APPENDIX A

Answers to Review Questions

Chapter 1

1. **C** A firewall provides a layer of security for a computer that has a direct connection to the Internet. Routers connect subnets. Switches connect computers. A virtual private network (VPN) provides access to a private network over a public network.
2. **True** Wireless access points (WAPs) often provide connectivity for wireless clients to the Internet.
3. **A** A local area network (LAN) is a group of computers connected in a single connection. A wide area network (WAN) is a group of computers connected across two or more locations. A virtual LAN is an advanced implementation of a switch and wasn't covered in this chapter. A virtual private network (VPN) allows connectivity to a private network over a public network.
4. **bits** A lowercase *b* indicates bits. An uppercase *B* indicates bytes.
5. **B** A domain supports single sign-on where each user needs only one username and password. A workgroup requires users to have multiple usernames and passwords to access multiple computers. A wide area network (WAN) typically connects two or more LANs over separate geographical distances. A VPN provides access to the private network over a public network.
6. A group of computers connected together in a network
7. Typically two or more LANs connected together over a large geographical distance
8. **D** A virtual private network (VPN) allows connectivity to a private network over a public network such as the Internet. A domain controller hosts Active Directory but does not provide connectivity over the Internet. A local area network (LAN) connects multiple computers in a single location. A wireless access point (WAP) is used to provide connectivity to wired networks from wireless clients.

9. **A, C** Remote access servers are either dial-up or virtual private network (VPN) based. Neither a wireless access point (WAP) nor a domain controller are types of remote access servers.
10. **False** Standards go through stages before they are considered standards, and many RFCs are submitted as Informational documents that do not go through stages to become standards.

Chapter 2

1. **C** Broadcast traffic is sent from one device to all other devices in a subnet. Unicast goes from one device to another device. Multicast goes from one device to many devices. There is no such thing as allcast.
2. **False** A switch passes broadcast.
3. **C** Switches connect devices together, and routers connect subnets together. They are not the same. Switches pass broadcasts, but routers do not pass broadcasts.
4. **True** Bridges can connect dissimilar physical topologies such as twisted pair on one network with fiber-optic connections on another network.
5. **rules** The most basic hardware- or network-based firewall is simply a router with rules. These rules control both inbound and outbound traffic.
6. **A software component that provides protection for a single system** Network-based firewalls include both hardware and software.
7. **False** A crossover cable is used to connect similar devices such as a switch to a switch, or a switch to a router. A straight-through cable is used to connect a computer to a switch.
8. **D** T568B defines the standard color code for twisted-pair cables.
9. **a perimeter network (or DMZ)** A perimeter network provides a layer of protection for systems that are accessible from the Internet.
10. **An extranet** An extranet is accessible via the Internet but only to trusted entities.

Chapter 3

1. **seven** The OSI Model has seven layers.
2. **Various answers are possible.** One mnemonic is All People Seem To Need Data Processing for layers 7 down to layer 1. Another mnemonic is Please Do Not Throw Sausage Pizza Away for layers 1 up to layer 7.

3. **False** TCP is a connection-oriented protocol. UDP is connection-less.
4. **B** A unit of data at the Transport layer is a segment.
5. **C** A Media Access Control (MAC) address, or physical address, is composed of six pairs of hexadecimal characters. Valid hexadecimal characters are 0 through 9 and A through F.
6. **Network** Both IPv4 and IPv6 operate on the Network layer.
7. **TCP and UDP** The two primary protocols operating on the Transport layer are TCP and UDP. Several other Transport layer protocols exist, but these are the ones stressed in this chapter.
8. **True** Devices such as hubs on layer 1 have very little intelligence. Devices such as advanced firewalls on layer 7 have much more intelligence.
9. **C** Routers operate on the Network layer, layer 3.
10. **E** Proxy servers operate on the Application layer, layer 7 of the OSI Model.

Chapter 4

1. **B** TCP is a connection-oriented protocol. UDP is connection-less.
2. **True** UDP does not provide guaranteed delivery of data. Undetected data loss is possible.
3. **A, B, D** Streaming media and VoIP traffic all commonly use UDP since the overhead of TCP can slow traffic down.
4. **C** The Address Resolution Protocol resolves IP addresses to MAC addresses.
5. **SMTP, POP3, and IMAP4** Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), and Internet Message Access Protocol version 4 (IMAP4) are used for email.
6. **IPSec** Internet Protocol Security is used with L2TP (as L2TP/IPSec) for VPNs.
7. **IGMP** The Internet Group Management Protocol is used to manage multicast transmission.
8. **D** RDS uses port 3389. LDAP uses port 389. Secure LDAP uses port 636. PPTP uses port 1701.
9. **B** SMTP uses port 25. L2TP uses port 1723. RDS uses port 3389.
10. **C** Kerberos uses port 88. SMTP uses port 25. HTTP uses port 80. HTTPS uses port 443.

Chapter 5

1. **B** IPv4 addresses are in dotted decimal format. Each decimal must be between 0 and 255. You cannot use 256, since 256 is not a valid number in an IPv4 address.
2. **C** The first decimal in a Class C address is in the range of 192–224.
3. **False** The first one has a network ID of 192.168.1.0, and the second one has a network ID of 192.168.2.0.
4. **True** Both have a network ID of 10.0.0.0.
5. **Point B** The default gateway is the interface on the near side of the router for the subnet.
6. **C** The /26 in the IP address is CIDR notation indicating how many bits are a 1 in the subnet mask. The first octet has eight 1s, the second octet has eight 1s, the third octet has eight 1s, and the fourth octet has two 1s. The subnet mask is 255.255.255.192.
7. **B** The reserved IP address ranges are as follows:

   10.0.0.1 through 10.255.255.254

   172.16.0.1 through 172.31.255.254

   192.168.1.1 through 192.168.255.254

   IP addresses can't have numbers greater than 255 as in 10.80.*256*.1.
8. **C** The formula is $2^h - 2$ where h is the number of bits used in the host ID. Since 26 bits are used in the network ID, 6 bits are left for the host ID (32 – 26 = 6) and 26 – 2 = 62.
9. **False** The first IP address has a subnet mask of 255.255.255.192 and a network ID of 192.168.1.64. The second IP address has a subnet mask of 255.255.255.192 and a network ID of 192.168.1.128.
10. **A** An address starting with 169.254 is an APIPA address. An APIPA address is assigned to DHCP clients when a DHCP server can't be reached. Manually configuring the default gateway or the DNS server IP address isn't needed for a DHCP client.

Chapter 6

1. **C** IPv6 addresses are expressed as groups of hexadecimal characters. Valid hexadecimal characters are 0 through 9 and *a* through *f*. Characters such as *x*, *g*, and *h* are not valid.
2. **E** Unique local addresses are assigned as private addresses. They have a prefix of fd hexadecimal.

3. **D** Internet Protocol Security (IPSec) is built into IPv6 and allows IPv6 to easily encrypt traffic.
4. **False** The IPv6 prefix of fd is for unique local addresses. Link-local addresses have a prefix of fe80.
5. **Teredo** Teredo is a tunneling protocol that encapsulates IPv6 packets within IPv4 datagrams. A lesser used protocol is 6to4, which can also be a valid answer.
6. **unique local addresses** Unique local addresses are assigned to hosts on private networks.
7. **A** Network Discovery uses ICMPv6 messages for router discovery.
8. **global unicast** Global unicast addresses are used on the Internet. They have a prefix of 2.

Chapter 7

1. **A, B** Electromagnetic interference (EMI) and radio frequency interference (RFI) can cause problems for networks.
2. **A** A short-duration increase in AC power is a power spike. A power surge is a relatively long-duration increase in AC power. Surge protectors can protect against power spikes and surges.
3. **False** An uninterruptible power supply (UPS) provides short-term power when power fails. The goal is to keep the system operational long enough to do a logical shutdown or to allow a generator to power up and stabilize before shifting from UPS power to the generator power.
4. **True** The shielding in shielded twisted pair (STP) provides protection against interference and cross talk.
5. **100** Twisted pair is limited to no more than 100 meters between devices. A repeater can extend the length of the cable.
6. **C** CAT 6 cable is rated at 1000 Mpbs. CAT 6A is rated at 10000 Mpbs.
7. **Twisted pair using four twisted pairs** The *T* indicates twisted pair, and currently used twisted-pair cables have four twisted pairs.
8. **A, B, C** Protocol analyzers can capture traffic going across a network. These are commonly called sniffers, and Microsoft's Network Monitor is one example of a protocol analyzer.
9. **A** 802.11g uses 2.4 GHz.

Chapter 8

1. **modular switch** You can expand a modular switch by adding modules.
2. **B** Ports on a 100 Mbps switch are labeled with F or Fa to indicate Fast Ethernet. The first port is 0, and the second port is 1. E is for 10 Mbps ports, and 1000 Mbps ports use Gi.
3. **False** A layer 2 switch creates separate collision domains, not separate broadcast domains.
4. **C** Switches create a separate collision domain for every device connected to the switch. Bridges creates separate collision domains but not one for every device. There's no such thing as a managed hub. Firewalls don't create separate broadcast or collision domains.
5. **False** A managed switch needs to be configured by an administrator to take advantage of the capabilities. Unmanaged switches work just by plugging them in.
6. **router** A layer 3 switch provides routing on layer 3 just like a router. It does so using hardware capabilities, so it is quicker than a router that routes using software capabilities.
7. **A** Switches create MAC tables to map MAC addresses to physical ports. Routers have routing tables to track subnetworks; although it's feasible to call a routing table a layer 3 table, it isn't an actual term, and it would track subnetworks, not computers. There's no such thing as a managed table.
8. **C** The minimum number of ports required for a VLAN is two. If the port has 48 ports, you can create as many as 24 VLANs.
9. **D** The five combined ports give a combined speed of 500 Mbps, and since full-duplex is being used, data can travel both ways, giving an effective throughput of 1000 Mbps (1 Gbps).
10. **Port security** Port security includes configuring the switch with specific MAC addresses and blocking access to unused ports.

Chapter 9

1. **A** The router knows only about directly connected routes by default.
2. **D** The easiest way is to add static routes to each router. Although you could add routing protocols such as OSPF or RIPv2 to create dynamic routes, it's much easier to just add static routes if you have only two routers and three subnets.
3. **False** Routers use the least cost path based on the metric to determine the best path.

4. **Routing table** A router stores all known routes in a routing table.
5. **A, B, C** Routing protocols allow clients to learn routes from each other dynamically. Common routing protocols on internal networks are RIPv2 and OSPF. ARP translates IP addresses to MAC addresses.
6. **False** Windows Server 2008 supports RIPv2 but not OSPF.
7. **B** A DHCP relay agent can be added to relay DHCP BootP broadcasts through routers that are not RFC 1542 compliant. RFC 1542-compliant routers can forward DHCP and BootP broadcasts. Adding another DHCP server would be an expensive solution and would work only if you had only two subnets connected. If you used this solution, you would need to add DHCP servers for every subnet.
8. **C** The IGMP Router and Proxy service can be added to a Windows Server 2008 server router so that it passes multicast traffic.

Chapter 10

1. **D** Host names are used on the Internet. Internal networks can have host names and/or NetBIOS names.
2. **B, D** Both host names and NetBIOS names are used on Microsoft networks, though the usage of NetBIOS names is being phased out. DNS resolves host names, and WINS resolves NetBIOS names.
3. **False** The primary name resolution method for NetBIOS names is WINS.
4. **True** Entries in the hosts file are automatically placed in the host cache (also called the *DNS resolver cache*). These entries can be viewed by entering `ipconfig /displaydns` at the command prompt.
5. **C** The `ipconfig /displaydns` command will display the host name cache. The `ipconfig /flushdns` command clears the cache. The `nbtstat` commands are used with NetBIOS names.
6. **False** WINS operates only on internal Microsoft networks to resolve NetBIOS names. WINS is not used on the Internet.
7. **A** The `ipconfig /flushdns` command removes entries from the host cache that have been resolved from a DNS server.
8. **Link-local multicast name resolution (LLMNR)** An IPv6 address with a prefix of fe80 is a link-local address. LLMNR is used for name resolution of link-local addresses.

Chapter 11

1. **A** The Internet is considered the riskiest network security zone. Users with Internet access from anywhere in the world can attack resources placed directly on the Internet.
2. **Network Address Translation (NAT)** NAT is a service that can run on routers and proxy servers. It translates public and private IP addresses, reduces the number of public IP addresses needed by a company, and hides internal computers.
3. **C** A proxy server can restrict access to certain websites by using filters. The filter includes what websites are restricted and blocks them, or it includes what websites are allowed and blocks all others.
4. **True** A perimeter network (also called a demilitarized zone or DMZ) provides a layer of security for Internet-facing servers.
5. **A, B** Perimeter networks can be created with one or two firewalls. One firewall is cheaper, though a perimeter network created with a single firewall can be more complex to create. Although a third or fourth firewall can technically be added to a perimeter network, they would be redundant and don't follow perimeter network models.
6. **C** Network discovery is a service that allows computers to discover other computers on the network.
7. **An extranet** An extranet provides access to internal resources to trusted entities over the Internet.

Chapter 12

1. **B, C** The SSID is a logical network name for a WLAN and has a maximum alphanumeric value of 32 bits. It doesn't identify the device type, and it doesn't identify the security encryption method.
2. **False** Wireless networks (802.11 networks) use CSMA/CA. 802.3 networks use CSMA/CD.
3. **D** 802.11a networks use 5 GHz. They have a speed of 11 Mbps.
4. **A** IEEE 802.11b and 802.11g operate in the 2.4 GHz range. 802.11a operates in the 5 GHz range, and 802.11n is compatible with all three standards. None of the standards uses 4.1 GHz or 2.4 MHz.
5. **C, D** 802.11n networks can use 2.4 GHz and 5 GHz. They have a speed of 300 Mbps.
6. **B** 802.11b networks can be as fast as 11 Mbps.

7. **True** 802.11n networks use MIMO technology allowing them to operate at 300 Mbps and sometimes higher.
8. **D** WPA2 Enterprise Mode is the strongest. WPA2 Enterprise mode uses an 802.1x server, while WPA2 Personal mode only needs a preshared key.
9. **False** A WAP is only an access point, but a wireless router includes an access point and additional components such as a router, a switch, and DHCP.
10. **B** A Point-to-Point (P2P) wireless bridge can connect wired networks in two buildings 25 miles apart.

Chapter 13

1. **A, C, D** Dial-up, DSL, and broadband cable are all methods that a SOHO could use for Internet access.
2. **B** An ISDN BRI uses two 64 Kbps B channels and one D channel.
3. **B** DSL connections require the user to be close to a central office since the digital signal can't travel as far over telephone lines as an analog signal.
4. **False** E1 and E3 lines are used in Europe. T1 and T3 lines are used in the United States.
5. **A** A T1 is 1.544 Mbps. An E1 is 2.048 Mbps, an E3 is 34.368 Mbps, and a T3 is 44.736 Mbps.
6. **C** The Routing and Remote Access Services service is part of the Network Policy Access Services role. You can configure it as a VPN or a dial-up server.
7. **A, B, C** PPTP, L2TP, and SSTP are all valid tunneling protocols.
8. **C** RADIUS is used for central authentication and logging. It cannot be used as a WAN link and doesn't provide encryption.

Chapter 14

1. **A** The `/?` switch provides help for almost any command. The format is command `/?`, as in `ipconfig /?`.
2. **A, B** Both `ipconfig` and `ipconfig /all` will show the default gateway.
3. **C** The `ping` command checks connectivity with remote computers. You can follow the computer name with the IP address.
4. **`-4`** You can use the `ping -4 computername` or `ping -4 IPAddress` command to ensure that `ping` uses IPv4.

5. **B** The error indicates that the host could not be resolved to an IP address. It could be a problem with DNS (or another type of name resolution), or it could be the host name is not entered correctly in the `ping` command.
6. **C** The error usually indicates a problem with routing. It could be that a router is not configured correctly or that one of the two systems does not have its default gateway configured correctly.
7. **False** `tracert` will identify the routers in the path, but it will not measure packet loss. `pathping` can measure packet loss.
8. **`netstat`** `netstat` (network statistics) can show statistics for protocols running on a system.
9. **D** `netstat -b` shows all the connections that all applications are using to connect to the network. `netstat` (without the `-b` switch) does not list the applications.
10. **False** Telnet is not installed by default in Windows Server 2008. You can add Telnet as a feature.