APPENDIX A

Answers to the "Do I Know This Already?" Quizzes and Q&A Sections

Chapter 1

"Do I Know This Already?"

1. A, B, C
2. B
3. B
4. D
5. D
6. A
7. A
8. A, B, C, D

Q&A

1. The Application Layer
2. The network is the essential piece that they all have in common. This applies to all infrastructure (Layers 1, 2, and 3) as well as supplemental services that might be shared additionally.
3. Teleworker architecture
4. Campus, data center, branch, WAN/MAN, enterprise edge, teleworker
5. This is a rather subjective answer as it calls upon the reader to reference a solution from his or her own experiences. To a large degree, the solution will be based on personal networking experiences. A sample solution would include
   - Cisco ISR with SRST, VPN, and Content Engine enabled. It may also be prudent to add an AIM-CUE to the ISR to provide a local automated attendant and voice messaging capabilities for some users (up to 25 on an AIM CUE).

- QoS-enabled MPLS WAN connectivity with bandwidth sufficient to support the voice, video, and data needs of those 50 users.
- Cisco IP Phones and IP Communicator Software for user laptops.

6. Voice and collaboration services

   Device mobility services

   Security and identity services

   Storage services

   Computer services

   Application networking services

   Network infrastructure virtualization

   Services management

   Adaptive management services

   Advanced analytics services

   Infrastructure management services

7. Resources to which virtualization capabilities apply include infrastructure components such as VLANs, VRFs, MPLS, virtual firewalls, VPNs, presence information, message routing, load balancing, hard disk space, IO, CPU cycles, and more.
8. SONA is the framework that provides a technological and architectural guide for enterprise networks in the quest to become an IIN. SONA is the path; IIN is the destination.

Chapter 2

"Do I Know This Already?"

1. C
2. C
3. B
4. D
5. A
6. A
7. C
8. A

Q&A

1. IPsec VPNs utilize a CPE router that maintains a nailed-up connection to the central site at all times. A remote-access VPN is a client-initiated connection to the central site.

2. High availability for services and applications, removal of any single point of failure, secure the network infrastructure, implement QoS throughout the entire network, decide on central site VPN solution (IPsec or remote access or both), Internet access, Cisco IP Phone, and Cisco Unified Video Advantage camera solution at teleworker's home.

3. MPLS provides larger sites with Layer 3 connectivity and any-to-any communication capabilities. MPLS also provides for QoS traffic markings to be honored within the provider's network.

   Frame Relay and ATM are traditional Layer 2 WAN technologies. These are useful in providing connectivity to sites that do not require integrated services and applications. Traffic flows are governed by traffic-shaping techniques that do not recognize Layer 3 DSCP markings.

   Site-to-site VPN is useful in connecting to partner or company site networks over the public Internet. Obviously, the nature of the public Internet means that all traffic is best-effort.

4. High-speed Internet access in residences, IP telephony, IP video capabilities, IPsec and remote-access VPNs, service provider network augmentation and service offerings, and QoS traffic classification and protection guarantees.

5. Network administration personnel go to somewhat great lengths to ensure the security of the network through firewall, IPS, IDS, and traffic filtering. This mitigates the effects of day-zero virus outbreaks, exploit exposure, and so on. When an enterprise chooses to support a teleworker solution, they extend the enterprise network presence to the home of the teleworker employee. This adds significant risk and exposure because the company might have a difficult time controlling traffic flow to and/or from the teleworker home. The Internet surfing habits of the teleworker and others in the home pose a potential risk as a point of entry for viruses, spyware, malware, and more. Support for the teleworker home network is also a significant factor. Most homes today have wireless networks that exist in varying degrees of security. Enterprise network administrators do not necessarily wish to dictate wired and/or wireless security practices to individuals in their own homes.

6. There are quite a few ways in which the risks posed to the enterprise by teleworker home networks might be mitigated. The teleworker must agree to the corporate security policy regarding network access, of course. However, some options, such as personal firewalls, anti-spam, anti-spyware, and other related software can assist in mitigating risks. Such software should be dictated and supported by the enterprise network administrators. Disallowing options in the VPN connectivity, such as split-tunneling, might also be considered.

7. Satellite connectivity does offer some degree of connectivity to the teleworker when other access methods are not available. It should be understood that the service levels provided by high-speed, low latency solutions such as DSL, cable, and fiber are more suited to the needs of a converged network. Some services might not function properly via satellite. Other options might include leased lines at the home. A T1 or fractional T1 terminated at a residential premise is not unheard of in the realm of possibilities. Obviously, there is the potential for significantly higher cost in such a solution.

   There are many additional possibilities. Each will come with its own set of challenges and benefits. These must be considered when offering teleworker services to employees.

8. Cisco.com contains a well-documented solution guide, known as an SRND, which contains tested best practices and configuration examples. It can be found at http://www.cisco.com/go/srnd.

Chapter 3

"Do I Know This Already?"

1. C
2. B
3. A
4. B
5. E
6. C
7. D
8. A
9. C
10. A
11. A
12. D
13. A, B, C
14. A
15. B
16. B

17. B

18. C

Q&A

1. As one example, consider a cable provider offering service to a very spread-out subscriber base, such as a rural setting. Fiber optic cable would allow longer distances to be reached and good signal strength to be maintained so that all customers would receive the offered applications and services at similar levels of service.

2. **Antenna site**—A location containing a cable provider's main receiving and satellite dish facilities. This site is chosen based on potential for optimal reception of transmissions over the air, via satellite, and via point-to-point communication.

   Headend—A master facility where signals are received, processed, formatted, and distributed over to the cable network. This includes both the transportation and distribution networks. This facility is typically heavily secured and sometimes "lights-out," meaning it is not regularly staffed.

   Transportation network—The means and media by which remote antenna sites are connected to the headend facility. Alternatively, this could be a headend facility connection to the distribution network. The transmission media may be microwave, coaxial supertrunk, or fiber optic.

   Distribution network—In typical cable system architectures, consists of trunk and feeder cables. The trunk is the backbone cable (usually 0.75-inch diameter) over which the primary connectivity is maintained. In many networks, the distribution network tends to be a hybrid fiber-coaxial network.

   Node—Performs optical-to-RF conversion of CATV signal as needed. Feeder cables (typically 0.5-inch diameter) originate from nodes that branch off into individual communities to provide services to anywhere between 100 and 2000 customers each.

   Subscriber drop—Connects the subscriber to the cable service network via a connection between the feeder portion of a distribution network and the subscriber terminal device (for example, a TV set, VCR, high-definition TV set-top box, or cable modem). The subscriber drop components consist of the physical coaxial cabling, grounding and attachment hardware, passive devices, and a set-top box.

3. From the cable providers' point of view, data over cable has enabled them to offer voice, video, and data services over a common access technology. They can now provide services similar to that of Vonage or other IP-based telephone service providers. From a teleworker perspective, the offerings could be as simple as corporate e-mail service, web services, content filtering and caching, security patches, virus updates, instant video conferencing, remote agent capabilities for call center agents, and more.

Future services might include video content streamed on-demand to the device of one's choosing or multiple devices simultaneously such as video-capable mobile phones, remote or in-car televisions, or devices in other locales.

4. Cable fits into the SONA framework at the networked infrastructure layer under the teleworker architecture. As part of the SONA framework, the teleworker architecture is vital to the evolution of the network into an IIN.

5. The steps defined by DOCSIS are as follows:

   - **Step 1: Downstream setup**—At power-on, the cable modem scans and locks the downstream path for the allocated RF data channel in order for physical and data link layers to be established.

   - **Step 2: Upstream setup**—The cable modem listens to the management messages arriving via the downstream path. These include information regarding how and when to communicate in the upstream path. These are used to establish the upstream physical and data link layers.

   - **Step 3: Layer 1 and 2 establishment**—The connection is established from the CM to the CMTS to build physical and data link layers.

   - **Step 4: IP address allocation**—After Layer 1 and 2 are established, Layer 3 can be allocated as well. This is done by the DHCP server.

   - **Step 5: Getting DOCSIS configuration**—The CM requests the DOCSIS configuration file from the TFTP server. This is an ASCII file created by DOCSIS editors. A DOCSIS configuration file is a "binary file" that has the parameters for cable modems to come online in accordance to what the ISP is provisioning, such as maximum downstream and upstream rates, maximum upstream burst rate, class of service or baseline privacy, MIBs, and many other parameters. This file can be loaded on the CM via TFTP or the CM can be manually configured.

   - **Step 6: Register QoS with CMTS**—The CM negotiates traffic types and QoS settings with the CMTS.

   - **Step 7: IP network initialization**—Once Layers 1, 2, and 3 are established and the configuration file is pulled from the TFTP server, the CM provides routing services for hosts on the subscriber side of the CM. It also performs some NAT functions so that multiple hosts might be represented by a single public IP address.

   As part of the initialization phase, the CM makes contact with a DHCP server on the provider's network. The DHCP server provides the following information to the CM:

   - IP address

   - Subnet mask

- Default gateway
- TFTP server
- DHCP relay agent
- The complete name of the DOCSIS configuration file
- Address of ToD server
- Syslog server address

Once this information is obtained, the CM can issue a request to the ToD server to set its clock to the correct time. This facilitates syslog timestamps. At this point, also, it can issue a TFTP request to the TFTP server for its DOCSIS configuration file (discussed in the previous section).

6. Channel bonding capabilities and IPv6 support.
7. Upstream: 120 Mbps; Downstream: 160 Mbps
8. Radio frequency information
   - Downstream frequency
   - Upstream channel ID
   - Network access configuration

   Class of service information
   - Class of service ID
   - Maximum downstream rate
   - Maximum upstream rate
   - Upstream channel priority
   - Minimum upstream rate
   - Maximum upstream channel burst
   - Class of service privacy enable

   Vendor-specific options
   - Vendor ID
   - Vendor-specific options

SNMP management

- SNMP write-access control and SNMP MIB objects

Baseline privacy interface configuration

- Authorize wait timeout
- Reauthorize wait timeout
- Authorization grace timeout
- Operational wait timeout
- Rekey wait timeout
- TEK grace time
- Authorize reject wait timeout

Customer premises equipment

- Maximum number of CPEs
- CPE Ethernet MAC address

Software upgrade

- TFTP software server IP address
- Software image filename

Miscellaneous

- Concatenation support
- Use RFC 2104 HMAC-MD5
- CMTS authentication

Chapter 4

"Do I Know This Already?"

1. B
2. A
3. C
4. B

5. A
6. B
7. A
8. C
9. B
10. A
11. A
12. B
13. A
14. B
15. B
16. D
17. A, C, D
18. B
19. A and C
20. C
21. A and B

Q&A

1. Loading coils, fiber optic cables, bridge taps
2. Voice: 0–4 kHz; upstream data: 25–160 kHz; downstream data: 240 kHz to 1.5 MHz
3. 256
4. DMT will relocate the signal to another channel.
5. Asymmetric DSL uses mismatched download/upload transfer rates, and symmetric DSL uses matching download/upload transfer rates.
6. 1.5 to 8 Mbps, but newer implementations such as ADSL2, ADSL2+, and ADSL4 promise bandwidths upwards of 20–30 Mbps in the not so distant future.
7. The G.lite standard was specifically developed to meet the "plug-and-play" requirements of the consumer market segment. G.lite is a medium-bandwidth version of ADSL that allows up to 1.5 Mbps downstream and up to 512 kbps upstream. G.lite allows voice and data to coexist

on the wire without the use of splitters. G.lite is a globally standardized (ITU G.992.2) interoperable ADSL system. Typical telco implementations currently provide 1.5 Mbps downstream and 160 kbps upstream.

8. PPP authentication in the form of PAP or CHAP
9. PPP LCP
10. Discovery serves to find the MAC address of the peering device (aggregation router) and obtain a SESSION_ID. It allows the CPE to find all DSLAMs and aggregation routers available to it.
11. The destination MAC is the broadcast address ff.ff.ff.ff.ff.ff.
12. RFC 1483/2684

Chapter 5

"Do I Know This Already?"

1. A
2. C
3. A
4. B and C
5. B and C
6. B
7. A
8. B
9. A and C
10. B
11. A, B, C, D
12. B

Q&A

1. In reality, all the options in this chapter would be relevant. The DSL connection and associated PPPoE session would need to be in place and passing traffic. DHCP may or may not be used on the subscriber-facing side of the connection as many power users make the decision to address their own devices on the home network.

2. Certainly, there is. The use of the static default route is a network administration decision. It may well be that an IT department wishes to use a dynamic protocol to reach every site, regardless of size. Protocols such as OSPF and EIGRP would allow the definition of stub areas, which allow for dynamic protocol connectivity while minimizing impact of convergence events on the stubs.

3. Yes, there are. The purpose of the teleworker architecture is to provide the "in-the-office" experience for remote workers and sites. To provide the same integrated services and applications available to central-site workers, it may be necessary to disable PAT and, at times, NAT. There are still a significant number of applications that do not support use across NAT/PAT boundaries. They are becoming fewer as time progresses, but alas, they are still out there.

   Also of note is the fact that any host that needs to be reached from the outside (for example, an FTP server) would need to use NAT as opposed to PAT.

4. The **import all** option will dynamically populate any DNS server, WINS server, or other options, such as TFTP server, into the database so that they can be provided to hosts on the subscriber network.

5. The dialer interface is a logical interface that will contain parameters necessary for connecting to the provider network. A physical interface is bound to a logical dialer interface through the use of the **pppoe-client dial-pool-number** *number* command. The pool number specified by the **pppoe-client dial-pool-number** *number* command must match the number configured in the **dialer pool** *number* command on the dialer interface to properly bind or associate them.

6. Among the tasks necessary to configure PPPoE are the following:

   - Ethernet/ATM interface configuration
   - Dialer interface configuration
   - PAT configuration
   - DHCP server services configuration
   - Static default route configuration

   Each of these tasks must be completed before the data connectivity will function properly.

7. **show pppoe session all**

8. When a router receives a DHCP request, it checks all configured DHCP pools for a network match. If one is found, an address will be assigned from the appropriate pool. If no match is found, no DHCP offer is made. To service the request, the router would require an additional pool configuration matching the network in question. Alternatively, if no pool is sharing its subnet, an IP helper address must be configured to forward the DHCP request to the appropriate server or no address will be allocated.

Chapter 6

"Do I Know This Already?"

1. A and B
2. B
3. D
4. B
5. B and D
6. B
7. A

Q&A

1. 32. 0–15 are reserved for use by the ITU and 16–31 are reserved for use by the ATM Forum.
2. The **dsl operating-mode auto** command sets the router to automatically detect the type of DSL modulation in use by the provider.
3. The LLC header provides the ability to transport multiple protocols over a single virtual circuit. It accomplishes this by providing an additional header and a protocol identifier for each CPCS-PDU payload.
4. The AAL5MUX encapsulation would be used. Each Layer 3 routed protocol would require a separate virtual circuit configuration. The following are some of the various reasons why this might be done:

   - Policy routing based on protocol. Each protocol can then be routed across the ATM network using different pathways.
   - Each protocol can be assigned a differing throughput rate across the ATM network based on protocol priority.

   Certainly there are additional possibilities. These are merely for example and to encourage additional contemplation of the possibilities.
5. The provider-facing interface is interface ATM 0/0, physically. Logically, the virtual-template interface is configured with the necessary Layer 3 component. The virtual-template IP address configuration notes that it should be a negotiated address. That is, the address will be provided via DHCP from the service provider.

6. A dynamic routing protocol must be configured on the router to ensure proper reachability. If no dynamic routing protocol is in use, static routes to all reachable networks must be manually added to the router configuration.
7. Yes, there is. In cases where a default route is critical, even in the event of the loss of reachability via the dynamic routing protocol, a static default route can be added with a high administrative distance. This is called a floating static route and will be used only as a route of last resort.
8. If an inside address does not match a definition of addresses eligible for NAT, according to the access list to which it is associated, the traffic will be forwarded based on an untranslated source address. No attempt will be made to process the address via NAT or PAT.

Chapter 7

"Do I Know This Already?"

1. C
2. B and C
3. A
4. C
5. B
6. D
7. B
8. B
9. A
10. B

Q&A

1. The PMD is the physical medium dependent sublayer. It is part of the physical layer and has the job of interfacing a particular media type, be it copper, fiber, air, or other. Its purpose is to perform physical layer framing functions. The order of the bits is specified by the technology in use. For example, T1 frame types specify a structure containing 24 time slots, each 8 bits in length. The resulting entity is a T1 frame and has an additional bit at the end to specify End of Frame. The structure goes on to specify structures for Superframe and Extended Superframe. This structure is replicated at the far end. Because both ends understand the structure, both can comprehend what is received.

The TC is the transmission convergence sublayer. This is also known as line code. This mechanism specifies the manner in which bits will be transmitted through changes in voltage, amplitude, frequency, polarity, phase, or other characteristics of the electrical or light signal.

2. There are many possible answers to this particular type of scenario. One course of action begins with a discussion with the teleworker.

   Ask probing questions such as, "What were you doing when the connection fell?" "Were any of the physical connections moved?" "Did you experience a power outage?" "Are all devices powered on?" "Have you installed any new software or devices on your PC or on the network itself?"

   All of these will lead to a bigger picture of the nature of the problem and the circumstances surrounding it. Once a state of satisfaction has been reached with all the answers, start simple. Have the user try to ping the local default gateway. If that works, move out one hop or perform a traceroute to the corporate VPN Concentrator and various well-known Internet sites. If no traffic is leaving the local subnet, begin by contacting the local service provider to verify that it is not experiencing an outage. This has the potential to save a great deal of time spent troubleshooting fruitlessly. With that done, begin troubleshooting at the physical layer, moving to the data link layer, and so on. If the DSL connection is training but no connectivity is restored, the provider should be re-engaged in the troubleshooting process.

3. Interface GigabitEthernet0/0 has been placed in a shutdown state as evident by the status administratively down. It has no IP address, a fact which would lead to the idea that the interface is not in use at this time.

4. Interface FastEthernet0/1/1 is in down/down state. Because it is an Ethernet interface, most likely nothing is plugged in to that interface or a bad cable is in use.

   Interface FastEthernet 0/1/8 is in up/down state and requires some further investigation. Because its status is up, it is evident that there is a Layer 1 connection. The line protocol is down, however, indicating a Layer 2 problem. According to the router prompt, this router seems to be a 2821, which is, in fact, the case. It contains an HWICD-9ESW PoE switch that takes up two of the HWIC slots. The ninth port (FastEthernet 0/1/8) is an uplink port that is not in use; however, it maintains up/down status.

   The remaining interfaces show to be up/up and are therefore happily in use and doing their jobs as designed.

5. A typical phone cord will usually suffice; however, twisted-pair cables are often preferred to ensure higher-quality connections. An RJ-11 standard connector is a six-pin connector. A typical phone cord uses only four wires, sometimes only two. The wires on a typical four-wire phone cord use a different color for each wire (red, green, black, and yellow). Typically, red/green are the inner pair and black/yellow are the outer pair.

Each pair of wires has one wire designated as *tip* and one designated as *ring*. The tip and ring wires for xDSL connections are pins 3 and 4, respectively, on the six-pin connector, or 2 and 3 on a four-pin connector.

Chapter 8

"Do I Know This Already?"

1. C
2. B
3. A
4. C
5. D
6. D
7. A
8. C

Q&A

1. When a packet arrives on the ingress interface, the packet destination network is read from the Layer 3 header. A routing table lookup is performed to determine whether or not a next-hop address and egress interface are known. If known, the packet is forwarded out the appropriate interface with the Layer 2 encapsulation appropriate to the media and framing type. It also may be necessary to perform address resolution for the next-hop address, thereby adding additional latency.
2. With process switching, every packet is treated identically with regard to routing table lookups. This is inefficient when considering multiple packets destined for the same destination networks. Fast switching keeps information pertinent to a particular destination, including needed address resolution information, in a cache where it can be queried rather than fully processing a routing table lookup. This allows the bypassing of the routing table and address resolution steps of the process for all but the first packet destined to a particular network. Subsequent packets can be essentially "rubber-stamped" and dispatched.
3. CEF switching information is stored in a FIB. All information in the FIB is copied from the routing table built by the local routing protocol running in the router. CEF updates are triggered by the local routing protocol reaction to convergence events. That is, when the local routing table is changed, CEF copies the changes and updates the FIB. CEF switching need

not maintain address resolution or encapsulation information because it maintains an adjacency table specifically for this purpose. The adjacency table is built at Layer 2 and linked to entries in the FIB.

4. An ordered set of labels attached to a packet header. Each label in the stack is independent of the others.

5. At times, an LSR immediately prior to the destination edge router will pop the label before sending the packet to the final edge LSR or node. This is known as a *penultimate hop pop* of the label. This is advantageous at times, because the final edge device does not need to perform both a label lookup and a network layer routing lookup once it figures out that it is the last hop prior to the destination.

6. Although both provide any-to-any connectivity between WAN sites, the Frame Relay connectivity requires an exponentially increasing number of circuits to accomplish what the MPLS connection can do with a single circuit. With Frame Relay, a 20-site deployment would require 190 circuits, whereas the MPLS equivalent would require only 20.

7. Full routing table lookup is performed only at the ingress edge LSR, at any device that receives an unlabeled packet, or at a device that does not have a label destination for a received labeled packet.

8. CEF-FIB updates are event triggered. There must be a change in the IP routing table for CEF-FIB update to be initiated.

Chapter 9

"Do I Know This Already?"

1. C
2. D
3. A
4. A
5. C
6. B
7. B
8. A
9. C
10. B

11. A and C
12. A
13. A
14. A

Q&A

1. The Control Plane maintains routing information and label information exchange between adjacent devices. Routing protocols such as OSPF, BGP, and others are part of the Control Plane.
2. The Data Plane forwards traffic based on destination addresses or labels. It is also known as the Forwarding Plane. The Data Plane functions based on the information constructed and provided by the Control Plane.
3. When a packet arrives at an LSR, the packet is checked for the inbound label. If no label exists, a label lookup can be performed for the destination. If no label entry exists in the local LFIB, a FIB lookup is done for that destination. The packet is then forwarded on to the next-hop based on FIB information. If no FIB entry exists, the packet is dropped.

   If the packet is indeed found to have a label on ingress, an LFIB lookup provides the needed outbound label and next-hop address information. The relabeled packet is forwarded to that next-hop.

   If a labeled packet is received and the LFIB shows no label entry for the outbound label, the label is popped and a FIB lookup is performed to determine next-hop information. This inefficiency can be eliminated by the use of PHP.
4. Label stacks are present when multiple labels are imposed on a single packet. The first label added is said to be the level 1 label and has its S-bit set to 1. The next label imposed is the level 2 label and has its S-bit set to 0, as will subsequently added labels.

   As a packet traverses the network, the LSR cares only about the highest-level label, ignoring the remainder of the stack.

   Additional labels can be added by MPLS-VPN tunnels or MPLS-TE tunnels or both. It is possible to traffic engineer an MPLS-VPN tunnel or route an MPLS-TE tunnel such that it will traverse an MPLS-VPN tunnel. It all comes down to the desired architecture and traffic flow. In such a case, one tunnel will logically ride inside the other, necessitating a label for each. Each tunnel need not ride inside the other to a common end. One may end well ahead of the other.

Each tunnel process will add its respective label to the stack. As the packet reaches the end of the first tunnel, the top label will be popped, thereby allowing the next label to be analyzed and the packet forwarded. Once the packet reaches the end of the next tunnel, the next label is popped. Once the final label is all that exists, the final edge LSR will pop the label and forward the packet based on FIB information, assuming PHP is not in effect.

5. The label itself is a four-octet (32-bit) structure. It includes the following fields:

   - Label—20 bits
   - Experimental CoS—3 bits
   - Bottom of Stack Indicator—1 bit
   - Time To Live (TTL)—8 bits

   The Label field itself can contain values between 0 and 1,048,575; however, the values from 0 to 15 are reserved for future use. Therefore, 16 is the first available label value.

   As noted, the second field is currently experimental. Its use is undefined in RFC 3031. Cisco uses this field for CoS using IP Precedence values.

   The Bottom-of-Stack bit is used when multiple MPLS labels are prepended for a single packet. The values for this field are 0 (false) and 1 (true). A value of 1 indicates that this particular label is the last label.

   The TTL field is just what it seems. It has a function identical to that of the TTL field in an IP header.

6. The label value imp-null denotes that this LSR is configured to perform a penultimate hop pop prior to forwarding the packet on to the next LSR, which will be the edge LSR. PHP allows the LSR immediately prior to the edge LSR to pop the label to save some processing resources for the edge LSR.

7. The term *frame mode MPLS* essentially denotes the use of MPLS with Ethernet-encapsulated or other frame-based-encapsulated interfaces. It does not include ATM-encapsulated interfaces. ATM uses cell mode MPLS and has a unique set of requirements due to the lack of a flexible framing structure.

8. A few different scenarios are possible with an edge LSR forwarding decision:

   - A received packet can be forwarded as a normal IP packet, based on the destination IP address. In this case, the outbound interface is not MPLS enabled.
   - A received packet can be forwarded as an MPLS labeled packet based on a destination IP address. In this case, the outbound interface is MPLS enabled.

- A received labeled packet is received and forwarded based solely on the label. The inbound label is examined and swapped based on the LFIB so that the packet can be dispatched to the next MPLS hop.
- A received labeled packet is forwarded based on the label; however, the LFIB shows that this edge LSR is the egress MPLS edge. Therefore, the label is popped and the packet routed normally.

  If a received labeled packet is dropped, this is symptomatic of a lack of an LFIB entry, even if the destination exists in the routing table.

  Similarly, a received IP packet might be dropped if there is no routing entry in the routing table, even if the entry does exist in the LFIB for the destination.

9. MPLS label switching relies only on labels. While the construction of the label table involves the independent routing tables of various protocols traversing the network, the actual switch process cares only about label-in, label-out, next-hop, and outbound interface. At no time does the MPLS label switching process rely on Layer 3 information.

Chapter 10

"Do I Know This Already?"

1. A
2. B
3. A
4. B
5. B
6. B

Q&A

1. CEF uses the FIB rather than a route cache to eliminate cache maintenance and fast/process switching of packets.

   The FIB and adjacency tables provide the operational base for CEF. CEF uses the FIB to make IP destination switching decisions. The adjacency table keeps a database of Layer 2 information, including Layer 2 next-hop information. CEF uses the adjacency table to prepend Layer 2 information to outbound traffic. This avoids any need for ARP or other Layer 2/3 resolution processes.

2. TDP is a Cisco proprietary label distribution protocol, whereas LDP is a standardized label distribution protocol. A mixed environment might be encountered during times of migration from TDP to LDP or in a multivendor environment.

   In a migration situation, it is prudent to carefully plan the migration from one to the other. Both can be enabled simultaneously or a flash cut from TDP to LDP can be done.

   In cases of multivendor deployments, a simple answer might be to remedy that issue and deploy all Cisco equipment. More realistically, a solution might be to enable both protocols on MPLS interfaces to accommodate both TDP and LDP. Also, a migration strategy could easily be put in place to migrate the Cisco equipment to LDP altogether and eliminate any dependence on TDP.

3. The MTU must be adjusted on all interfaces of all devices in the LSP that will be transporting MPLS traffic, including routers and switches. The size must be set to accommodate the technologies in use. For example, if label stacking is in use, then the MTU must be adjusted to accommodate the entire label stack size at 4 bytes per label.

4. Labels in the range of 0 to 15 are reserved values. The value 3 signifies that the outlabel is implicit null or **imp-null** in **show** command output. This means that the label is to be popped before forwarding the packet to the next-hop device.

Chapter 11

"Do I Know This Already?"

1. A
2. B
3. B
4. A
5. C
6. B
7. C
8. C
9. B
10. C
11. B
12. B

Q&A

1. A Layer 2 overlay VPN is synonymous with what is traditionally known as WAN connectivity. Technologies such as Frame Relay, ATM, SMDS, and more are Layer 2 VPN overlays. The provider has no involvement in the routing processes of a Layer 2 overlay VPN. Typical topologies include full mesh, partial mesh, and hub-and-spoke deployments.

2. A peer-to-peer VPN is Layer 3 aware. The service provider conveys routing information from CE router to CE router. Peer-to-peer VPNs offer optimal routing redundancy and full mesh capabilities with a single connection to the P network.

3. The most overlooked potential issue is a single point of failure between the CE and PE. In many cases, a single access point is available to a particular building. A single fiber cut can reduce even the most ornate redundancy scheme to nothing if all of those fiber strands share a single entry/exit point at the premises.

   Routing loops are also a potential issue. With MPLS VPNs, the provider and customer need to work together to eliminate them. It is necessary to ensure that routes advertised via one circuit are not redistributed out to the PE and then right back in via the redundant circuit to the CE. This will cause a significant routing loop. Split horizon will not stop it, because the update is not received via the interface through which it was initially sent.

4. Router A is running an IGP across the connection to the PE router. The 192.168.1.0/24 prefix is advertised across that link and entered into the VRF in the ingress PE router. That prefix is prepended with an RD to create a VPNv4 prefix and then appended with a VPN-specific export RT prior to being propagated to the egress PE by an MPBGP neighbor relationship between the two PE routers. Upon receipt of the update, the import RT is examined to determine VPN membership. The route is then redistributed into the appropriate VRF and then on to the CE router via the customer IGP.

5. The ICMP packet enters CE-B, where a routing table lookup is performed. The result of the lookup dictates that the interface connected to the PE router is the outbound interface and next-hop address. The packet is encapsulated inside an appropriate frame for the media type and transmitted to the ingress PE.

   The ingress PE performs a routing table lookup in the VRF associated with this customer and determines that the route to the 192.168.1.0/24 network is known as being advertised by the egress PE through MPBGP.

   The PE router imposes a VPN label appropriate to the customer-specific VPN instance. An additional label, an LDP label, specific to the LSP that will get the packet to the egress PE is also imposed.

   Each P router in the LSP performs a label lookup and swap based on only the LDP label (that is, the top label in the stack) to forward the packet.

When the egress PE is reached, a label lookup occurs, resulting in no outbound label entry. Therefore, the top label is popped, revealing the VPN-specific label. This label contains information regarding the VRF containing the customer routes. A routing table lookup is performed in the VRF, finding that the outbound interface is specified. This means that the next-hop device is the CE; therefore the label is popped and the packet is routed to the next-hop address of the CE router and on to the 192.168.1.5 host.

With that accomplished, the path is successfully traced from CE to shining CE.

Chapter 12

"Do I Know This Already?"

1. C, D, E
2. C
3. A, C, D
4. A, E
5. C
6. C, D
7. A, D
8. B
9. B, E
10. E
11. A, B, E
12. C
13. B
14. C

Q&A

1. Data integrity, data confidentiality, anti-replay, and origin authentication are the features of IPsec.
2. IKE, ESP, and AH
3. Data confidentiality is the use of encryption to scramble data as it travels across an insecure media. Data integrity verifies that the data was not modified or altered during transit.

4. Data authentication and data integrity are performed by an HMAC.
5. With IPsec transport mode, the IPsec headers are inserted into the IP packet after the IP header. Thus, the original IP header is exposed during transit. In tunnel mode, a new IP header is applied to the packet. This new header uses the tunnel end points as the source and destination IP addresses. The entire original packet, including the original IP header, is protected in tunnel mode.
6. ESP uses IP protocol 50. AH uses IP protocol 51. And IKE uses TCP port 500.
7. A one-time password is good for only one IPsec session. It is typically implemented as a PIN or a TAN. The discovery of a one-time password would prove useless to anyone.
8. The use of username/password and preshared keys both must be preconfigured into the IPsec endpoints prior to the IPsec tunnel establishment.
9. IKE dynamically exchanges keys for secure communications
10. IKE phase 1.5.
11. IKE uses the bidirectional SA to exchange all IPsec parameters and keys.
12. Main mode uses six messages during IKE phase 2 to exchange security parameters, exchange public keys, and authenticate each end. If main mode is selected, aggressive mode is not used.

    Aggressive mode is an abbreviated version of main mode. The six packets of main mode are condensed into three messages. When aggressive mode is used, main mode is not.

    Quick mode negotiates the IPsec SAs during IKE phase 2. This mode runs after either main mode or aggressive mode.
13. Dead peer detection (DPD), NAT traversal, mode configuration, and Xauth are additional IKE functions.
14. A single shared secret key is used for bidirectional encryption, and it is best used for bulk encryption requirements.
15. RSA is an asymmetric encryption algorithm, while Diffie-Hellman is an asymmetric key exchange protocol.
16. RA can handle enrollment requests.
17. Digital certificates
18. Both LDAP and HTTP are examples of distribution mechanisms.

Chapter 13

"Do I Know This Already?"

1. C
2. B and C
3. C and E
4. A
5. E
6. A, B, D
7. B
8. C
9. A, B, C, D, E
10. A, C, D
11. B, C, D
12. E
13. A and B
14. B
15. B and C
16. A and D
17. A, B, E
18. C
19. A, B, C
20. D
21. C and D
22. C and E
23. C
24. B

Q&A

1. IKE phase 2
2. An IPsec tunnel is terminated when a preconfigured amount of data has gone through the tunnel or when the tunnel has been operational for a particular amount of time.
3. It is sent out the interface to its intended destination, but not through the VPN.
4. Extended IP ACL
5. Main mode uses the third and fourth packets for Diffie-Hellman, while aggressive mode uses the first two packets.
6. The IPsec process is halted.
7. IKE phase 2
8. Quick mode
9. **crypto ipsec transform-set**
10. **crypto isakmp key**
11. Security Policy Database (SPD)
12. Yes, an IPsec tunnel can expire even if there is traffic flowing through it. In this case, a new tunnel is typically established before the old one is torn down. However, data flow is interrupted until the new IPsec tunnel is established.
13. To prevent weaker sets from being agreed upon between peers
14. IKE phase 1
15. **crypto ipsec transform-set test esp-aes esp-sha-hmac**
16. Remote peer, interesting traffic, and IPsec transform set
17. **access-list 101 permit 172.16.5.0 0.0.0.255 10.1.2.0 0.0.255.255**
18. **crypto map test**
19. Protocol 51
20. Home, Configure, Monitor, Refresh, Save, Search, and Help
21. Site-to-Site VPN, Easy VPN Remote, Easy VPN Server, and Dynamic Multipoint VPN wizards
22. The interface on the local router used to source the IPsec VPN
23. Preshared keys and digital certificates
24. You might choose to send traffic from a single IP address or small subnet in the clear, but send the remainder of the larger subnet through the IPsec VPN.

25. Traffic that does not match the ACL is sent in the clear.
26. The encrypted and decrypted packet counts will be greater than zero, and should increase with successive show screens.

Chapter 14

"Do I Know This Already?"

1. C
2. B, C
3. C
4. B
5. E
6. B, C, E
7. C
8. D
9. A, B
10. A
11. C, D
12. A, B, C
13. A, B, C
14. B, C
15. D

Q&A

1. GRE offers basic encryption, but the encryption key is carried within the packet, which minimizes the effectiveness.
2. Checksum, encryption, and sequencing
3. The key carried in the GRE packet can be used to uniquely identify different tunnels that are set up between the same two sites.
4. The tunnel source at one end is the tunnel destination on the other, and vice versa.

5. Both tunnel and transport modes are possible with GRE over IPsec.
6. GRE provides the ability to exchange dynamic routing information, whereas IPsec alone cannot.
7. Click the **Configure** button, click the **VPN** button, click the **Site-to-Site VPN** option, click the **Create Site to Site VPN** tab, click the **Create a secure GRE tunnel (GRE over IPSec)** radio button, and click **Launch the selected task**.
8. Source interface/IP address, destination IP address, internal IP address/subnet mask, (optional) MTU path discovery
9. Source interface/IP address
10. VPN authentication information (pre-shared keys or digital certificates), IKE proposals, and IPsec transform sets
11. Static routes, RIP, OSPF, and EIGRP
12. 1
13. Either OSPF or EIGRP
14. Go back into the wizard to modify the configuration (click **<Back**), finish the wizard (click **Finish**), and optionally test the GRE over IPsec connection when the wizard is finished

Chapter 15

"Do I Know This Already?"

1. A, C, D, E
2. A, B, D
3. A, B, E
4. B, D, E
5. B
6. D
7. B and C
8. C
9. A
10. B
11. C

12. B and E
13. B and E

Q&A

1. Access link failure, remote peer failure, device failure, and path failure
2. The use of multiple interfaces, multiple interface cards, or multiple endpoint devices
3. DPD, the use of an IGP within GRE over IPsec tunnels, and HSRP
4. On-demand
5. The excessive overhead of encrypting the DPD keepalive messages
6. **crypto isakmp keepalive** *seconds* [*retries*] [**periodic** | **on-demand**]
7. OSPF or EIGRP
8. For a particular HSRP group, the HSRP active router handles all traffic sent to the virtual IP/MAC addresses, while the HSRP standby router only works when the active router fails.
9. The VPN drops and is reestablished to the same virtual IP address.
10. HSRP and SSO
11. The IGP metrics must be configured such that the WAN connection is preferred if it is available.
12. A floating static route is a static route that has a high administrative distance, and is only used if the path is no longer available from dynamic routing updates.

Chapter 16

"Do I Know This Already?"

1. A
2. A
3. B
4. B
5. B
6. B
7. B

8. C
9. B
10. A
11. A
12. C

Q&A

1. Stage 1 is Group Level Authentication, which represents a portion of the channel creation process. During this stage, two types of authentication can be used, either preshared keys or digital certificates.

   Stage 2 of the authentication is known as Extended Authentication, or Xauth. The remote side of the connection submits a username and password to the central site VPN device. This is the same method used when a Cisco VPN Software Client is prompted for a username and password to activate a VPN tunnel. However, in this case, a user is not authenticated to the central site. Instead, the Easy VPN Remote Router itself is authenticated. Although Xauth is optional, it is typically used to improve security. When the Xauth is successfully completed and the VPN tunnel is created, all PCs behind the Easy VPN Remote Router can use the connection.

2. The VPN Client initiates IKE phase 1.

   The VPN Client establishes an ISAKMP SA.

   The Easy VPN Server accepts the SA proposal.

   The Easy VPN Server initiates user authentication.

   Mode configuration begins.

   The Reverse Route Injection (RRI) process begins.

   IPsec quick mode completes the connection.

3. Extended Authentication, or Xauth, allows the remote side of a connection to submit a username and password to the central site VPN device. However, in this case, a user is not authenticated to the central site. Instead, the Easy VPN Remote Router, itself, is authenticated. Although Xauth is optional, it is typically used to improve security. Once the Xauth is successfully completed and the VPN tunnel is created, all PCs behind the Easy VPN Remote Router can use the connection.

4. Reverse Route Injection (RRI) is the process of injecting a static route into the Interior Gateway Protocol (IGP) routing table. This static route points to the client's destination network. This is useful when per-client static IP addressing is used with VPN Clients rather than per-VPN address pools.

   Without the RRI, there would be no path for return traffic to reach the VPN client.

5. Options can be configured for all users within the group membership, including

   Group Name

   Pre-Shared Key

   Pool Information

   DNS/WINS Server

   Split Tunneling

   Backup Servers

   Personal Firewall information

   Local LAN Access while connected

   Maximum Number of Group Connections

   Xauth Options such as Group Lock and Saved Password capability

   Maximum Number of Logins Per User

6. The choice of transform set is made by a progressive trial-and-error method. The configured transform sets are proposed in order of entry until both client and server agrees upon one of them. When a match is made, processing of transform sets ceases. This means that additional transform sets below the one agreed upon will not be processed.

7. **Client**—Specifies that NAT or PAT will be used so that end stations at the remote end of the VPN tunnel do not use IP addresses in the space of the destination server. The needed security associations (SA) are created automatically for IP addresses assigned to remote hosts.

   Network Extension—Specifies that remote-end hosts use IP addresses that are fully routable and reachable by the destination network over the tunnel connection so that they form a single logical network. In such cases, PAT is not used, to allow remote-end PCs direct access to destination network services and applications.

   Network Extension Plus—Identical to Network Extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec SAs for this IP address are automatically created.

8. Cisco Easy VPN Remote does not support transform sets providing encryption without authentication or those providing authentication without encryption. Both encryption and authentication must be represented.

Chapter 17

"Do I Know This Already?"

1. A
2. B
3. A
4. D
5. B
6. C

Q&A

1. Once the VPN Client has been launched, click the **New** button. This opens the Create New VPN Connection Entry dialog box. This dialog box requires the configuration of the Connection **Entry CorporateVPN** as provided in the scenario given in the question. The entry of a description is optional.

   In the Host field, enter **vpnserver1.mycompany.com**, the specified VPN server.

   The Authentication tab is already active by default when a new connection is created. Under the Name field, enter the username **RoadWarrior**. Enter the password **cisco** and then confirmation of the password **cisco** in the respective fields. Because the certificate has already been provided, no further information is needed on this tab.

   On the Transport tab, check **Enable Transparent Tunneling**, as specified in the scenario. Click the **IPsec over UDP (NAT/PAT)** radio button. No other options need be configured on this tab.

   On the Backup Servers tab, check **Enable Backup Servers** and add an entry for **vpnserver2.mycompany.com** as specified. Because it is the only backup server, no reordering of connections is needed.

   Because there is no information specified in the scenario's parameters, no dialup information needs to be configured on the Dial-Up tab. Click the **Save** button at the bottom of the Create New VPN Connection Entry dialog box to enact all changes. This connection entry is ready for use.

2. IPsec over UDP typically uses UDP port 4500 to transport IPsec packets through a NAT/PAT device, but the port can be negotiated. IPsec over TCP uses a preconfigured port on both ends and can be used to send IPsec packets through a stateful firewall.
3. The primary server could be congested or inoperable. If only a single server is configured and it is unavailable, the VPN connection will fail. Backup servers enable the VPN client to step through a list of IP addresses in an attempt to establish a successful VPN connection.
4. Local LAN Access permits access to network resources on the local subnet. Without this option, all traffic is sent through the VPN to the central site. Local resources, such as printers and file shares, would not be accessible. Both the client and the VPN central server must be configured for Local LAN Access.
5. The Group Authentication method requires a username and password to be entered. Both Mutual Group Authentication and Certificate Authentication require the use of certificates for authentication.
6. Although a large majority of devices are accessible via the Internet today, not all are. Some require the use of a dial-up connection to establish connectivity, and thus to create a VPN connection.

Chapter 18

"Do I Know This Already?"

1. E
2. A and D
3. B and D
4. B, C, E
5. B and D
6. B and E
7. C
8. A and C
9. B and C
10. C and D

Q&A

1. CDP should either be completely disabled or disabled where it is not needed, such as external interfaces.
2. BOOTP, MOP, and PAD
3. ICMP redirects, ICMP unreachables, and ICMP mask replies
4. Gratuitous ARP and proxy ARP
5. The sheer volume of Cisco IOS commands makes it easy to miss an important feature and possibly leave the router vulnerable.
6. AutoSecure offers either an automated or interactive means of securing a Cisco IOS router. In automated mode, various features are secured without user input. In interactive mode, the user can select which features need to be secured.
7. **auto secure no-interact**
8. The **full** option causes all options to be examined. This is the default behavior.
9. 1. Identify the outside interface(s). 2. Secure the management plane. 3. Create a security banner. 4. Configure passwords, AAA, and SSH. 5. Secure the interfaces. 6. Secure the forwarding plane.
10. Either restore the manually saved pre-AutoSecure configuration, or execute **configure replace flash:pre_autosec.cfg** if using Cisco IOS Software Release 12.3(8) or later.
11. SDM offers the Security Audit and the One-Step Lockdown wizards.
12. The user first selects the inside/outside interface. Next, the user selects the security parameters to be corrected. Next, the user can create the appropriate configurations to correct the vulnerabilities. And finally, the user can deliver the configurations to the router.
13. The user is only allowed to execute the One-Step Lockdown wizard. There are no user-accessible steps within the wizard.

Chapter 19

"Do I Know This Already?"

1. C
2. C and E
3. B and C
4. B, C, F

5. A, B, E
6. D
7. E
8. B
9. A
10. C
11. D
12. A, C, E
13. E
14. C
15. A
16. A and D
17. B
18. E
19. B

Q&A

1. The console port, the aux port, and the vty ports
2. A Cisco router can be configured via the CLI, which is available on the console and aux ports, and via a Telnet or SSH session. The router can also be configured via SDM via HTTP and HTTPS. SNMP can be used to configure and poll the router.
3. Enforce a minimum length, require a mix of characters, do not permit dictionary words, and force password changes often.
4. Passwords in a Cisco IOS device can be anywhere between 1 and 25 characters (the longer the better), the first character cannot be a space or number, and the password may contain any character (including spaces).
5. IOS imposes a 15-second login delay and logs the failed attempt to access the router.
6. *seconds* defines the login delay. *failed-attempts* defines the number of consecutive login failures. *watch-period* is the time period that *failed-attempts* must occur to impose the *seconds* penalty.

7. Setup does not permit these two passwords to match, and continues to ask for an enable password until a unique one is entered.
8. The enable secret password is encrypted with an MD5 one-way hash, which is considered virtually unbreakable. The enable password is initially stored in plaintext, and at best can be encrypted with the Vigenere cipher, which is known to be very weak.
9. The **login** command enables password checking, which forces the use of the configured password. Without this command, any configured password would be ignored during a login attempt.
10. An access class allows only specific IP addresses or subnets to access the router via Telnet or SSH. This prevents any device on the network from attempting to access the router.
11. The **exec-timer** disconnects a line after a determined amount of time. This prevents an unoccupied terminal from offering access into the router.
12. Nothing. This only forces new passwords to be a minimum of 15 characters.
13. To restore passwords to plaintext, password encryption must be disabled (**no service password-encryption**) and the passwords must be entered again.
14. A banner does not provide any security mechanisms to a router, but it offers warnings to those who connect to the router.
15. The command **login local** must be applied to the lines to use the username database.
16. Level 0 is user mode, level 15 is privileged mode, and levels 1 to 14 are defined by the user.
17. Each IOS command can be used only one time across all privilege levels. The same IOS command can be used in all IOS views. Also, privilege levels do not offer command isolation, such as a particular interface. IOS views offer this level of granularity.
18. A superview is a collection of views. Many individual views can be combined into a superview. However, no individual IOS commands may be configured in a superview.
19. **no service password-recovery** prevents access to ROMMON mode during the router's boot cycle. ROMMON can be used to perform password recovery and access the router without knowing the passwords. But it can also be used to recover a lost Cisco IOS image. Once ROMMON is disabled, there is no way to access the router during boot.

Chapter 20

"Do I Know This Already?"

1. D
2. B

3. D
4. A
5. D
6. D
7. D
8. B
9. C
10. A
11. D
12. C
13. B

Q&A

1. There are many consequences. Among these are
   - Scalability
   - Ability to see when servers have failed
   - Using different servers or technologies for authentication, authorization, and accounting
   - Individual command level control
   - Multiprotocol support
   - Interoperability
2. You must have authentication running before you can enable accounting. It is not possible to track a user until you are sure that the user is who they claim to be.
3. This scenario appears to be perfect for TACACS+. RADIUS is known to suffer, mainly because of its UDP protocol reliance, when deployed in large environments. Although RADIUS has been used successfully in large environments, TACACS+ tends to scale more easily than will RADIUS.
4. This user probably has not been given authority to access the vty lines. Alternatively, the user might not even be in the database.

5. This is almost certainly an issue of privilege level for the command. Check the user's privilege level for the affected commands and change them, if necessary, with the **aaa authorization** command.
6. The **aaa accounting** command allows you to use the **stop** parameter instead of the **start-stop** parameter to track only the last access time.
7. You should look at the **tacacs-server host** command because this allows you to change the default timeout.

Chapter 21

"Do I Know This Already?"

1. B
2. A and B
3. D
4. D
5. B
6. F
7. C
8. E
9. C and D
10. C and D
11. B
12. B and C
13. C

Q&A

1. Place each of the servers on a separate DMZ. This allows for protection of the corporate network and ensures that compromise of a single server does not affect the other servers.
2. Packet filtering, which uses the IP address and/or port number to allow access; application layer gateway, which works as a proxy server, preventing the user from direct access to the server; and stateful packet filtering, which uses dynamic ACLS and tracks the state of connections to determine access

3. The Cisco IOS Firewall recognizes many different protocols, including BGP, FTP, RADIUS, SNMP, and HTTP/HTTPS.
4. UDP is a connectionless protocol. Therefore, there is no "session" as in a connection-oriented protocol such as FTP. Instead of relying on connection status, the firewall uses timeouts to determine whether a session is still active.
5. This is the stateful packet filter.
6. Because you have such sensitive data on this server, you should never allow direct access to the server. We recommend placing this server on its own DMZ and using an ALG for access to the server.
7. Cisco IOS IPS allows you to monitor a single protocol and log all instances of that specific protocol.
8. This server is using stateful packet filtering, which dynamically changes the ACLs.
9. An Authentication Proxy Server is used to provide proxy services related to AAA.

Chapter 22

"Do I Know This Already?"

1. C
2. D
3. B
4. A
5. B
6. B

> **NOTE** The Basic Firewall Wizard may be used on routers with multiple untrusted interfaces. However, the Basic Firewall Wizard will only allow you to configure a single untrusted interface and does not allow you to configure a DMZ.

7. C
8. C
9. B

Q&A

1. There are many advantages, some of which are as follows:
   - Speed of configuration
   - Graphical interface allows you to see what you are doing
   - Less chance of forgetting a critical configuration item
   - No need to remember the CLI syntax
2. Generally, the Basic Firewall Wizard should be used when there is only a single untrusted network and no DMZ. When you have a DMZ or DMZs or multiple untrusted networks, you should use the Advanced version. Some people choose to always use the Advanced version to see all the options that are available.
3. The steps are as follows:

   Step 1 **Choose the interface**—Decide which interface(s) to be protected by the ACL and IP inspection and whether you should apply the ACL and IP inspection going into or out of the interface.

   Step 2 **Configure an IP ACL for that interface**—Create an extended access list.

   Step 3 **Define the inspection rules**—Decide which protocols need to be watched.

   Step 4 **Apply the inspection rules and the ACL to the interface**—Apply the ACL and the rule to the interface.

   Step 5 **Verify**—Use **show** and **debug** commands.
4. The default timeouts are designed for the "average" network. Because no two networks are identical, every one has different requirements. The timeouts may be changed depending on the needs and usage of a network. For example, some networks have a large number of FTP files that can be accessed by the general public. In this case, the time between alerts regarding FTP will be raised because the network could become inundated by the amount of data we receive. Alternatively, we may have a network where the FTP files should be considered secret. In this case, we would lower the time between reports to give us more rapid information.

Chapter 23

"Do I Know This Already?"

1. C
2. B
3. B, D, E
4. A
5. B, D, E
6. A

7. B
8. D
9. A, C, E
10. C

Q&A

1. Intrusion detection and intrusion prevention systems
2. An IDS sits outside the packet flow and examines a copy of network traffic. If it finds a problem, it sends an alert and can configure network devices to stop further packets. An IPS sits in the packet flow, and when it finds a problem, it can stop the offending packets immediately.
3. A single network IDS or IPS can monitor traffic destined for multiple hosts. It cannot inspect encrypted traffic, nor asses the success or failure of an attack. A host-based IDS or IPS monitors behavior on an individual device. Cisco Security Agent is an example of this.
4. Signature-based, policy-based, and anomaly-based,
5. The policy-based mechanism may need access to such a database that keeps up-to-date information.
6. Exploit, connection, string, and DoS
7. The system may send an alarm, drop the packet, reset the connection, block traffic from a particular source IP address, block traffic on the connection in question, or any combination of the these.
8. **ip ips sdf location** *name*
9. Inbound, to scan packets before they enter the network device
10. **show ip ips configuration**
11. The Create IPS tab, which is used to create a new IPS rule from scratch, and the Edit IPS tab, which is used to edit existing IPS configurations

Index

A

B

C

D

E

F

G

H - I

J - K - L

M

N

O - P

Q - R

S

T

U - V

W

X - Y - Z