain why TCP/IP communication relies heavily on broadcast packets.

Subnetting

1. Introduce subnetting.

2. Describe how subnetting allows a large network to be broken down into smaller, more manageable networks.

3. Mention that another reason to subnet is to conserve IP addresses.

4. Describe how to subnet with the purpose of creating more networks, or with the purpose of creating more hosts.

a. Teach students to first figure out how many bits will be needed to accommodate whatever they're trying to work with. For example, 120 hosts would require 7 bits (2^7 = 128)
b. Explain how to reallocate these bits to accommodate for these hosts. The intent in 1-a is presumably to only provide for those 120 hosts, while simultaneously creating some additional networks. If a class C address was used, say 192.168.1.0, the subnet mask would become 255.255.255.128. This would create two subnets on the class C: 192.168.1.0 and 192.168.1.128.
c. Students must be aware of the formula 2^n-2 when subnetting.

5. Use Table 1-6 to discuss the pattern of subnetwork numbers.

6. Discuss with students that the host addresses in each subnet can be determined by cycling through the host bits. Use Table 1-7 in your discussion.

7. Explain the steps necessary to calculate a new subnet mask, given the example in the text.

8. Give students an example of why they might need to calculate a subnet mask based on a certain number of host addresses. Use Table 1-8 to explain how to calculate the subnet mask given a certain number of hosts.

Supernetting

1. Explain supernetting, and how it is most commonly used for summarizing routes in route tables.
   a. Supernetting is essentially the reverse operation of subnetting.

Teaching Tip	Students may read more about subnetting at http://technet.microsoft.com/en-us/library/bb726997.aspx

Quick Quiz 1

1. Which of the five IP Address class ranges are available for host assignment?
   Answer: Classes A, B, and C.

2. _____ allows an organization to use private IP addresses while connected to the Internet.
   Answer: Network Address Translation (NAT)

3. What is the name of the process of dividing a single network address into two or more subnetwork addresses, each with fewer available host IDs than the original network address.

Answer: subnetting

4. What subnet mask does the following network in CIDR notation have? 192.168.2.0/27
   a. 255.255.255.224
   b. 255.255.255.192
   c. 255.255.255.240
   d. 255.255.255.128

   Answer: 255.255.255.224

5. True or False: The differences between TCP/IPv4 and TCP/IPv6 are limited to the TCP part of the protocol.
   Answer: False

Configuring IPv4 Addresses

1. Explain the rules to remember when assigning a computer an IP address:
   a. Every IP address configuration must have a subnet mask.
   b. All hosts on the same physical network must share the same network ID in their IP addresses.
   c. All host IDs on the same network must be unique.
   d. An administrator cannot assign an IP address in which all the host ID bits are 0. This type of IP address is reserved as the network ID.
   e. An administrator cannot assign an IP address in which all the host ID bits are 1. This type of IP address is reserved as the network broadcast address.
   f. Computers assigned different network IDs can communicate only by sending network packets to a router, which forwards the packets to the correct network.

Configuring Multiple IP Addresses

1. Use Figure 1-6 to illustrate how Windows operating systems allow the assignment of multiple IP addresses to a single network connection in the Advanced TCP/IP Settings dialog box.

2. Describe the situations where multiple IP addresses can be useful:
   a. The computer is hosting a service that must be accessed by using different addresses.
   b. The computer is connected to a physical network that hosts multiple IP networks.

Configuring the Default Gateway

1. Introduce and define the default gateway router.

2. Mention that an administrator can configure multiple default gateways in the Advanced TCP/IP Settings dialog box.

3. Define a metric and explain its use in configuring default gateways.

4. Discuss how multiple gateways provide fault tolerance to a computer.

5. Define and describe a multihomed server.

6. Describe the situations where a multihomed server can be used:
   a. A server is accessed by internal clients (clients on the network) and external clients (clients on the Internet or an extranet).
   b. A server provides resources for computers on multiple subnets of the network.
   c. A server is configured as a router or VPN server.

7. Explain why renaming each network connection to describe the network it connects to is recommended.

8. Discuss why Windows always chooses only one default gateway for sending packets to remote networks.

Teaching Tip	Students may read more about configuring multihomed servers at http://technet.microsoft.com/en-us/library/cc772564.aspx.

9. Introduce routing tables and explain their purpose.

10. Explain how the routing table contents are displayed with the route command.

11. Use Figure 1-7 to illustrate a partial result of the route print command.
    a. Explain the network destination of 0.0.0.0 with a netmask of 0.0.0.0.
    b. Explain what happens to a packet with a destination address that does not match any entries in the routing table.
    c. Note that all Network Destination entries beginning with 127 indicate the computer's loopback address.

12. Describe how the route command can be used to change the routing table.

Teaching Tip	Students may read more about the Route command syntax at http://technet.microsoft.com/en-us/library/bb490991.aspx.

IP Configuration Command-Line Tools

1. Introduce other command-line tools:
   a. `netsh`
   b. PowerShell cmdlets
   c. `ipconfig`
   d. `ping`
   e. `arp`
   f. `tracert`
   g. `nslookup`

2. `netsh`: Discuss how the netsh.exe command can be used to perform a variety of network configuration tasks. Mention that students can see a list of netsh commands by typing netsh /? at the command prompt.

3. PowerShell:
   a. Mention to students that Microsoft certification exams place much emphasis on the ability to use PowerShell for configuration tasks.
   b. Discuss the numerous IP configuration cmdlets introduced in the section. Use Figure 1-9 to show the output from using the Get-NetIPConfiguration cmdlet.
   c. Explain how students can get detailed help on each Cmdlet by typing Get-Help in front of the cmdlet.

4. Ipconfig:
   a. Introduce and describe the ipconfig command.
   b. Review some of the ipconfig command options.

5. Ping:
   a. Introduce and describe the ping command.
   b. Discuss the output from a ping command.
   c. Explain how to see options available with the ping command.
   d. Review some of the ping options.

Teaching Tip	Students may read more about the Ping command syntax at http://technet.microsoft.com/en-us/library/bb490968.aspx.

6. Arp:
   a. Introduce and describe the arp command.
   b. Describe the use of the ARP cache.
   c. Review some of the arp command options.

7. tracert
   a. Introduce and describe the tracert command.

b. Note that tracert displays the address or DNS name of each router a packet travels through to reach the specified destination.
c. Explain why tracert is useful for troubleshooting the routing topology of a complex network and finding the bottleneck between a computer and a destination network.

1. `nslookup`
   a. Introduce and describe the `nslookup` command.
   b. Note that by default, `nslookup` uses the DNS server address configured in the IP address settings.
   c. Explain how to use `nslookup` in interactive mode.
      i. Note that an administrator can type a question mark at the interactive mode prompt to get a list of available options and commands.

Teaching Tip	Students may read more about the Nslookup command syntax at http://technet.microsoft.com/en-us/library/bb490950.aspx.

Internet Protocol Version 6

1. Discuss some of the features of IPv6 that address IPv4's biggest shortcomings.

2. Point out that methods have been developed to allow IPv4 and IPv6 networks to coexist and communicate with one another.

IPv6 Overview

1. Describe the improvements and changes in IPv6 from IPv4:
   a. Larger address space
   b. Hierarchical address space
   c. Autoconfiguration
   d. Built-in Quality of Service (QoS) support
   e. Built-in support for security
   f. Extensibility

Teaching Tip	Students may learn more about IPv6 at http://technet.microsoft.com/en-us/library/bb726944.aspx.

IPv6 Address Structure

1. Note that with IPv6 subnetting as done in IPv4 will be obsolete.

2. Explain that an administrator will still need to work with binary numbers.

3. Note that there are 128 bits in the address.

4. Describe IPv6 addresses.

5. Introduce and describe the interface ID of an IPv6 address.

6. Discuss the different ways an IPv6 interface ID can be assigned to a host:
    a. Using the 48-bit MAC address
    b. randomly generated permanent interface identifier
    c. A temporary interface identifier
    d. Via DHCPv6
    e. Manually

IPv6 Address Types

1. Point out that unicast and multicast addresses in IPv6 perform much like their Ipv4 counterparts, but anycast addresses are altogether different.

IPv6 Unicast Addresses

1. Remind students that a unicast address specifies a single interface on a device.

2. Explain that there are three primary types of IPv6 unicast addresses.

3. Link-Local Addresses:
    a. Define and describe link-local addresses.
    b. Point out to students that addresses starting with fe80 are called link-local IPv6 addresses.

4. Unique Local Addresses
    a. Define and describe unique local IPv6 addresses.
    b. Describe the global ID and how it is identified.
    c. Point out that unique local addresses can begin with fc or fd and that global IDs beginning with fd are called “locally assigned”.

5. Global Addresses
    a. Explain that global unicast IPv6 addresses are analogous to public IPv4 addresses.
    b. Discuss the advantages IPv6 addresses have over IPv4 addresses, aside from the much larger address space.
    c. Discuss the formatting features of IPv6 global addresses.

6. IPv6 Special-Purpose Addresses: Discuss the IPv6 addresses and prefixes that have a special purpose:
    a. Loopback address
    b. Zero address
    c. Documentation
    d. IPv4-to-IPv6 transition

Subnetting with IPv6

1. Explain how subnetting will still be used in IPv6 networks. Use Figure 1-10 to illustrate the structure of a typical IPv6 address.
    a. Explain the strategies that can be used with the 16 bits available:
        - A small network that does not have multiple subnets can simply leave the subnet ID as all 0s.
        - A network that does need to subnet could just take the 16 bits for the subnet ID and start counting.
        - Note that the IPv6 developers reserved 2001:DB8 for use in documentation.
        - Large organizations with multiple locations could take a more structured approach and assign each location a bank of subnets.

Multicast Addresses

1. Explain that a multicast address in IPv6 performs the same function as its IPv4 counterpart. Discuss the structure of a multicast address.

Anycast Addresses

1. Explain what makes anycast addresses unique.

2. Point out that anycast addresses do not have a special format and that a node that is assigned this type of address must be configured to recognize these addresses.

IPv6 Autoconfiguration

1. Discuss the two IPv6 autoconfiguration methods: stateless and stateful.

Autoconfiguration on Windows Hosts

1. Explain that the Windows autoconfiguration process occurs in steps. Go over the steps with your students.

2. Discuss the options that allow Windows Server 2016 devices to be configured to send router advertisements. Reference Figures 1-11 and 1-12 for PowerShell cmdlets and output.

3. Use Figure 1-13 to discuss the output from the `ipconfig` command after configuration with the advertised prefix.

Transitioning from IPv4 to IPv6

1. Explain that starting with Windows Server 2008 and Vista, the Windows OS has maintained a dual IP architecture by default.

2. Introduce students to the technologies and special address types that help ease the transition to IPv6 while maintaining compatibility with IPv4.

Dual IP Layer Architecture

1. Discuss the purpose of a dual IP layer architecture.

IPv6-over-IPv4 Tunneling

1. Define and describe tunneling.

2. Use Figures 1-17 and 1-18 discuss how IPv6-over-IPv4 tunneling works.

3. Explain how a IPv6-over-IPv4 tunnel can be created manually. Reference Figure 1-19.
    a. Explain the `netsh` command used to create the tunnel.
    b. Point out that the command needs to be repeated on the server on both sides of the tunnel.
    c. Also note the command that must be entered to specify the tunnel as the interface to use to reach the IPv6 network

Intra-Site Automatic Tunnel Addressing Protocol

1. Define and describe Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).

2. Mention to students that ISATAP is enabled by default on Windows Server 2016 as well as other Windows OSs starting with Windows Vista.

3. Discuss the format of ISATAP addresses, differentiating public and private.

4. Describe the three methods of enabling ISATAP interfaces. Display the interface, citing Figure 1-20

5. Show students how to test an ISATAP interface by using `ping`. Refer to Figure 1-21.

6to4 Tunneling

1. Define and describe 6to4 tunneling.

2. Discuss the format of a 6to4 address.

Teredo Tunneling

1. Define and describe Teredo tunneling.

2. Explain the three components of Teredo.

3. Discuss the format of a Teredo address.

Quick Quiz 2

1. True or False: All hosts on the same network must share the same network ID.
   Answer: True

2. How many bits are in an IPv6 address?
   a. 16
   b. 32
   c. 64
   d. 128
   Answer: D

3. Which IPv6 address type can't be routed and are equivalent to Automatic Private IP Addressing (APIPA) in IPv4?
   a. Global addresses
   b. Anycast addresses
   c. Link-local addresses
   d. Unique local addresses
   Answer: C

4. Which command displays the route packets take between two computers?
   a. route
   b. tracert
   c. nslookup
   d. ping
   Answer: B

5. Which of the following tunneling protocols requires that the IPv4 address embedded in the tunneling address must be a public address?
   a. Teredo
   b. ISATAP
   c. IPv6-overIPv4
   d. 6to4
   Answer: D

Class Discussion Topics

1. Discuss the advantages of subnetting in IPv4.

2. Discuss whether IPv6 will truly resolve the issues it claims to address. Have the students explain why or why not.

3. Discuss factors that will influence how long IPv6 will adequately support network structures before it becomes obsolete.

Additional Projects

1. Have the students research IPv6. The student should prepare a report on their findings. Report sections should include an introduction, background, the current development state, the current implementation state, and the future of IPv6.

2. There are numerous IP subnet calculators available. Have the students search the Internet for IP subnet calculators and provide a report of their findings.

Additional Resources

1. History and evolution of TCP/IP:
https://en.wikipedia.org/wiki/Internet_protocol_suite

2. Supernetting and Classless Interdomain Routing
https://technet.microsoft.com/en-us/library/cc958837.aspx

3. Netsh Command Syntax, Contexts, and Formatting
https://docs.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh-contexts

Key Terms

- **6to4** An IPv4-to-IPv6 transition protocol that provides automatic tunneling of IPv6 traffic over an IPv4 network. It can handle host-to-router or router-to-host tunneling but is most often used to create a router-to-router tunnel.
- **Automatic Private IP Addressing (APIPA)** A method of automatic IP address assignment that occurs when a computer can't contact a DHCP server; uses the range 169.254.1.0 through 169.254.254.255.

- **broadcast** A packet addressed to all computers on the network.
- **broadcast domain** The bounds of a network that defines which devices must receive a packet that's broadcast by any other device; usually an IP subnet.
- **CIDR notation** A method of expressing an IP address in the format A.B.C.D/*n*; *n* is the number of 1 bits in the subnet mask or the number of bits in the network ID. *See also* Classless Interdomain Routing (CIDR).
- **classful addressing** The use of IP addresses with their default subnet masks according to their address class: A, B, or C.
- **Classless Interdomain Routing (CIDR)** The use of IP addresses without requiring the default subnet mask. *See also* subnet mask.
- **default gateway** Part of a computer's IP address configuration, it is the address of a device, usually a router, that tells the computer where packets destined for another network should be sent.
- **destination IP address** The IP address of the computer a packet is sent to.
- **dual IP layer architecture** The current architecture of the IPv6 protocol in Windows, in which both IPv4 and IPv6 share the other components of the stack.
- **Extended Unique Identifier (EUI)-64 interface ID** An autoconfigured IPv6 host address that uses the MAC address of the host plus an additional 16 bits.
- **frame** A Data Link layer unit of data that contains a destination and source MAC address and an error-checking code that is ready to be transferred to the network medium.
- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)** An automatic tunneling protocol used to transmit IPv6 packets between dual IP layer hosts across an IPv4 network. *See also* dual IP layer architecture.
- **link-local** An address that can only communicate on the local LAN.
- **link-local IPv6 address** Similar in function to the IPv4 APIPA addresses, link-local IPv6 addresses begin with fe80, are self-configuring, and can't be routed. *See also* Automatic Private IP Addressing (APIPA).
- **localhost** A reserved name that corresponds to the loopback address, 127.0.0.1. *See also* loopback address.
- **logical AND operation** A binary operation in which there are two operands; the result is 0 if either operand is 0 and 1 if both operands are 1.
- **loopback address** The IP address 127.0.0.1, which always refers to the local computer and is used to test the functioning of TCP/IP.
- **MAC address** A physical-layer address that is an integral part of a network interface card (NIC).
- **metric** A value assigned to the gateway based on the speed of the interface used to access the gateway.
- **multicasting** A network communication in which a packet is addressed so that more than one destination can receive it.
- **Network Address Translation (NAT)** A process that translates the source or destination IP address in a packet to a different value; often used to allow using private IP addresses while connected to the Internet.
- **octet** An 8-bit value; a number from 0 to 255 that's one of the four numbers in a dotted decimal IP address.

- **packet** A Network-layer unit of data used by IPv4 and IPv6 which contains destination and source IP addresses along with other flags and parameters.
- **segment** A Transport-layer unit of data that is used by TCP and UDP which contains the destination and source port numbers used to identify Application-layer protocols.
- **source IP address** The IP address of a computer that's sending a packet.
- **subnet mask** A 32-bit dotted decimal number consisting of an unbroken series of binary 1 digits followed by an unbroken series of binary 0 digits. Used with an IP address to determine the network ID.
- **subnetting** A process that reallocates bits from an IP address's host portion to the network portion, creating multiple smaller address spaces.
- **supernetting** A process that reallocates bits from an IP address's network portion to the host portion, effectively combining smaller subnets into a larger supernet.
- **Teredo** An automatic IPv6-over-IPv4 tunneling protocol that solves the problem of 6to4's requirement of a public IPv4 address and the inability to traverse NAT routers. *See also* 6to4.
- **Teredo client** A host device behind a NAT router that's running IPv4 and IPv6 and wants to use Teredo tunneling to access IPv6 devices or other Teredo clients across an IPv4 network.
- **Teredo relay** A router running IPv6 and IPv4 that forwards packets between Teredo clients and hosts on IPv6 networks. The Teredo relay advertises the 2001::/32 network to let hosts know that it provides Teredo relay services.
- **Teredo server** A host on the Internet running IPv4 and IPv6 that's connected to both IPv4 and IPv6 networks that facilitates communication between Teredo clients.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)** A network protocol suite designed to deliver data packets to computers on any scale of network, from a small two-computer LAN to the worldwide Internet.
- **tunneling** A common network protocol technique that allows transmitting a packet in a format that would otherwise be incompatible for the network architecture by encapsulating the packet in a compatible header format.
- **unicast address** An address in a unit of network data intended for a single destination computer.
- **unique local IPv6 address** An address for devices on a private network that can't be routed on the Internet.
- **zone id** A number which is used to distinguish which interface an IPv6 link-local address is bound to.