A

APPENDIX

NETWORK + EXAM SUPPLEMENT

1.0 NETWORK ARCHITECTURE

1.1 Explain the functions and applications of various network devices

HIDS—Host-based intrusion detection system. This is an intrusion detection system that monitors the computer system for changes such as system file modifications, changes to the registry, file changes, and system logs. HIDS software packages are configured to prevent malicious activity on the host system, and if an unauthorized change or activity is detected, an alert is issued. Based on policy settings, the central server could be notified or the activity could be blocked.

IDS/IPS—Intrusion detection system/intrusion prevention system. Intrusion detection systems are designed to monitor both inbound and outbound data traffic and report any suspicious activity that could indicate an attack. The IDS system identifies misuse or potential attacks by matching the data packets against known signatures that have been classified as bad. IDS solutions are available in terms of shareware and open source programs, to more expensive vendor software solutions. In some cases, an IDS solution might be in the form of both a software package and a hardware appliance installed at various places within your network.

An intrusion prevention system (IPS) monitors and analyzes the network traffic. In real time, it identifies misuse and any anomaly on the network. The IPS detects a misuse intrusion by matching the network packets with its IPS signatures for known attacks or activities classified as bad. The network anomaly can be detected by building up a profile of the system being monitored and detecting significant deviations from this profile. The IPS has the capability to stop or prevent malicious attacks that it detects by interacting with the firewall.

Content filter (also known as information filtering)**—**Many organizations have strict policies on how their users can use the network. Web traffic is usually one of the first things to be monitored and filtered, and a content filter appliance is designed to do just that. In the K-12 school environment, web filtering is critical. K-12 school districts are required by law to implement filtering to block adult, illegal, or offensive content from minors. The law is known as the Children's Internet Protection Act (CIPA). A content filter appliance has a database containing inappropriate websites. A web filter appliance monitors the web traffic both via HTTP and HTTPS and matches it against the database. If an inappropriate website is detected, either it is discarded or the user is redirected to a security web page for further action. The web filter appliance gets its database updated continually. Also, there is always an option for a network administrator to manually mark a website as inappropriate.

Packet shaper—This is a device that sits between the campus network and the outside network. The device is set up so that all data traffic, incoming and outgoing, passes through it. The packet shaper box is configured with a set of "rules" used to prioritize data traffic. This is important when it comes to better managing your network's data bandwidth. The *packet shaper* can be used to set rules to limit download traffic off the Internet. It can also be used to make sure that applications such as VoIP are given a higher priority so that the operation and quality of service are not affected.

VPN concentrator—The purpose of the VPN concentrator is to manage a secure VPN connection. The VPN concentrator is essentially an advanced router enabled to handle multiple connections (tunnels) into a network. A tunnel is created by an encapsulation technique, which encapsulates the data inside a known protocol (IP) agreed upon by the two endpoints. A tunnel creates a virtual *circuit* between the two endpoints and makes the connection appear like a dedicated connection even though it spans the Internet infrastructure. Two types of VPNs commonly used today are

- **Remote access VPN (Host-to-site)**: A remote access VPN is used to facilitate network access for users in remote office networks or for remote users who travel a lot and need access to the network. The client usually initiates this type of VPN connection.
- **Site-to-site VPN**: A site-to-site VPN is used to create a virtual link from one site to the other. It essentially replaces the traditional WAN-type connection used in connecting typical sites. This type of VPN requires network hardware like a router or a firewall to create and maintain the connection.

You might also see mentioned a *host-to-host VPN,* which deals with a single connection between two machines. The machines could be using VPN software or hardware for establishing the VPN connection.

In regards to tunneling, one of the original tunneling protocols is Generic Routing Encapsulation (*GRE*). GRE was developed by Cisco in 1994 and is still being used today. GRE is commonly used as a site-to-site VPN solution because of its simplicity and versatility. It is the only tunneling protocol that can encapsulate up to 20 types of protocols. Other protocols include the Point-to-Point Tunneling Protocol (*PPTP*) developed jointly by Microsoft, 3Com, and Alcatel-Lucent in 1996. Layer 2 Forwarding Protocol (*L2F*) was developed by Cisco around the same time as PPTP. L2F does not require any VPN client software. An L2F connection is intended to be done by L2F hardware. Layer 2 Tunneling Protocol (*L2TP*) was developed by the Internet Engineering Task Force (IETF) in 1999. L2TP was created with the intention of merging two incompatible proprietary tunneling protocols, PPTP and L2F. L2TP is considered to be an enhancement of the two previous protocols. L2TP does not require a specific hardware.

1.2 Compare and contrast the use of networking services and applications

Network Controllers—The purpose of this device is to authenticate users and network devices using Kerberos in domain environments. Kerberos is a network authentication protocol for client/server applications. In non-domain environments, certificates are required for authentication. Associated with the Network Controller is the API (Application Programming Interface). The API is defined in southbound and northbound applications. Southbound applications allow a controller to define switches while the northbound applications gather information used to monitor and configure the network.

1.3 Install and configure the following networking services/ applications

Reservations—This is used to ensure that a DHCP client always receives the same IP address when it reconnects.

Scopes—This is a grouping of IP addresses that use the DHCP (Dynamic Host Control Protocol) service for a group of computers located on a subnet.

SNAT—This stands for Source Network Address Translation, which enables private network data traffic to go out to the Internet. SNAT enables multiple VMs so they can reach the public network through a single gateway public IP address.

DNAT—This stands for Destination Network Address Translation. DNAT allows any host on the “outside” of the network to get to a single host on the “inside” of the network.

Reverse proxy—A *proxy server* is used by clients to communicate with secure systems using a proxy. The client gets access to the network via the proxy server. This step is used to authenticate the user, establish the session, and set policies. The client must connect to the proxy server to connect to resources outside the network. In reverse proxy, the client computer is outside the network trying to gain access to the server inside the network. The client computer issues the request for website information, which is sent to the proxy. The proxy obtains information from the website and sends it to the client. Its function is to provide control for traffic flow from the server to the client.

Dynamic DNS—This is a method where name server and Domain Name Server are automatically updated.

1.4 Explain the characteristics and benefits of various WAN technologies

CWDM—This stands for coarse wavelength division multiplexing. This is a technique for combining multiple signals on laser beams for transmission. The signals are at different wavelengths but have less total wavelengths compared to dense wavelength division multiplexing (DWDM).

MPLS—This is Multiprotocol Label Switching, which is a data-carrying service for telecommunication networks that route data from one network node to the next based on labels for short path rather than long network addresses.

1.5 Install and properly terminate various cable types and connectors using appropriate tools

UTP coupler—This is a small device used to connect two UTP cables. It is also called an inline coupler. UTP couplers can be used to couple CAT5 and RJ-11 phone lines but can introduce signal degradation.

BNC connectors—BNC stands for Bayonet Neill-Concelman, which is a quick connector for coaxial cable. This was a common connector used with ThinNet Ethernet cabling.

Fiber coupler—These couplers come in a variety of styles that support single-mode and multimode fibers. These devices allow a single fiber to be split into two outputs, and multiple input fibers can be combined into one output fiber.

APC versus UPC—APC stands for angled physical contact and UPC stands for ultra physical contact. The difference between the two types of connectors is the fiber endface. APC has a polished endface at an 8-degree angle. UPC endfaces are polished with no angle. APC and UPC connectors are easily identified by their color. APC adapters are green, and UPC adapters are blue.

Fiber to coaxial—This device is used to convert an optical signal carried over fiber to an electrical signal carried over coaxial cable. A typical application for this is coupling cabling that carries digital optical signals to a digital coaxial cable.

PVC versus Plenum—PVC cable is a common plastic cable insulation or jacket that consists of polyvinyl chloride chemical compounds that emit toxic smoke when burned. Plenum rated cable has special coating that emits less toxic smoke when burned.

1.6 Differentiate between common network topologies

Hybrid—This is simply a combination of two or more network topologies. For example, a STAR and a BUS topology combination.

1.7 Differentiate between network infrastructure implementations

NFC—This stands for near field communication. NFC is a set of communication protocols used to enable two electronic devices to communicate. A typical NFC device is a smartphone, and NFC smartphones can establish communication if they are within 4 cm of each other. Applications of NFC include reading electronic tags or even making payments.

SCADA/ICS—SCADA stands for supervisory control and data acquisition. ICS stands for industrial control systems. Applications for SCADA systems include electrical power systems, railroads, and pipelines. ICS systems are computer-based systems associated with the monitoring and control of industrial processes. The difference between SCADA and ICS systems is SCADA systems are large systems or systems that extend over many miles or multiple sites. Industrial control systems are designed to operate and monitor the critical industrial infrastructure.

ICS server—Industrial control systems servers are designed to withstand the harsh environment of industry. The physical cabinet housing the server has a heavier enclosure, improved electronics, and a high-watt power supply. The operating systems for ICS servers are typically more robust to better protect the system from cyber threats. Typical components that can be included in a control system configuration are

- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)
- (SCADA) systems
- Control server
- Master Terminal Unit (MTU)
- Remote Terminal Unit (RTU)
- Intelligent Electronic Devices (IED)
- Data Historian
- Input/Output (IO) server

DCS/closed circuit—Distributed Control System (DCS) is a system that has multiple subsystem controllers geographically dispersed throughout the network. In modern DCS systems, the local controllers connect to the ICS server. A human interacts with the controllers through what is called a human machine interface (HMI). DCS systems have been the primary solution for automation in a process environment; however, many PLC (Programmable Logic Controller) vendors are advocating that PLCs or PACs (Programmable Automation Controllers) are an improved solution.

Remote Terminal Unit (RTU)—This is a control unit designed to support SCADA remote stations.

Programmable logic controller (PLC)—A PLC is used for control of machinery in manufacturing and related industries. PLCs handle both analog and digital inputs, are designed for the harsh environment of a manufacturing floor, and have excellent noise immunity. A PLC is designed to provide responses to inputs in real time. Remote PLCs are also called *field devices*.

Medianets—This is an intelligent network that has been optimized for high traffic video applications. The system has the capability of identifying whether the destination is a smartphone or a desktop computer and can adjust bandwidth based on the target. Medianets also have the capability to deliver surveillance video over the same IP network carrying the company's data traffic. Cisco's Medianet technologies enable the video applications to better interact with the overall system thereby improving the Quality of Service (QoS) for the deployment.

VTC—This stands for video teleconferencing. Medianets improve the QoS for video teleconferencing by integrating complex equipment to distribute the video teleconference. Some older systems use ISDN (Integrated Services Digital Network); however, IP/SIP based VTC is now the norm. SIP is the Session Initiation Protocol used for the signals and control of multimedia sessions such as a video teleconference and Internet telephony.

1.8 Given a scenario, implement and configure the appropriate addressing schema

Autoconfiguration—This is an IPv6 feature. With IPv6, a computer can automatically configure its network settings without a DHCP server by sending a solicitation message to its IPv6 router. The router then sends back its advertisement message, which contains the prefix information that the computer can use to create its own IPv6 address. This feature significantly helps simplify the deployment of the IPv6 devices, especially in the transient environments such as airports, train stations, stadiums, hotspots, and so on.

To complete the autoconfiguration IPv6 address, the subnet prefix of *FE80::/64* is then prepended to the interface identifier resulting in a 128-bit link-local address. To ensure that there is no duplicate address on the same link, the machine sends a Neighbor Solicitation message out on the link. The purpose of this solicitation is to discover the link-layer address of another IPv6 node or to confirm a previously determined link-layer address. If there is no response to the message, it assumes that the address is unique and therefore assigns the link-local address to its interface. The process of detecting another machine with the same IPv6 address is called Duplicate Address Detection (DAD).

EUI 64—This stands for Extended Universal Identifier-64, and this option allows the router to choose its own host identifier (rightmost 64 bits) from the EUI-64 (Extended Universal Identifier-64) of the interface. The following example uses the IPv6 address of 2001:DB88:FEED:BEEF::1 on the router interface. This has a 64-bit network prefix of 2001:DB88:FEED:BEEF. The interface identifier of the link-local address is derived by transforming the 48 bits of the EUI-48 MAC address to 64 bits for EUI-64. This EUI-48 to EUI-64 transform algorithm is also used to derive the interface identifier for the global unicast address.

The following example demonstrates how to convert an EUI-48 MAC address of 000C291CF2F7 to a modified EUI-64 format.

1. Expand the 48-bit MAC address to a 64-bit format by inserting “FFFE” in the middle of the 48 bits.

   000C29 **FFFE** 1CF2F7

2. Change the 7th bit starting with the leftmost bit of the address from 0 to 1. This 7th bit is referred to as the U/L bit or universal/local bit. 000C29 is 0000 00**0**0 0000 1100 0010 1001 in binary format. When its 7th bit is changed to 1, it becomes 0000 00**1**0 0000 1100 0010 1001, which is 0**2**0C29 in hexadecimal number.

3. The result is a modified EUI-64 address format of 020C29FFFE1CF2F7.

Toredo, miredo—Toredo is a tunneling protocol that provides IPv6 connectivity for IPv6 capable devices that are on an IPv4 platform. Toredo is a temporary measure for clients that don’t have IPv6 capability and is expected to be removed as IPv6 networks mature. Miredo works behind NAT (Network Address Translation) devices. It also doesn’t require that tunnel endpoints or accounts be defined.

DHCP6—This is the Dynamic Host Control Protocol for DHCP6. An IPv6 client can request an IPv6 address, and it can request a DHCPv6 prefix.

1.9 Explain the basics of routing concepts and protocols

Routing redistribution—Routing redistribution is another important practice that a network engineer may have to face when working in a big network environment. Routing redistribution is the technique of injecting routes from one routing protocol to another routing protocol. Routes are only exchanged automatically with routers running the same routing protocol. Each routing protocol speaks its own language; they do not automatically communicate with each other. Each routing protocol has its own metric or cost. Static routes use administrative distance, OSPF uses cost, IS-IS uses metric, and EIGRP uses composite metric. Therefore, routes from different routing protocols cannot be exchanged automatically. This process has to be configured manually.

There are several reasons why routing redistribution is necessary. One common reason is to redistribute static routes. These routes are not learned but are configured manually. They must be redistributed into a dynamic routing protocol so that they can be advertised. Another reason is when two or more dynamic routing protocols are used on the network. This scenario happens often when connecting one network to another either for peering purposes or for business acquisition. When connecting to another network of different routing protocols, rather than converting to a single routing protocol, it is much easier to accept the new routing protocol and to distribute the new routes into the existing routing protocol. This saves time and money. Another reason for routing redistribution is that certain routing protocols may not be supported by certain network devices. A prime example of this is the EIGRP, which is a Cisco proprietary protocol and is not supported by any other network vendors. If a non-Cisco router were to connect to an existing EIGRP-running Cisco router, the Cisco router will need to redistribute routes learned from another routing protocol into EIGRP.

Route aggregation—This is a technique used to minimize the number of routing tables required in an IP network.

High availability—This refers to information technology systems that are in continuous operation for a long time and downtime must be minimal. Typical high availability systems include hospitals and data centers. These systems are intended to be in operation 100% of the time. There are three principles in engineering high availability systems:

1. Eliminate single points of failure by adding high redundancy.
2. Provide reliable crossovers to avoid a single point of failure.
3. The systems must be able to detect failures. A reliable/redundant system might make it so that failures are not seen, but the failures must be noted in the maintenance log.

VRRP—This is the Virtual Router Redundancy Protocol that provides automatic assignment of routers to hosts participating in the network. The objective is to increase reliability and availability of routes. For participating hosts, the default gateway is assigned to a virtual router instead of a physical router. Each VRRP is limited to a single subnet. VRRP also functions with IPv6, IPv4, MPLS, and Token Ring. The virtual IP address for VRRP can be assigned manually or via DHCP (Dynamic Host Configuration Protocol). The most common application for VRRP is to have one router dedicated to forwarding data packets from hosts in a LAN.

Virtual IP—This is a virtual IP address also called a VIPA. When using a VIPA, there isn't an actual or physical network device. The virtual IP address is shared among multiple servers and domains. Data packets still travel over existing network paths but are no longer dependent on a single network interface card (NIC). A reason to implement a virtual IP address is to improve redundancy and provide failover capabilities for the machine.

HSRP—This is the Hot Standby Router Protocol. This protocol enables a framework of routers so that a default gateway always is available, hence the status of "Hot Standby." HSRP does not advertise routes and is not a routing protocol. However, if a router goes down, the backup router takes over as the primary router and still provides a default gateway.

SPB—This is stands for shortest path bridging. It is based on the IEEE 802.1aq standard for enabling multipath routing. It is a replacement for the IEEE 802.1D, IEEE 802.1w, and IEEE 802.1s spanning tree protocols. While the intent of the older spanning tree protocol was to block a layer 2 loop, SPB lets all paths be active with equal costs, thereby providing a larger layer 2 topology.

1.10 Identify the basic elements of unified communication technologies

VoIP—Voice over IP (VoIP), or IP telephony, is the transport of phone conversations over packet networks. Many companies and individuals are taking advantage of the development of new technologies that support the convergence of voice and data over their existing packet networks. The network administrator can also see an additional benefit with the cost savings using a converged voice/data network. This has created a new role for the network administrator, that of a telecommunications manager. The network administrator must not only be aware of the issues of data transport within and external to the network, but also the issues of incorporating voice data traffic into the network.

QoS—An important issue in the delivery of real-time data over a network (for example, voice over IP) is quality of service (QoS). The following are QoS issues for a VoIP network:

- Jitter
- Network latency and packet loss
- Queuing

Jitter—Digitized voice data requires a fixed time interval between data packets for the signal to be properly converted back to an audible analog signal. However, there is a delay problem with transported voice data over a packet network. Variability in data packet arrival introduces jitter in the signal, which produces a poorly reconstructed signal at the receiver. For example, assume that a 1000 Hz tone is sent over a VoIP network. The tone is digitized at regular time intervals, assembled into frames and packets, and sent out as an RTP packet. Random delays in the packets' travel to the destination result in their arriving at irregular time intervals. The reproduced 1000 Hz analog tone will contain jitter because the arrival time for each data packet varies.

Buffering the data packets long enough for the next data packet to arrive can minimize the effects of jitter. A *buffer* is temporary storage for holding data packets until it is time for them to be sent. The buffer enables the data packets to be output at regular time intervals, thereby removing most of the jitter problem. Buffering works as long as the arrival time of the next packet is not too long. If the arrival time is too late, the data packet might have to be considered "lost" because the real-time data packets can't wait too long for the buffered packet without affecting the quality of the reconstructed signal. Another issue is that the buffering stage introduces delay, and having to wait additional time only introduces more delay.

Network latency—It takes time for a data packet to travel from the source to the destination. This is called network latency, and it becomes an important issue in VoIP data traffic. Telephones (both traditional and IP) feed a portion of the user's voice into the earpiece. If the round-trip delay of the voice data is too lengthy (> 50 ms), the user begins to hear an annoying echo in the earpiece.

Delay issues can be minimized by making sure the network routers and switches are optimized for VoIP data traffic. The VoIP network can be configured so that high-priority data packets (for example, voice packets) are transported first over the IP network. Nonsensitive data packets are given a low-priority status and are transmitted only after the high-priority packets are sent.

Another source of packet delay is network congestion. This can have a negative effect on any type of data traffic but is disruptive to VoIP telephony. The network administrator must make sure that congestion problems are avoided or at least minimized and could have the option of configuring the routers to optimize routes for IP telephony.

Queuing—This is another technique the network administrator can use to improve the quality of service of data traffic by controlling the transfer of data packets. The administrator must identify the data traffic that must be given priority for transport. The queuing decision is made when the data packet arrives, is first queued, and is placed in a buffer. There are many types of queuing arrangements, with the most basic being FIFO (first in, first out). In this case, the data packets are placed in the queue on arrival and transmitted when the channel is available.

A technique called *weighted fair queuing (WFQ)* is available on many routers and is used to determine what data traffic gets priority for transmission. This technique applies only if the buffer is full, and a decision must be made as to which data packet goes first. WFQ can be modified to provide a class-based weighted fair queuing (CBWFQ). This improvement enables the network administrator to define the amount of data traffic allocated to a class of data traffic (for example, VoIP).

Other queuing techniques are PQ and CQ. Priority queuing (PQ) is used to make sure the important data traffic gets handled first. Custom queuing (CQ) reserves a portion of the channel bandwidth for selected data traffic (for example, VoIP traffic). This is a decision made by the network administrator based on experience with the network. The problem with CQ is it doesn't make allowances for other traffic management when the channel is full; therefore, queuing techniques such as WFQ or WRED can't be used to manage the data flow.

DSCP—This is the Differentiated Services Code Point. A field is placed in the IP data packet that is used to enable services. It is a combination of the IP Precedence and Type of Service fields.

COS—This stands for Class of Service. With COS, flow control for data throughput can be better managed.

UC servers—The UC stands for unified communication. This refers to the integration of various real-time technologies such as IP telephony, instant messaging, audio and video conferencing. Essentially, UC enables a message that is sent using one technology to be received using a different technology.

UC devices—This refers to unified communication devices.

UC gateways—This refers to gateways used by unified communication technologies.

1.11 Compare and contrast technologies that support cloud and virtualization

Virtual firewall—This is a network device running in a virtual environment. This device provides the same functionality as a physical firewall.

Software-defined networking—This enables network administrators' manageability of the network, enabling network control to be programmable.

Storage area network (SAN)—This network is used to provide access to storage devices for multiple servers. The SAN is robust and is built to handle any type of failure. Additionally, the SAN must be able to grow as the network grows. The main benefit of SANs is that storage is treated as a pool of resources. These storage resources are centrally managed and made available as needed.

ISCSI—This stands for Internet Small Computer System Interface. This feature allows SCSI commands to be sent over the LAN or Internet.

Jumbo frame—These are simply Ethernet frames that contain more than 1500 bytes of data. A jumbo frame can carry up to 9216 bytes and is supported by most Gigabit switches. Not all Fast Ethernet switches support jumbo frames. The advantage with jumbo frames is the reduced overhead; however, jumbo frames can have a negative impact on network performance, in particular latency, in low bandwidth networks.

Network attached storage (NAS)—This is a type of storage for nodes on the local area network. This device has its own Ethernet connection and IP address. NAS also provides the ability to share its files with multiple clients on the network.

Cloud concepts—The word "cloud" is such a nontechnical term that when it represents a technology, it sounds so vague and nebulous. Cloud computing is one of the most talked about technologies in recent years, discussed by IT people and users alike. Cloud has become a new noun, as in "people can connect to the cloud," or "my stuff is stored on the cloud," or "I migrate everything to the cloud." The cloud is magically in the middle of everything. Yet, people still don't know what and where the cloud really is. Its famous existence has developed many punch lines of its own and created many questions. The bottom line is that the *cloud* is just another name for the Internet.

Cloud infrastructure—There are different types of cloud infrastructures used by IaaS, PaaS, and SaaS. These infrastructures offer different levels of security, resource restrictions, and management. Most notable cloud models are

- **Public cloud—**This cloud infrastructure is owned and operated by the cloud service company but made available for use by the general public.
- **Private cloud—**This cloud infrastructure is operated by the organization and is made available only to members of the organization.
- **Community cloud—**This cloud infrastructure offers two or more organizations exclusive access to the infrastructure and computing resources. These organizations may have shared common policies that allow them to operate in a distributed mode.
- **Hybrid cloud—**This cloud infrastructure offers a combination of at least one private cloud and one public cloud.

1.12 Given a set of requirements, implement a basic network

Environment limitations—Access to the network and in particular the Internet can be limited for users. For example, download times and saturated networks can have a negative impact on the computer's Internet access and frustrate users. This limitation on the networking environment is constantly being addressed by network engineers.

Compatibility requirements—One significant improvement in today's networks is the interoperability of most network devices. Setting up and physically connecting any device to an Ethernet connection is virtually the same for all operating systems (OS) and computers. Yes, the underlying OS differs, but they all function pretty much the same and provide similar features and TCP/IP support. Access to the Internet is also similar for each OS and computer system regardless of whether you are operating at a home or at a business. The difference is typically a home supports a few computer systems and maybe one or two Internet connections. The business might have numerous computers and a high bandwidth Internet connection.

2.0 NETWORK OPERATIONS

2.1 Given a scenario, use appropriate monitoring tools

TRAP—SNMP TRAP is one of the SNMP protocol data unit (PDU) types. It is used to enable an agent to notify the SNMP network management station (NMS) of significant events. Instead of an NMS polling information and getting a response from an SNMP agent, the agent sends an unsolicited SNMP message to the NMS as triggered by specified events.

Walk—In the situation where an OID (object identifier) is not returned, snmpwalk searches SNMPv2-SMI::mig-2.

SYSLOG—It is a standard protocol used to collect log messages sent from devices to a server running a SYSLOG service or daemon. The server is typically known as a SYSLOG server. SYSLOG servers run on UDP port 514 or TCP port 601.

SIEM—Security Information and Event Management is an IT security system that can provide a holistic view and real-time analysis of an organization’s IT security. A SIEM system combines the Security Event Management (SEM) and the Security Information Management (SIM) by gathering security alerts and information generated by the network or security hardware, servers, and applications.

2.2 Given a scenario, analyze metrics and reports from monitoring and tracking performance tools

Log management—This is a way to collect log files from different devices and to store the log data over time, so that information can be extracted, analyzed, and reviewed. Log files can be gathered from many different sources in many different ways, and they can have different formats. The standard is to use SYSLOG so the log files from devices such as routers, switches, web servers, database servers, and so on can be generated with a consistent format, and they all can be sent to the same aggregation point like SYSLOG server.

Graphing—Graphing is a standard representation used by many monitoring tools to show the performance, behaviors and trends of interested targets over time. These tools convert the raw data collected from log files, SNMP messages, or proprietary system information into useful and readable reports by illustrating them in graphical formats. For the computing hardware, one might be interested in tracking the CPU utilization, memory usage, I/O rate, and storage or disk consumption. For the network devices, one might be interested in tracking the network device CPU, network device memory, interface or link status, network utilization, network packets, network errors, and network discards.

Utilization storage—They key point is you want as much memory as you can afford and you also want fast devices. Solid state memory (storage) is the best choice.

Network device CPU—The issue with the CPU is an overtaxed CPU is slow. This can be because too many processes are running or you don't have sufficient memory to handle the workload.

Network device memory—You want to install as much memory as your system can handle, and you want to use fast devices.

Link status—The easiest way to verify link status is by using the **ping** command. You can verify the link lights when possible.

Discards—Data packets have what is called a "Time-to-Live," which is the number of routers the data packet can pass through before it is discarded.

SMS—Short message service can send text messages of alerts and notifications. This is a feature that typically is integrated into most monitoring tools.

2.3 Given a scenario, use appropriate resources to support configuration management

NAC—Network Access Control is sometimes known as Network Admission Control. It is a security mechanism that can be implemented on a network to register, authenticate, authorize, and enforce security policies on all endpoint devices before they are allowed to access the network. NAC is gaining popularity as a method to manage BYOD (Bring Your Own Device) and keep track of these devices. It can be deployed in many forms from hardware appliance, virtual appliance, client agent, or clientless agent. It can be used to manage the on-boarding and off-boarding of mobile devices.

To manage network devices and resources properly, an organization must have a good policy for change management for network device configuration and standard procedures for network maintenance. To prepare for disaster recovery, an organization must have a backup plan, which entails backing up network equipment configurations and archiving them for recovery. One of the most fundamental elements of network operations is documentation. Documentation can consist of network drawings and diagrams, asset management, and even vendor documentation. Having network diagrams helps engineers visualize and understand how things are connected. Asset management gives engineers details of their network equipment from model numbers to software version and their locations.

2.4 Explain the importance of implementing network segmentation

SCADA systems/Industrial control systems—Industrial Control Systems (ICS) are command and control networks designed to support industrial processes in critical infrastructures such as power plants, transportation systems, utility facilities, refineries, and factories. The largest subgroup of ICS is Supervisory Control and Data Acquisition (SCADA) systems. Since critical infrastructures are controlled and monitored by ICS/SCADA over the network, they need to be secured and protected against vulnerabilities, exploitations, and malicious attacks. An ICS/SCADA system must be on its own network; it must be segmented off from other networks and must be placed behind the network firewall with strict access.

Legacy systems—Legacy systems can be categorized as "end-of-life" or "end-of-support." This means that they are no longer supported by their vendors and manufacturers. One of the biggest security risks for a legacy system is there will not be a firmware, hardware, or software update. This makes a legacy system more vulnerable and susceptible to security hacks and exploitations. If it is on a network, a hacker can exploit it via its known vulnerabilities. Legacy systems should be decommissioned as soon as possible. If needed services are running on these systems, an organization must plan to transition these services to another system. If legacy systems must be on the network, it is best to segment the legacy systems off to a protected network and restrict access to these systems.

Honeypot—Honeypot is a computing environment specifically set up to gather information regarding network attacks and intrusions and to study the vulnerabilities of a system. A honeypot typically consists of decoy servers or systems including a real network that connects to the Internet. The honeypot environment is designed to be more vulnerable, which allows for easier access and intrusion than the real protected environment. It is also designed to be on a separate network with constant monitoring and logging to gain more insights of how attackers can break into or penetrate into the systems.

Testing lab—Testing lab is another good environment to have for an IT organization. It is a best practice for an IT organization to have both a production environment and a testing environment, where the testing environment is almost a clone of the real production environment. For a smaller IT shop, a testing lab can be set up to mimic the hardware environment in a much smaller scale. However, it serves the same purpose of testing the software and hardware installations, upgrades, and patches before doing it on the production environment. For mission critical services, it is imperative to do all the necessary testing in the testing environment or lab, so the detrimental issues can be discovered and worked out and to lessen the negative impact on users.

2.5 Given a scenario, install and apply patches and updates

Driver updates—These updates are required for the operating system or the software to operate the hardware component. Also, when there are changes to the OS or the software, the driver may need to be reinstalled or updated.

Major versus minor updates—Typically, minor updates are subsets of a major update. Major updates are strongly recommended by the vendors, while minor updates are done as needed.

2.6 Given a scenario, configure a switch using proper features

Interface configuration—VLAN interface configuration is different from a router interface configuration. With a router interface configuration, a subnet is created, and it is local to that router interface. With VLAN interface configuration, a subnet is created, and it is local to that VLAN. Since more than one switch port can be assigned to a specific VLAN, this means the same subnet can span different physical ports or user locations. This allows for greater flexibility to have many locations sharing the same subnet.

VTP—VTP or VLAN Trunking Protocol is Cisco's proprietary protocol used to manage and propagate the VLAN definitions to all the VTP capable switches. This is to reduce the administrative overhead in maintaining the VLANs in all the switches on the network. With VTP, a new VLAN can be defined on a VTP server, and then the VLAN information gets propagated to every switch on the network.

Port bonding (LACP)—Link Aggregation Control Protocol (LACP), sometimes called port bonding, is part of an IEEE specification (802.3ad) that allows for multiple physical ports on an Ethernet switch to be bundled as one single logical channel. LACP is a standard protocol supported by most network switches, while PAgP (Port Aggregation Protocol) is a Cisco proprietary protocol that performs a similar function to create an EtherChannel.

Port mirroring (local versus remote)—Port mirroring is a capability offered by many network switches. Port mirroring, as implied by the name, makes a copy of the network traffic from a specified port or ports and sends the traffic to a specified destination. When a copy of the traffic is sent to another port on the switch, it is local port mirroring. When the destination is on another switch, it is remote port mirroring. For remote mirroring, the copy of traffic is sent over a dedicated VLAN created for this purpose. Port mirroring is essential for monitoring and logging the network traffic without having to install a device in-line with the traffic and disrupt the network traffic flow.

In-band/Out-of-band management—The management of the remote network devices can be done in two ways. One is in-band management, and another is out-of-band management. In-band management refers to when the management traffic is using the same network channel as the regular network traffic on the managed network device. Out-of-band management refers to when the management traffic is using a different or dedicated network channel than the regular network traffic on the managed network device.

AAA—AAA stands for authentication, authorization, and accounting. It is a common access control used by RADIUS and Kerberos.

2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices

Device density—The device density is the number of connecting wireless clients. Every wireless access point has a maximum device density that it can handle at one time. This is crucial in wireless AP deployment planning. More WAPs are always needed in a more populated area to handle more wireless devices.

Wireless controllers—Wireless controllers are used more in an enterprise wireless environment when managing hundreds of APs or more. In a traditional standalone wireless environment, each AP is managed individually. With an enterprise wireless controller environment, an AP communicates with its controller when booting up to download its necessary firmware and software, to register and authenticate itself, to receive its network information settings, and to receive its wireless LAN (WLAN) configuration. The wireless controller becomes the brain and manager of the whole operations. When wireless changes need to be made, it can be done at the controller, which pushes the changes out to all of the APs.

VLAN pooling—VLAN pooling is a solution offered by many wireless manufacturers to deal with the large number of connecting wireless devices, and every device is required to have an IP address. Multiple VLANs of different subnets can be grouped together with VLAN pooling to accommodate the large number of IP addresses needed. Every device shares the same WLAN, but may have an IP address of a different subnet.

LWAPP—Lightweight Access Point Protocol (LWAPP) is a Cisco Proprietary Protocol that has been superseded by the standard called CAPWAP (Configuration and Provisioning of Wireless AP). LWAPP is the underlying wireless control protocol for Cisco APs to communicate with their wireless controllers.

Goodput—Goodput refers to the actual wireless data throughput as measured by an application on the end device. It is a way to represent the actual transmission rate of a wireless connection, which is not the maximum theoretical transmission rate.

High throughput—A wireless adapter with high throughput or high successful data delivery rate can be referred to as 802.11a-ht or 802.11g-ht depending on the protocol 802.11a or 802.11g protocol used by the adapter.

Ad hoc—Ad hoc wireless connection is a peer-to-peer connection between wireless devices. This connection does not require a wireless access point, as wireless devices communicate directly with each other.

Cell phone—Another way to connect a wireless device to the Internet is via a cell phone. A cell phone can be set up as a hotspot that a wireless device can connect to and use the data plan to connect to the Internet.

3.0 NETWORK SECURITY

3.1 Compare and contrast risk related concepts

Business continuity—The IT group is responsible for servicing all organizations within a business. The IT group needs to have a plan because everyone uses computers and the network. Software and hardware decisions need to have input from all organizations so that there is good continuity among all groups requiring IT support.

3.2 Compare and contrast common vulnerabilities and threats

Botnet—A group of infected or compromised computers on the Internet that are being used to launch coordinated denial of service attacks against another system on the network. A botnet computer is controlled via an Internet Relay Chat (IRC) channel by a server called a command and control server.

Coordinated attack—A type of distributed denial of service attack that is deliberate toward a specific target and is orchestrated by a controller source like the command and control server in a botnet. In recent news, the Anonymous group is synonymous with the coordinated attacks as they planned many attacks to bring down websites deliberately to send their political message.

Friendly/unintentional DOS—This type of denial of service is not a malicious attack. It is typically caused by heavy legitimate traffic to a server or a website that inadvertently overwhelms the server resources or the network connection. So, the server or the network cannot handle the massive volume of traffic.

Permanent DOS—Permanent DOS or PDOS is a malicious type of attack that aims to sabotage the hardware and render it useless. A PDOS attack can damage a hardware system to the point that it requires replacement or reinstallation of hardware.

Reflective/amplified—A recent reflective attack used DNS servers configured as open resolvers on the Internet. These open resolvers answer any DNS queries from anyone. A small DNS query asking for all information about the DNS zone is sent to an open resolver; then in turn the open resolver replies with the huge DNS zone information. The message has increased or amplified, hence the name DNS amplification attack. When a botnet sends these small DNS query messages to a list of open DNS resolvers with the source IP being the victim, the amplified messages are then sent or reflected back to the victim overwhelming the resources on the victim.

NTP—Similar to DNS amplification attacks, this is another reflective attack using public Network Time Protocol (NTP) servers. This time a botnet sends an old NTP remote command called monlist requesting a list of the last 600 hosts connected to the server and spoofs the source IP to be the victim. Again, this DDOS is used to overwhelm the victim and bring down the system.

Packet/protocol abuse—Hackers can compromise a system or gain valuable information from a system by taking advantage of inherent weaknesses in network packet and network protocols. Ping of Death, SYN attack, and DNS reflective attack are just a few examples of packet/protocol abuse.

Man-in-the-middle—Man-in-the-middle is an attack where an attacker seamlessly places itself in the middle of the conversation of others. Therefore, the attacker becomes the recipient of all information sent by victim computers.

ARP cache poisoning—This is a technique used in man-in-the-middle attacks. On the same network segment, network devices communicate using MAC addresses. These MAC addresses are stored in the ARP cache, which contains IP address to MAC address mappings. If an attacker can change the MAC addresses in the victim's ARP cache or "*poison the ARP cache,*" then the conversations get redirected to the attacker.

Evil twin—Evil twin can be categorized as a man-in-the-middle attack in which a rogue wireless access point poses as a legitimate one by broadcasting a legitimate SSID and eavesdropping on the wireless network. Typical users only recognize the SSID and do not know behind the scene which APs are broadcasting this wireless network. Attackers can collect information from wireless users connecting through this wireless access point.

War chalking—War driving is a process in which attackers search for locations with an open wireless network or a weak wireless network, so that they can gain more access to collect information or data of connecting users. War chalking is the next step after war driving, which leaves marks or symbols on the premise, outside the premise, or even online to notify other hackers about the wireless vulnerabilities of the location.

Bluejacking/Bluesnarfing—Both Bluejacking and Bluesnarfing are attacks on Bluetooth devices. Bluejacking is considered more annoying than harmful as it sends unsolicited messages to other Bluetooth devices in the vicinity, while Bluesnarfing is truly an attack to gain unauthorized access of another Bluetooth device over the Bluetooth connection with the intention to obtain information stored on the Bluetooth device.

WPA/WEP/WPS attacks—To crack encrypted systems requires the "bad guy" to collect a lot of information. For example, a lot of information is transmitted with an ARP request in a wireless system. The "bad guy" can use this information to extract the WEP key from this data. It is not simple, but it can be done.

Session hijacking—Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services on a computer. It is more synonymous with the exploitation of the web session control by stealing a session cookie and using it to establish a session with remote servers that still think the session is valid.

VLAN hopping—VLAN hopping is an attack to gain information or resources only available in specific VLANs. There are two types of VLAN hopping attacks. A switch spoofing attack works by taking advantage of an incorrectly configured trunk port whereby the attacker tricks a switch into thinking that another switch is forming a trunk port and therefore gaining access to all the VLANs allowed on the trunk port. Another type of VLAN hopping attack is the double-tagging attack whereby the attacker embeds a second 802.1Q tag inside the frame. This second tag allows the frame to be forwarded to a VLAN that the original 802.1Q did not intend.

Compromised system—Compromised system is generally referred to as a computer, a group of computers, or a part of the network that has been adversely impacted by an untrusted source.

Zero-day attacks—A zero-day attack refers to the exploitation of vulnerability in software that is unknown to the developer. Since the developer is not aware of it, there is no patch to fix it.

Unencrypted channels—Any network transmission done by using a protocol that does not encrypt the data is said to be an unencrypted channel. Some of the protocols that cannot encrypt data are TELNET, FTP, HTTP, TFTP, TEMPEST, and SNMP v1 and v2.

TEMPEST/RF emanation—TEMPEST is a standard for computer systems certification commenced by the US government in the late 1950s. TEMPEST standard specifies the amount of Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) or RF emanation emitted by a device. The purpose of TEMPEST is to shield the wireless RF signal within the area and not divulge intelligence about system information.

3.3 Given a scenario, implement network hardening techniques

Anti-malware network-based—This type of anti-malware is installed on a device connected to the network that is capable of monitoring all traffic in and out of the network. Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Application or a Next-Generation Firewall can be equipped with anti-malware capability.

Cloud/server-based antimalware—This type of antimalware has a lightweight agent installed on a device. The agent then communicates with and sends its information to a server or a cloud server for signature definition detection and analysis. So the heavy lifting is done by the server or the cloud server instead of by the software on the device.

Switch Port Security—This security option is prominent in Cisco switches where it can be configured to enable many switch port security features.

DHCP snooping—This security feature detects any rogue DHCP server and stops DHCP packets from untrusted ports from propagating.

Personal WPA/WPA2—Wi-Fi Protected Access (WPA) and its successor WPA2 are wireless security standards developed by the Wi-Fi Alliance. Both personal WPA and WPA2, also known as WPA-PSK (Personal Shared Key), use a passphrase consisting of 8 to 63 ASCII characters. The big difference is WPA uses Temporal Key Integrity Protocol (TKIP), which is based on RC4 stream cipher. WPA2 uses Counter Mode Cipher Block Chaining Message Authentication code protocol (CCMP), which is based on the Advanced Encryption Standard (AES) and is significantly stronger than RC4-based TKIP.

TLS/TTLS—Transport Layer Security (TLS) is the successor to the Secure Sockets Layer (SSL), and it is designed to ensure privacy between the communicating parties. TLS ensures that no third party may eavesdrop or tamper with any messages between a server and a client. TLS requires both the client and the server to use certificates to verify their identities to each other.

Tunneled Transport Layer Security (TTLS) is similar to TLS in that it also ensures the privacy, but it does not require that each party be issued a certificate. Instead, only the authentication server is issued a certificate. The client authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificate.

Kerboros—Kerboros is the authentication protocol for Windows Active Directory. When users log on, a special token or ticket containing information linking it to the users is issued by the Kerboros authentication server. Kerboros uses this ticket to validate user access to a resource or a service.

Multifactor/two-factor authentication—When two different authentication factors are used, that is called two-factor authentication. An example of a two-factor authentication would be password (what you know) and smartcard token (what you have). When two or more factors of authentication are used, it is a multifactor authentication. An example would be password, smartcard token, and biometrics (what you are).

Authentication/Single sign-on—Single sign-on (SSO) is a process that permits the users to access different systems after one successful authentication. For an enterprise environment, this makes it convenient for users not having to enter the same credentials to access different systems such as file server, email, and ERP.

MSCHAP—This was created by Microsoft for authenticating remote Windows-based systems. **CHAP** and **MSCHAP** both use a challenge response mechanism to authenticate connections without requiring sending any passwords.

3.4 Compare and contrast physical security controls

Mantraps—A mantrap is an interlocking door controller in a small room, where one door of a mantrap cannot be unlocked or opened until the other door has been closed or locked. Mantraps are used in high security areas where only authorized personnel are allowed.

3.5 Given a scenario, install and configure a basic firewall

UTM—Unified Threat Management (UTM) is an all-in-one solution that integrates a wide range of security features into one appliance. A UTM appliance may have a combination of firewall, network IDS/IPS, VPN, gateway antivirus, gateway antispam, load balancing, and content filtering. This type of appliance is popular in small to medium businesses where the network is too big and complicated. It helps reduce administrative time and cost overhead.

Virtual wires versus routed—With a virtual wire, the firewall takes the data packets coming into one port and sends these to another port. Data packets from the outside are sent inside. In a way, this is just a transparent bridge between the two ports.

Application aware/context aware—This type of firewall is sometimes known as a next generation firewall because of its capability to operate beyond the typical layer 4 of the OSI model. This type of firewall can perform deep packet inspection to analyze each packet. It can incorporate application and context information with other network information to make security decisions.

3.6 Explain the purpose of various network access control models

Posture assessment—Posture assessment is the evaluation of system security based on the applications and settings that a particular system is using. A posture assessment is typically performed on a device before it is permitted to access the network. If a device is found not to have all necessary security settings or software, it can be placed in a quarantine network until it can pass the assessment.

Guest network—A guest network is a special segmented network provided to visitors to access the Internet and certain unrestricted networks. However, visitors are not allowed to access the secure corporate network or corporate resources. Sometimes, certain restriction controls such as bandwidth, time, and network protocols are implemented.

Persistent versus nonpersistent agents—A persistent agent is already installed on the system and is waiting to be used as needed. This agent can be detecting incidents or just waiting to be called on. A nonpersistent agent is typically installed and used as needed.

Edge versus access control—Edge control is applied at the boundary of the network, where firewalls or routers are used to protect the network. This control can restrict access in and out of the network. Access control has an advantage over edge control in that it can be more granular as the control is applied at the resource itself.

4.0 TROUBLESHOOTING

4.1 Given a scenario, implement the following network troubleshooting methodology

Divide and conquer—Using this troubleshooting approach, an OSI layer is selected and tested for its functionality. If this layer is good, the technician tests the next layer, which could be higher or lower. Selecting the layer you start with in the troubleshooting process varies depending on the technician's experience. An experienced technician has a better understanding where to start.

4.2 Given a scenario, analyze and interpret the output of troubleshooting tools

tracert/tracert -6/traceroute6/traceroute -6—These are all commands used to trace the routes that data packets take in an IP network. The commands with a (6) after the command indicate they are for tracing routes in an IPv6 network.

nbstat—This is a diagnostic tool for checking NetBIOS over TCP/IP. The following are some basic functions:

- **nbstat –a <name>—**This checks the NetBIOS adapter status on the computer <name>.
- **nbstat –a <IP address>—**This checks the NetBIOS adapter status on the computer with the specified IP address.
- **nbstat –c /—**This displays the contents of the NetBIOS name cache.
- **nbstat—n /—**This lists the names that are locally registered by NetBIOS applications.
- **nbstat—r -/—**This command lists the count of NetBIOS names.
- **nbstat—R /—**This command purges the name cache.
- **nbstat –RR /—**This command releases packets to the WINS and starts a refresh.
- **nbstat—S /—**This command lists the current NetBIOS sessions.

Multimeter—This is a device used to measure voltage, current, and resistance. A basic function related to cabling is conducting a continuity check, which is used to verify two ends are connected.

Light meter—The function of a light meter is to shine light down a fiber. This assumes that the fiber is not connected to anything at either end.

Toner probe—The function of a toner probe is to inject a tone on a cable. The technician can then use a speaker/sensor to verify that a tone is present at the other cable end. This is also useful when having to locate a cable end. The cable being searched for will have the tone.

Speed test sites—These are used so a speed test can be run to measure a computer's upload and download speeds.

Looking glass sites—These sites are used to obtain routing information related to the network's backbone and efficiency.

4.3 Given a scenario, troubleshoot and resolve common wireless issues

Signal-to-noise ratio—This is a measure of the signal level relative to the noise level. The value is usually expressed in dB, and a high dB value is desirable.

Window film—Sometimes the covering on windows interferes with the propagation of wireless signals. The technician must be aware of this possible problem.

Mismatched channels—Wireless access points and the client computer must use the same frequencies to communicate. The most common frequencies are channels 1, 6, and 11 since these are nonoverlapping channels.

Device saturation—Wireless networks use a shared media, and as the number of wireless units trying to access the network increases, data throughput declines. Remember, wireless networks use the CSMA/CA Carrier Sense Multiple Access/ Collision Avoidance.

Bandwidth saturation—A communication channel has a limited bandwidth. In other words, the channel can carry only so much data. As the user demand increases, the capacity is limited and only so much information can be carried. This is similar to the concept that a garden hose can carry only so much water. If more water capacity is required, you have to get a bigger pipe.

Untested updates—In this case, the updates have not been fully tested for your network. Potential compatibility issues have not been identified. Network administrators normally wait so that problems can be isolated and fixed or wait for a software update that fixes known problems.

Open networks—This is a wireless network that is not using encryption or is using the factory default SSID. In either case, security is now a big threat since the "bad guys" have access to your network.

Incompatibilities—Compatibility issues are important in wireless networks. You need to know the operating frequency for each standard. The current wireless standards are listed here:

- **802.11a (Wireless-A):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5 GHz. (Modulation OFDM)
- **802.11b (Wireless-B):** This standard can provide data transfer rates up to 11Mbps with ranges of 100–150 feet. It operates at 2.4 GHz. (Modulation DSSS)
- **802.11g (Wireless-G):** This standard can provide data transfer rates up to 54Mbps up to 150 feet. It operates at 2.4 GHz. (Modulation DSSS or OFDM)
- **802.11n (Wireless-N):** This high-speed wireless connectivity promises data transfer rates over 200+ Mbps. It operates at 2.4 GHz and 5 GHz. (Modulation DSSS or OFDM)
- **802.11i:** This standard for WLANs provides improved data encryption for networks that use the 802.11a, 802.11b, and 802.11g standards.

- **802.11r:** This standard is designed to speed hand-offs between access points or cells in a WLAN. This standard is a critical addition to 802.11 WLANs if voice traffic is to become widely deployed.
- **802.11ac**: This is the next generation of high-speed wireless connectivity. This technology promises data rates up to 1 Gbps. It operates over the 5 GHz band.

Wrong encryption—There are several encryption types for wireless networks. When setting up a wireless router, you find multiple options for encryption. There are options for WEP (not very secure), WPA, and WPA2. *WPA* stands for Wi-Fi Protected Access, and it supports the user authentication provided by 802.1x and replaces WEP as the primary way for securing wireless transfers. WPA2 is an improved version of WPA. The 802.1x standard enhances wireless security by incorporating authentication of the user. It is important that your networking devices use the same encryption. *(WEP, WPA, and WPA2 are discussed in Chapter 4 section 5.)*

Bounce—This refers to the fact that wireless networks use signal radio waves to communicate. Radio waves bounce off metal surfaces. As a result, the radio signals experience signal loss. Wireless LANs have a maximum distance the signal can be transmitted. This is a critical issue inside buildings when user mobility is required. Many obstacles can reflect and attenuate the signal, causing reception to suffer. Also, the signal level for mobile users is hampered by the increased distance from the access point. Distance is also a critical issue in outdoor point-to-multipoint wireless networks. *(Additional information is provided in Chapter 4 section 3.)*

AP configurations—One of the biggest misconceptions about a wireless network is that it does not require a wired connection. This is not quite correct. The connection to a wired LAN is provided by a wireless access point, which provides a bridge between the wireless LAN and the wired network. A physical cable connection (typically CAT6/5e) ties the access point to the wired network's switch or hub (typically Ethernet). It is also necessary that the SSID, type of encryption, and the channel be specified. (*Additional information on all aspects related to configuring the access point is provided in Chapter 4 sections 2-3 and 5*)

LWAPP—This is the Lightweight Access Protocol. This protocol can be used to simplify the control of multiple wireless access points at the same time. With Cisco's LWAPP, the controller is also used as the gateway from the WLAN to the LAN. The system provides for the assignment of a primary, secondary, and even a tertiary controller for the wireless network.

Thin versus thick—A "thick" network is also called an "intelligent" network. Its purpose is to handle authentication, encryption, and management of the wireless devices connected to it. A "thin" network is referring to "dependent" access points. They are called dependent because they can't operate as a stand-alone device.

4.4 Given a scenario, troubleshoot and resolve common copper cable issues

Cable placement—Cable placement is an important consideration, especially when running cable in high EMF environments or next to electrical mains. Electrical noise can be induced in unshielded cable and can affect data reception. You should not suspend cabling from ceiling tiles for safety and fire regulations. The cable bends should be limited to less than four times the diameter of the cable.

Bad SFP/GBIC (cable mismatch)—There can be compatibility issues using the SFP (Small Form Factor Pluggable), and this is replacing the GBIC. Make sure you have the correct connector.

4.5 Given a scenario, troubleshoot and resolve common fiber cable issues

There is always a chance that your fiber link has gone down or the fiber has been cut. Use the appropriate troubleshooting techniques to fix this.

4.6 Given a scenario, troubleshoot and resolve common network issues

Incorrect IP configuration/default gateway—The most common static route used in a host computer is the default gateway. The *default gateway* specifies where the data traffic is to be sent when the destination address for the data is not in the same LAN or is unknown. If you don't have a route specified for a subnet in your network, the default route is used. For example, if your PC is on the 10.10.0.0 network and it wants to send data to 100.100.20.1, the data is sent to the default gateway as specified by the TCP/IP setup on your PC. If you input an incorrect IP address for the default gateway, your data packets will be discarded.

Duplicate IP address—It is possible that a network could have a duplicate IP address. This typically happens when the ID addresses are configured manually. Most systems detect that a duplicate IP address has been assigned and issue an error message. If two devices are configured with the same IP address, there will be a lot of communication problems, but most likely an error message will be issued first and prevent the IP address assignment.

End-to-end connectivity—This can be verified using the **ping** command. After you have the networking devices physically connected, use the **ping** command to verify that the networking devices are communicating. **ping** uses *Internet Control Message Protocol (ICMP)* echo requests and replies to test that a device on the network is reachable. The ICMP protocol verifies that messages are being delivered. The **ping** command is available in the command window of Windows to verify the networking devices are communicating. The command structure for the **ping** command is as follows:

```
Usage ping[-t][-a][-n count)[-1 size][-f -i TTL][-v TOS] [-r count][-s
  count]
[[-j host-list]:[-k host-list][-w timeout] destination-list
Options
-t Ping the specified host until stopped
To see statistics and continue, type Control-Break
To stop, type Control-C
```

Incorrect VLAN assignment—If you suspect a misconfigured VLAN, simply use the command **show vlan brief** to check what VLAN a switch port has been assigned to. If you spot an error, then reconfigure the settings to correct the problem.

Misconfigured DHCP—Dynamic Host Configuration Protocol (DHCP) simplifies the steps for IP assignment even further. DHCP's function is to assign a pool of IP addresses to requesting clients. A possible error could be that the MAC address assigned to an IP address is misconfigured and the DHCP server doesn't know what computer to assign the IP address to since the MAC-IP addresses relationship is not known. This results in an error, and a valid IP address is not assigned from the DHCP pool of addresses.

Misconfigured DNS—*DNS* is the domain name service. DNS translates a human readable name to an IP address or an IP address to a domain name. The translation of a name to an IP address is called *forward domain name service*, and translation of an IP address to a domain name is called *reverse domain name service*. It is possible that a misconfigured DNA will prevent access to the Internet. When troubleshooting this type of problem, first check to see what the primary and secondary IP addresses for your DNS are. Verify the IP addresses are correct. The *NS record* or *Name Server record* is another place to check. This specifies the name of the authoritative name server of the domain. The record must map to a valid A record, not an IP address or a CNAME. The NS records are associated with the domain, not a particular host. Therefore, one needs to look up the name server information based on the domain. The following example demonstrates the use of the **nslookup** command to look up the NS records of the domain example.com:

```
C:\nslookup -query=NS example.com
Server: 192.168.1.1
Address: 192.168.1.1#53
Non-authoritative answer:
example.com nameserver = a.iana-servers.net.
example.com nameserver = b.iana-servers.net.
```

Cable placement—Cable placement is an important consideration especially when running cable in high EMF environments or next to electrical mains. Electrical noise can be induced in unshielded cable and can affect data reception. You should not suspend cabling from ceiling tiles for safety and fire regulations. The cable bends should be limited to less than four times the diameter of the cable.

Interface errors—Connecting to the Internet is possible via multiple interfaces on the computer. For example, the Internet interface could be an Internet connection to your Internet Service Provider (ISP). This typically involves a cable or DSL modem connection. The most common types of errors experienced are loss of connectivity. The problem could be as simple as a loose cable, or it could be that the system is down due to bad weather conditions or loss of power at the ISP. A good troubleshooting step is to verify that your wireless router is still functioning before passing on the blame to the ISP. You can also try rebooting your modem and/or computer to see whether this corrects the problem.

Simultaneous wired/wireless connections—Sometimes a wireless bridge might have a full-duplex wired connection on one side, but the radio side is not full-duplex. It is possible that data packets continue to be delivered on the cable connected side resulting in the buffer filling up. This is because the ACK packet is not being returned quickly. As a result, the same packet gets retransmitted.

Discovering neighboring devices/nodes—During the power-up process for a wireless router, it starts searching for any wireless signals and indicates whether the channels are unlocked or locked. Locked channels require a secure login.

Power failure/power anomalies—Temporary loss of power is not uncommon with any network. Data loss can be minimized by utilizing a UPS (Uninterruptable Power Supply). These devices can be used to keep the local system functioning until the main power is restored.

MTU/MTU black hole—MTU stands for Maximum Transmission Unit. For Ethernet networks, the MTU is 1518 bytes. An MTU black hole is a result of a misconfigured router resulting in data packets not being properly delivered. In this case the router is called an MTU black hole router.

Missing IP routes—Missing IP routes are due to misconfiguration of the router. When a routing protocol is configured, the network routes are entered for the desired destination networks. A misconfigured route results in nondelivery of the data packet. The network routes can be checked by issuing the **show ip route** command from the router's privilege EXEC mode.

NIC teaming misconfiguration—An NIC is a network interface card. Sometimes more than one NIC is installed on a computer. The purpose is to provide load balancing and fault tolerance (traffic failover). The idea of traffic failover is to keep the computer connected even if there is a failure of the NIC.

Active-active versus active-passive—This addresses the concept of providing high availability (H/A) networks. The term active/passive addresses failover and load balancing. The term active/active supports redundancy for either databases or sessions. An advantage of active/passive configuration using load balancers is providing uninterrupted service. In the active/active mode, the servers working in tandem keep requests stored in cache and as a result improve access time because the server that handled the previous request will be able to respond to the request.

4.7 Given a scenario, troubleshoot and resolve common security issues

TACACS—This stands for the Terminal Access Controller Access Control System and is an older protocol used for user authentication.

Ping of death—This is a type of denial of service attack intended to crash the victim's system or to inject malicious code onto the system. The attack is a malformed ping packet that is too large for the victim to handle and therefore causes a buffer overflow.

Firmware/OSs—It is best practice to keep the firmware of the network equipment such as routers and switches up to date. Also, patches, especially security patches, must be applied to operating systems and software applications regularly.

Misconfigured firewall—The purpose of a firewall is to prevent unauthorized access to your network. Firewall protection is available in both the Windows and MAC operating environments. If a firewall is misconfigured, meaning the rules are not configured properly, errors can occur and worse yet, the "bad guys" can gain access to your network and data. If you still suspect problems with your firewall, you should check the firewall's logging and look for errors. You might also check the security policies that have been set on the firewall.

Misconfigured ACLs/applications—Access lists (ACLs) are the basic form of firewall protection, although an access list is not stateful and is not by itself a firewall. Access lists can be configured on a router, on a true dedicated firewall, or on the host computer. The access lists consist of permit and deny statements to control traffic in and out of the network interface. There is an implicit denial at the end of an access list in Cisco routers, and this statement alone blocks all data packets. To allow other data packets that do not match the ACL's permit and deny statements to enter and exit the LAN, the command **access-list permit ip any any** must be added to the last line of an access list to explicitly allow all other data packets. If the intention is to deny other data packets that do match the permit statements, the explicit permit statement is not needed. The issue with misconfigured access lists is you may have opened a hole in the network allowing unauthorized user access. It is important that you test your own network and conduct penetration testing. A penetration test is a way to evaluate the security of the user's network. This is accomplished by trying to exploit vulnerabilities in the network. This includes identifying any potential problems with the operating systems, services, and applications as well as verifying user adherence to policies. The penetration test also validates any protection mechanisms currently in place.

Unreachable default gateway—When something like this happens, the problem could be a router has failed or the connection is down. A troubleshooting command to use is **tracert <*host*>** so that the router hops are listed and you can tell whether the gateway is reached. Make sure you either enter the default gateway's IP address or use an IP address not in the router's routing table so the data packets are sent to the default gateway.

Banner grabbing/OUI—Banner grabbing refers to error messages generated when a bad request is issued to a device in the network. The information contained in the error message might be enough for the "bad guy" to gain access to the network. It is also possible that the error message can contain its MAC address. The MAC address is 6 bytes, or 48 bits, in length. The address is displayed in 12 hexadecimal digits. The first six digits are used to indicate the vendor of the network interface, also called the **organizationally unique identifier (OUI)**, and the last six numbers form a unique value for each NIC assigned by the vendor. The OUI information lets the intruder know what kind of equipment is being used. At least for the network interface card, this provides the intruder with one piece of the puzzle about your network.

4.8 Given a scenario, troubleshoot and resolve common WAN issues

Loss of Internet connectivity—The connection to the Internet does go down on occasion. To verify that the Internet is down, try connecting to a different Internet site. If you still can't connect, then try a different computer. You need to eliminate any unknowns and the problem could possibly be with your computer, so try it and if the Internet connection is still down, you might try a different computer with a different Internet Service Provider.

Interface errors—It is important to verify that the interface to the WAN is properly configured. Next, ping the ISP's IP address. If this fails you can issue the **ping 127.0.0.1** command. This is the loopback address for your NIC. A reply back lets you know that your NIC is working. If the WAN connection is properly configured and the NIC is functioning, the problem could be with your ISP or telco (telephone company).

Split horizon—This is a technique used to prevent routing loops caused by a routing path being specified to send data packets back to the router that sent them. In split horizon, the packets are sent in a forward direction. The split horizon feature is integrated into distance vector routing protocols.

Interference—Interference problems with your WAN connection are not common, but any problems should be reported to your ISP or telco (telephone company). Interference problems can adversely affect your data throughput.

Smart jack/NIU—A smart jack is a network interface device that provides additional capabilities such as diagnostics. An NIU (Network Interface Unit) defines the demarcation point between telco and the customer's equipment (Customer Premise Equipment—CPE).

Copper line drivers/repeaters—This is primarily an issue with telco (telephone company). Land-based telephone systems use many miles of copper wire to get from the customer's site to the phone company's central office. The phone company provides line drivers and repeaters so that an acceptable signal can be received after traveling many miles.

Throttling—This is a technique used by communication carriers to regulate and manage network data traffic. The purpose of this is to minimize congestion on the network. This is also a technique used to prevent server crashes. Throttling limits upload and download capabilities.

Fair Access Policy/utilization limits—A Fair Access Policy or FAP is a company's policy used to set a network usage guideline for its users. This policy is intended for all users to receive an equitable share of network bandwidth. Also, this policy can be used to set the priority of the traffic based on the types of traffic. As a result, utilization limits can be set for users and different types of traffic.

5.0 INDUSTRY STANDARDS, PRACTICES, AND NETWORK THEORY

5.2 Explain the basics of network theory and concepts

De-multiplexing—Multiplexing is a communications system in which more than one signal is within a single channel. The process of de-multiplexing simply reverses the process and separates the multiplexed channel back into the individual channels.

Encapsulation/de-encapsulation—*Encapsulation* is a process where information is attached to the data packets in the *headers*. *De-encapsulation* is the process used when a data packet is received and the header is extracted.

Octal—This refers to the base-8 numbering system. The digits run from 0-1-2-3-4-5-6-7. It can also refer to the grouping of four numbers such as the four octets associated with an IPv4 address, 192.168.20.5, where each decimal number is represented by 8 binary numbers.

Speed—Speed is the rate in which data can be transmitted in a time interval. It currently is measured in bits per second (bps). In the old days, data transmission was modulated and transmitted over analog medium. Speed was measured as baud rate, which is a modulation rate.

Sampling size—The sampling size of digitized signals determines the dynamic range of the sampled systems. A general rule of thumb is that you get 6db/bit when sampling. Audio systems for CDs use 16-bit sampling and use an oversampling technique to provide 96db of dynamic range.

5.4 Given a scenario, deploy the appropriate wired connectivity standard

100BaseFX—This is a multimode fiber technology. It uses a 1300nm wavelength and is good for transmission lengths of 2km.

10Base2—This is a legacy coax cable network called ThinNet. The cable is terminated with BNC connectors, and the cable type is RG-58A/U.

10GBaseSR—This is a10-Gigabit Ethernet physical layer *standard* for use with multimode fibers for a short range of 300 meters to 400 meters.

10GBaseER—This is a10-Gigabit Ethernet physical layer *standard* for use with single mode fibers for extended range or reach up to 40 km.

10GBaseSW—This is a10-Gigabit Ethernet physical layer *standard* for WAN connection, which is designed for longer distance type connections like SONET by adding extra encapsulation support. The maximum distance for this standard is up to 80 km.

IEEE 1905-1-2013—This is an IEEE standard that integrates wired technologies with wireless connectivity. This standard includes the IEEE 1901 Standard for Broadcast over Power Lines.

Ethernet over HDMI—This standard provides for Ether connectivity via HDMI. The benefit is another cable is not required for an Ethernet connection. This enables multiple network devices to share a connection. Additionally this provides the potential for simplifying home theatre systems' connectivity.

Ethernet over power line—Simply put, this is a system that uses the electrical wiring in your home or business to transmit a modulated carrier signal containing Ethernet data. The technology requires an adapter connected to the home's Ethernet connection, and another adapter is connected anywhere in the house where an Ethernet connection is needed. These adapters can support data rates up to 80 Mbps.

Wiring standards—The wiring standards for modern computer networks are defined by the EIA/TIA 568-C standard. This standard defines specifications for 4-pair 100-ohm category 5e twisted-pair cabling. Defined within this standard are the CAT5e, CAT6, CAT7, and the RJ-45 (8P8C) twisted pair cable terminations.

5.5 Given a scenario, implement the appropriate policies or procedures

Consent to monitoring—Organizations are required to have a consent to monitoring policy in place. The intent is to protect the individual from unlawful observation. Most facilities also have guidelines in place about the use of cameras, particularly IP cameras. Your facility should have a checklist and training related to monitoring. All installations of cameras and their locations should be monitored, and installation should be coordinated with your organization's administration. The networking group should be involved with this so access to IP cameras is restricted.

MLA—MLA is a master license agreement that defines the owner rights, terms, and conditions of the intellectual property.

5.6 Summarize safety practices

Electrical safety—Some computers connect to the electrical outlet. You should always use caution when working with any electrical system. Best practice is to always disconnect electrical power prior to working inside any electrical device including computers. Always use caution when working with power supplies because the filter capacitors can hold a charge.

Grounding—All electrical devices should have a ground for safety. This includes the electrical devices used in computer networks, including devices mounted in the racks and the rack itself. Never remove the ground pin from an electrical device. That ground connection is there for a very good reason, to protect you.

ESD—ESD stands for electrostatic discharge. ESD can damage integrated circuits, so the technician should always use a grounding strap connected to his wrist to prevent any unwanted static discharge. The grounding strap is typically connected to the electrical ground.

Static—Any type of static discharge is undesirable around electronic systems. A static discharge can damage integrated circuits, so the technician should always use a grounding strap connected to her wrist to prevent any unwanted static discharge. The grounding strap typically connects to the electrical ground. The power should be disconnected and a grounding strap should be placed on the technician's wrist prior to opening any electronic equipment.

Installation safety—Installation safety rules are outlined in Federal Regulation 29 CFR PART 1926—SAFETY AND HEALTH REGULATIONS FOR CONSTRUCTION. Cabling installers are required to follow OSHA rules and general construction safety guidelines. It is critical that the technician be careful when climbing ladders installing racks.

Lifting equipment—Always use due caution when lifting heavy boxes. It is recommend that when lifting, you should bend at the knees and get someone to help you.

Rack installation—Racks are used in a multitude of places in network systems. The racks could be installed in closets or there could be many racks in a data center. You can also expect to have server rack frames with air blowing over the devices for cooling. Racks must be securely installed and grounded. Rack types vary for sites, but the most common are 19-inch rack frames. There also two-post racks used for smaller telecommunication equipment. Four-post racks are typically used for servers.

Placement—In a data center, you can expect the equipment to have locks on the racks for security reasons. These racks are placed in a well monitored area. You also have “hot” and “cold” aisles. The hot air from the equipment in the hot aisles is blown out of the racks and recirculates to the ceiling ducts. The cold aisles are where the air is being pulled through the equipment using its fans.

Tool safety—Tool safety is always of concern especially when power tools are involved. The technician must make sure all power tools are properly grounded. It is also important that you understand the purpose or intent of any tool you are working with. There is always a risk if you are trying to use the wrong tool for a job. Don’t take shortcuts.

Building layout—Always seek advice from an expert when planning the building layout for a networking or data center. There are many issues concerning safety, power distribution/requirements, grounding, shielding, heating and cooling considerations, fire suppressant systems, security, door access control, security cameras, and video monitoring. You also want to make sure you have room for growth. An expert can help you with planning this.

Fail-open/fail-close—When systems fail, there are two ways of responding. The two ways are fail-open and fail-closed. If a systems fails-open, this means everything is left the same as it was before the failure. Fail-closed implies that the system closes down when the problem occurs. The proper response depends on the system you are working with.

5.7 Given a scenario, install and configure equipment in the appropriate location using best practices

Cable management—If you are in a large office and campus network, cable management becomes an issue. The ANSI/TIA/EIA Administrative Standard for Telecommunications Infrastructure of Commercial Buildings describes how to manage your cable installation. This standard describes how your cable structure should be managed. Some of the topics outlined in the standard include drawings, reports, work orders, labeling, grounding, fire stopping, backbone cabling, cross connects, intra- and interbuilding cabling, building records, horizontal cabling, and types of cable.

Power management—Power for a campus network or a large data center has specific needs that must be addressed. For example, how do you address the failure of a power supply? The good news is it is practical to have redundant power supplies so that the system can switch to a new power supply if there is a failure. It is also possible that the electrical power could be coming from two different sources or two separate feeds from the electric company. How do you manage the loss of one power source? The threat of the loss of power is something you need to plan for because if it can happen, it will.

Power converters—The basic power converter is the power supply that converts the AC voltage from the electric company to a DC voltage used by the networking devices. Power supplies fail, so you need to have a plan in place to replace power supplies for your various networking devices. Other examples of power converters are solar panels (convert photons to electricity) and backup generators, which convert mechanical energy to electrical energy.

Circuits—This is referring to the electrical circuits that power your clients' networking equipment or the equipment in your data center. There are many issues concerning power distribution/requirements, grounding, and shielding. Consulting with an expert is a good step.

Inverters—An inverter or a power inverter is a device that converts DC (direct current) into AC (alternating current). This enables generation of AC power for your appliances when your only power source is a DC voltage source, such as a battery.

Power redundancy—Simply put, this means that you are operating with backup power supplies and/or a backup generator. The system is typically designed to automatically switch over to the backup system if power is lost.

Device placement—Device placement in a networking facility or a data center can be important. You don't want to have your staff bumping into each other or continually having to walk long distances to fix problems. Your objective is to thoughtfully place your equipment so that access is easy, and normal operations are not impeded.

Cable trays—The purpose of cable trays is to provide a place to hold cable runs to keep the cables secured away from other items such as pipes, steam, water, people, and so on. Cable trays are found in ceilings, tunnels, and inside walls.

Rack systems—The purpose of your rack systems is to mount your equipment. While mounting the equipment make sure you have equipment properly consolidated and you have allowed sufficient access to the back side of the equipment for the technician to troubleshoot problems and make repairs/changes. You also want to make sure that cable pathways in the racks are well defined and you have provided room for growth.

Server rail racks—This provides an easy way to replace servers by simply pulling them out from the racks and installing the replacement device.

Two-post racks—Two-post racks are often used for smaller telecommunication equipment. These systems just provide two rack posts for rack mounting the equipment. There are also less expensive than racks that have doors and are fully enclosed.

Four-post racks—Four-post racks are typically used for servers and larger electronic systems. They can have open sides or do have the options for enclosures and doors.

Free-standing racks—These are just racks of different sizes and shapes that are free-standing and used for many different situations.

Labeling—Labeling is important for all aspects of your computer network and data center. To begin with, all racks should be labeled identifying the purpose of the equipment installed in the rack. For example, maybe the rack houses the telecommunication equipment that connects to your WAN connection. Another example is to label names for your server that identify the purpose and possibly the name of the server machine. Another important label is for cabling. Both cable ends or wall plates should be labeled with some identifying marks that correspond to your building drawings. This makes it possible for the technician to easily identify the cable and its path.

Port labeling—When labeling your equipment and cabling, develop a standardized format that contains all the information you will need at a later time. Remember, your facility will eventually have a lot of equipment and cables, and being able to easily identify these will be of great benefit to the technical staff. Also make sure the labels correspond to your drawings.

System labeling—These labels are important so that the technical staff are referencing the same system. A large facility will eventually have many systems doing similar tasks, and being able to identify the correct system will simplify your work.

Circuit labeling—In this case, we are referring to labeling your electrical power circuits. This is important for documenting breakers that trip and identifying why this happened. It could be that you have too many devices on the circuit. You also want to have circuits labeled so you know exactly what systems are being affected if the breaker has to be shut off.

Naming conventions—You will probably want to develop a naming strategy for your networking equipment. For example, maybe your computers are named according to the building and room number and then machine number. For example brown-rm35-275. This makes it easy for the technician to easily identify the location of the machine.

Patch panel labeling—You need to label all patch panels so you can easily identify the source and destination when connecting a jumper cable. The normal convention is that sources (outputs) are on top, and destination (inputs) are on the bottom.

Rack monitoring—Critical systems need to be monitored for possible tampering or just to have visual confirmation why something is being changed. You might be monitoring who entered certain locked cabinets. A quick review of the trouble reports should quickly explain who and why someone was in the rack.

Rack security—The racks could house equipment that processes secure data or could be connected to a secure connection, and monitoring the rack would be mandatory. Racks can also provide protection against unauthorized access and prevent unauthorized changes to the network.

Intermediate distribution frame—An intermediate distribution frame or IDF connects back to the main distribution frame (MDF). This wiring closet typically exists when an MDF cannot support the distance of the cable run.

Air flow—In data centers, server racks must be positioned in such a way to take advantage of air flow. Racks are positioned with alternating cold aisles and hot aisles, where equipment fans can draw cold air from a cold aisle and vent its hot air to a hot aisle.

5.8 Explain the basics of change management procedures

Configuration procedures—What operating system are you going to install on the many computers you manage? What problems do you foresee if you upgrade the OS? What about people's preferences? How will this configuration change affect your company? The bottom line is you need to have a procedure in place to manage changes to your system and your equipment so your questions and concerns can be addressed. It is important that your changes be well documented.

Rollback process—You just made changes to your network, but it doesn't work properly. In your configuration process, you want to have a plan for a rollback to the previous version or hardware. Good documentation is still a must, and notifying all affected personnel is extremely important.

Potential impact—Anytime you make changes, particularly technical changes, it is going impact your staff and your system. What if you are planning to make the move to cloud-based services? How is this going to impact your staff and your overall operation? Don't make changes without putting a lot of thought into it. The objective is to plan your transitions carefully to avoid major disturbances with your budget, your technical operations, and your staff.

Notification—It is of paramount importance that you make sure all users of your system are notified of any planned downtimes for scheduled maintenance and upgrades. It is also equally important to notify your users, staff, and help desk of any plans to discontinue support for software or hardware or your plan to upgrade to a newer software or hardware technology.

Approval process—Make sure you have an approval process in place to monitor changes. You always want to have a record that the change was approved. This can be online or a paper trail, but it is important to keep a record. The approval process should outline the steps for approval and who should approve each step in the process. The approval process can also outline what steps are to be taken if the request is withdrawn or rejected.

Authorized downtime—It is important that planned downtime be authorized. You need to have an approval process in place to track this. It is also important to know what downtime is actually costing you and your organization. You also want to know whether a recovery time is associated with the planned downtime. Downtime is unavoidable, but the objective is to keep this to a minimum. It is also important to know how much downtime your organization can afford. Some highly critical systems can't afford any downtime.

Notification of change—If a change is planned for your organization, make sure your support staff, the help desk personnel, and your customers are aware of this change. It is also a good idea to let everyone know what the possible impact of the change might be.

5.9 Compare and contrast the following ports and protocols

2427/2727 MGCP—This is the Media Gateway Protocol. The Media Gateway Control Protocol (MGCP) is a protocol used within a distributed Voice over IP system. This is also called H.248, and its purpose is to handle signal and session management that is used in real-time multimedia conferences. It essentially provides a way to convert data from a packet-switched network to a circuit-switched network.

PROBLEMS

Section 1.0—Network Architecture (supplement)

1. What is the purpose of HIDS?

   a. This system identifies misuse or potential attacks by matching the data packets against known signatures that have been classified as bad.

   b. A device that sits between the campus network and the outside network. The device is set up so that all data traffic, incoming and outgoing, passes through it.

   c. This is an intrusion detection system that monitors the computer system for changes, such as system file modifications, changes to the registry, file changes, and system logs.

   d. All of the above.

2. What is the purpose of a content filter?

   a. This is a web filter appliance that monitors the web traffic via both HTTP and HTTPS and matches it against the database. If an inappropriate website is detected, it is either discarded or the user is redirected to a security web page for further action.

   b. This device is used to stop or prevent malicious attacks that it detects by interacting with the firewall.

   c. This device identifies misuse and any anomaly on the network by matching the network packets with its IPS signatures for known attacks or activities that are classified as bad.

   d. This device is configured to prevent malicious activity on the host system, and if an unauthorized change or activity is detected, an alert is issued.

3. What is the purpose of SNAT?

   a. This is used to ensure that a DHCP client always receives the same IP address when it reconnects.

   b. This device enables private network data traffic to go out to the Internet, so it can reach the public network through a single gateway public IP address.

   c. This allows any host on the "outside" of the network to get to a single host on the "inside" of the network.

   d. None of the above.

4. What is the purpose of scopes ?

   a. This step is used to authenticate the user, establish the session, and set policies.

   b. This allows any host on the "outside" of the network to get to a single host on the "inside" of the network.

   c. The purpose of this is to authenticate users and network devices in domain environments.

   d. This is a grouping of IP addresses that use the DHCP (Dynamic Host Control Protocol) service for a group of computers located on a subnet.

5. Define MPLS.

   a. This is a technique for combining multiple signals on laser beams for transmission.

   b. This device is used to connect two UTP cables.

   c. This is a data-carrying service for telecommunication networks that route data from one network node to the next based on labels for short path rather than long network addresses.

   d. These devices allow a single fiber to be split into two outputs, and multiple input fibers can be combined into one output fiber.

6. What is near field communications?

   a. NFC systems are computer-based systems associated with the monitoring and control of industrial processes.

   b. NFC is a set of communication protocols used to enable two electronic devices to communicate.

   c. NFC systems are designed to withstand the harsh environment of industry.

   d. NFC systems are designed to operate and monitor the critical industrial infrastructure.

7. What is an ICS server?

   a. ICS systems are computer-based systems associated with the monitoring and control of industrial processes.

   b. This is a data-carrying service for telecommunication networks that route data from one network node to the next based on labels for short path rather than long network addresses.

   c. Industrial control systems servers are designed to withstand the harsh environment of industry.

   d. None of the above.

8. What is a medianet?

   a. This is an intelligent network that has been optimized for high traffic video applications.

   b. This is a system that has multiple subsystem controllers geographically dispersed throughout the network.

   c. This is a control unit designed to support SCADA remote stations.

   d. This device is used for control of machinery in manufacturing and related industries.

9. What is the purpose of autoconfiguration?

   a. This option allows the router to choose its own host identifier (rightmost 64 bits) from the EUI-64 (Extended Universal Identifier-64) of the interface.

   b. This is an IPv6 feature. With IPv6, a computer can automatically configure its network settings without a DHCP server by sending a solicitation message to its IPv6 router.

   c. This is a data-carrying service for telecommunication networks that route data from one network node to the next based on labels for short path rather than long network addresses.

   d. None of the above.

10. What is EUI 64?

   a. This is a tunneling protocol that provides IPv6 connectivity for IPv6 capable devices that are on an IPv4 platform.

   b. This is a data-carrying service for telecommunication networks that route data from one network node to the next based on labels for short path rather than long network addresses.

   c. This is an intelligent network that has been optimized for high traffic video applications.

   d. This option allows the router to choose its own host identifier (rightmost 64 bits) from the EUI-64 (Extended Universal Identifier-64) of the interface.

11. What is route redistribution?

   a. This is a preferred method for router IP packets.

   b. Routing redistribution is the technique of injecting routes from one routing protocol to another routing protocol.

   c. This is the replacement for RIP.

   d. This is a low overhead solution to routing.

12. What is HSRP?

    a. This is the Hot Standby Router Protocol. This protocol enables a framework of routers so that a default gateway is always available, hence the status of "Hot Standby."

    b. This is the High Source Routing Protocol, and this protocol enables a framework of routers so that a default gateway is always available.

    c. This is the Hot Standby Router Protocol, and it provides automatic assignment of routers to hosts participating in the network.

    d. All of the above.

13. Select three QoS issues for VoIP networks. (Select three of the following.)

    a. Route selection

    b. Jitter

    c. Shortest path bridging

    d. Network latency and packet loss

    e. Queuing

    f. Unified communications

14. What is a virtual firewall?

    a. This device is built to handle any type of failure.

    b. This network device is used to provide access to multiple servers.

    c. This network device provides access to the network and in particular the Internet.

    d. This is a network device running in a virtual environment. This device provides the same functionality as a physical firewall.

15. Which of the following is true about the cloud?

    a. The cloud is just another name for the Internet.

    b. Setting up and physically connecting to the cloud is virtually the same for all operating systems (OS) and computers.

    c. Access to the cloud can be limited for users.

    d. The advantage of the cloud is the reduced overhead.

Section 2—Network Operations (supplement)

16. What is the name for an operation used to enable an agent to notify the SNMP network management station (NMS) of significant events?

    a. SIEM

    b. MIB

    c. Walk

    d. TRAP

17. What is SYSLOG? (Select two.)

    a. IT security system that can provide a holistic view and real-time analysis of an organization's IT security.

    b. It is a standard protocol used to collect log messages sent from devices to a server running a SYSLOG service or daemon.

    c. Servers run on UDP port 514 or TCP port 601.

    d. None of the above.

18. What is NAC?

    a. This is an IT security system that can provide a holistic view and real-time analysis of an organization's IT security.

    b. It is a security mechanism that can be implemented on a network to register, authenticate, authorize, and enforce security policies on all endpoint devices before they are allowed to access the network.

    c. This is a network device running in a virtual environment.

    d. All of the above.

19. Which of the following applies to "legacy systems?" (Select the best answer.)

    a. Legacy systems can be categorized as "end-of-life" or "end-of-support."

    b. Legacy systems should be decommissioned as soon as possible.

    c. A legacy system is more vulnerable and susceptible to security hacks and exploitations.

    d. One of the biggest security risks for a legacy system is there will not be a firmware, hardware, or software update.

    e. All of the above.

20. This is a computing environment specifically set up to gather information regarding network attacks and intrusions and to study the vulnerabilities of a system.

    a. Honeypot

    b. SCADA

    c. NAC

    d. Scope

21. Define VTP.

    a. VTP or VLAN Tunneling Protocol is Cisco's proprietary protocol used to manage and propagate the VLAN definitions of all the VTP-capable switches.

    b. VTP or VLAN Tunneling Protocol is Cisco's proprietary protocol used to manage and store the VLAN definitions of all the VTP-capable switches.

    c. VTP or VLAN Trunking Protocol is Cisco's proprietary protocol used to manage and propagate the VLAN definitions of all the VTP-capable switches.

    d. This means the same subnet can span different physical ports or user locations. This allows for greater flexibility to have many locations sharing the same subnet.

22. This allows for multiple physical ports on an Ethernet switch to be bundled as one single logical channel.

    a. Port mirroring

    b. Port enabling

    c. Port sharing

    d. Port bonding

23. What is VLAN pooling?

    a. This is a technique where a MAC address is shared with multiple computers in the same VLAN.

    b. VLAN pooling is a solution offered by many wireless manufacturers to deal with the large number of connecting wireless devices, and every device is required to have an IP address.

    c. VLAN pooling is a solution offered by many wireless manufacturers to deal with connecting wireless devices, and every device is required to have a MAC address.

    d. This is a technique where an IP address is shared with multiple computers in the same VLAN.

24. Define Goodput. (Select two.)

    a. Goodput refers to the actual wireless data throughput as measured by an application on the end device.

    b. Goodput is the underlying wireless control protocol for Cisco APs to communicate with wireless controllers.

    c. Goodput is a way to represent the actual transmission rate of a wireless connection, which is not the maximum theoretical transmission rate.

    d. Goodput is the underlying wireless control protocol for Cisco APs to communicate with Ethernet controllers.

25. Define device density.

    a. This defines the number of Ethernet clients.

    b. This is defined by Thick clients.

    c. This means the same subnet can span different physical ports or user locations.

    d. This is the number of connecting wireless clients.

Section 3—Network Security (supplement)

26. What is a botnet?

    a. This is an IT group responsible for servicing all organizations within a business. Also call a BizNet.

    b. This is an attack where an attacker can seamlessly place itself in the middle of the conversation of others.

    c. This is a group of infected or compromised computers on the Internet that is being used to launch coordinated denial of service attacks against another system on the network.

    d. This is a technique used in man-in-the-middle attacks.

27. What is a type of distributed denial of service attack that is deliberately toward a specific target and is orchestrated by a controller source like the command and control server in a botnet?

    a. Evil twin

    b. Coordinated attack

    c. Reflective attack

    d. War chalking

28. What is Bluejacking? (Select two.)

    a. These are attacks on Bluetooth devices.

    b. This is an attack to gain unauthorized access of another Bluetooth device over the Bluetooth connection with the intention to obtain information stored on the Bluetooth device.

    c. This is a process in which attackers search Bluetooth devices for an open wireless network connection, so that they can gain more access to collect information or data of connecting users.

    d. This is the exploitation of a valid Bluetooth device with the intent to gain unauthorized access.

29. Define session hijacking.

    a. This is an attack to gain information or resources that are only available in specific VLANs.

    b. This is generally referred to as a computer, a group of computers, or a part of the network that has been adversely impacted by an untrusted source.

    c. This is an exploitation of vulnerability in software that is unknown to the developer.

    d. This is the exploitation of a valid computer session to gain unauthorized access to information or services on a computer.

30. What is TEMPEST? (Select the correct answer.)

    a. This is a standard for computer systems certification commenced by the US government in the late 1950s.

    b. This refers to the exploitation of vulnerability in government software that is unknown to the developer.

    c. This specifies the amount of Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) or RF emanation emitted by a device.

    d. The purpose of TEMPEST is to shield the wireless RF signal within the area and not divulge intelligence about system information.

31. What is TLS? (Select two.)

    a. This is used by the **ping** command to verify packet delivery.

    b. This is an authentication protocol for Windows Active Directory.

    c. This is the successor to the Secure Sockets Layer (SSL), and it is designed to ensure the privacy between the communicating parties.

    d. TLS ensures that no third party may eavesdrop or tamper with any messages between a server and a client.

32. What is Unified Threat Management (UTM)?

    a. This is generally referred to as a computer, a group of computers, or a part of the network that has been unified.

    b. This is the authentication protocol for Windows Active Directory.

    c. This is an all-in-one solution that integrates a wide range of security features into one appliance.

    d. None of the above.

33. This is a special segmented network provided to visitors to access the Internet and certain unrestricted networks. (Select one.)

    a. Persistent agent

    b. Guest network

    c. Posture

    d. Virtual segment

34. What is single sign-on? (Select the best answer.)

    a. Single sign-on (SSO) is a process that permits users to access different systems after one successful authentication.

    b. Single sign-on (SSO) is a process that permits guests to access different systems.

    c. This is used to control or minimize internal access by limiting the number of times you can connect to a system.

    d. All of the above.

Section 4—Troubleshooting (supplement)

35. What is meant by divide and conquer?

    a. This is a basic troubleshooting approach for UTP cable.

    b. Using this troubleshooting approach, an OSI layer is selected and tested for its functionality. If this layer is good, then the technician tests the next layer, which could be higher or lower.

    c. A basic function related to cabling that is used to verify two ends are connected.

    d. All of the above.

36. What is a looking glass site?

    a. A site used to run connectivity tests.

    b. A site used to obtain routing information related to the network's backbone and efficiency.

    c. A network site that has a fragile connection.

    d. A site used so a speed test can be run to measure a computer's upload and download speeds.

37. What are the most common frequency channels used in wireless communication?

    a. 1,6,11

    b. 2,7,9

    c. 1,2,3

    d. 1, 5, 10

38. What is the operating frequency for 802.11a?

    a. 5 GHz

    b. 2.4 GHz

    c. 2.4 GHz and 5 GHz

39. What is the operating frequency for 802.11b?

    a. 5 GHz

    b. 2.4 GHz

    c. 2.4 GHz and 5 GHz

40. What is the operating frequency for 802.11n?

    a. 5 GHz

    b. 2.4 GHz

    c. 2.4 GHz and 5 GHz

41. What is the operating frequency for 802.11ac?

    a. 5 GHz

    b. 2.4 GHz

    c. 2.4 GHz and 5 GHz

42. What is LWAPP?

    a. The system provides for the assignment of a primary, secondary, and even a tertiary controller for the wireless network.

    b. This protocol can be used to simplify the control of multiple wireless access points at the same time.

    c. This is the Lightweight Access Protocol.

    d. All of the above.

43. Which of the following is true for MTU? (Select two.)

    a. MTU stands for Maximum Transmission Unit. For Ethernet networks, the MTU is 1518 bytes.

    b. This stands for Multimedia Transcriber Unit. It is assigned to data packets to avoid black holes.

    c. A misconfigured MTU results in nondelivery of the data packet.

    d. An MTU black hole is a result of a misconfigured router resulting in data packets not being properly delivered.

44. Which of the following are issues with a misconfigured firewall?

    a. A bad request is issued to the network.

    b. Timing on stateful connection is affected.

    c. Penetration testing will be useless.

    d. Errors can occur and worse yet, the "bad guys" can gain access to your network and data.

45. What is banner grabbing and why is this important? (Choose two.)

    a. Refers to error messages generated when a bad request is issued to a device in the network.

    b. This is used to verify that a penetration test was successful.

    c. This is used to verify the integrity of the MAC address.

    d. The information contained in the error message might be enough for the "bad guy" to gain access to the network.

46. Which of the following is a technique used to prevent routing loops caused by a routing path being specified to send data packets back to the router that sent them?

   a. Loop grabbing

   b. TTL

   c. Throttling

   d. Split horizon

Section 5—Industry standards, practice, and network theory (supplement)

47. What is Ethernet over HDMI?

   a. This made RJ-45 connectors compatible with HDMI.

   b. This made 8P8C connectors compatible with HDMI.

   c. This is intended to speed up HDMI network connections.

   d. This standard provides for Ether connectivity via HDMI.

48. This is a system that uses your electrical wiring in your home or business to transmit a modulated carrier signal containing Ethernet data.

   a. Ethernet over 120

   b. Ethernet over AC

   c. Ethernet over power line

   d. Ethernet over zip line

49. What is the name for the wiring standards for modern computer networks?

   a. IEEE 802.1

   b. IEEE 802.11

   c. EIA/TIA 568-C

   d. EIA/TIA 395-B

50. What is the purpose of a consent to monitoring policy? (Select the best answer.)

   a. The intent is to protect the individual from excessive oversight.

   b. To ensure the IT group adheres to copyright laws.

   c. To maintain oversight of computer installations.

   d. The intent is to protect the individual from unlawful observation.

51. This is the power supply that converts the AC voltage from the electric company to a DC voltage used by the networking devices. (Select two.)

   a. Power inverter

   b. Inverter

   c. Induction system

   d. Sweeping system

52. Why is labeling important? (Select the best answer.)

  a. All racks should be labeled identifying the purpose of the equipment installed in the rack.

  b. Label names for your server that identify the purpose and possibly the name of the server machine.

  c. Cable ends or wall plates should be labeled with some identifying marks that correspond to your building drawings.

  d. All of the above.

53. What is the rollback process?

  a. A plan to decrease data storage

  b. A plan to make room for upgrades

  c. A plan for a rollback to the previous version or hardware

  d. None of the above

54. What is the purpose of the Media Gateway Protocol and the port numbers?

  a. MGCP is a protocol used within a distributed Voice over IP system. It uses ports 2427/2727.

  b. MGCP is a protocol used within data storage for multimedia applications. It uses ports 2001/2002.

  c. MGCP is a protocol used for distributed Internet connections. It uses ports 1298/1398.

  d. MGCP is a protocol used within a distributed Voice over IP system. It uses ports 2427/2428.