STUDY GUIDE

CompTIA

Network+ N10-004

ExamForce

About the Exam

There are six major topic areas that make up this Network+ (2009 edition) exam. The percentage listed indicates the level of focus within the exam, but must not be taken as an exact, strict number. In other words, 20% percent of the exam's weight will be the topic of Network Technologies.

- Network Technologies - 20%
- Network Media Topologies - 20%
- Network Devices - 17%
- Network Management - 20%
- Network Tools - 12%
- Network Security - 11%

This guide walks you through all of the technologies in the objectives and sub-objectives as published by CompTIA.

Domain 1.0: Network Technologies

1.1 Explain the function of common networking protocols

- TCP
- FTP
- UDP
- TCP/IP suite
- DHCP
- TFTP
- DNS
- HTTP(S)
- ARP
- SIP (VoIP)
- RTP (VoIP)
- SSH
- POP3
- NTP
- IMAP4
- Telnet
- SMTP
- SNMP2/3
- ICMP
- IGMP
- TLS

1.2 Identify commonly used TCP and UDP default ports

- TCP ports
- FTP – 20, 21
- SSH – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- HTTP – 80
- POP3 – 110
- NTP – 123
- IMAP4 – 143
- HTTPS – 443
- UDP ports
- TFTP – 69
- DNS – 53
- BOOTPS/DHCP – 67
- SNMP – 161

1.3 Identify the following address formats

- IPv6

- IPv4
- MAC addressing

1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes

Addressing Technologies

- Subnetting
- Classful vs. classless (e.g. CIDR, Supernetting)
- NAT
- PAT
- SNAT
- Public vs. private
- DHCP (static, dynamic APIPA)

Addressing schemes

- Unicast
- Multicast
- Broadcast

1.5 Identify common IPv4 and IPv6 routing protocols

Link state

- OSPF
- IS-IS

Distance vector

- RIP
- RIPv2
- BGP

Hybrid

- EIGRP

1.6 Explain the purpose and properties of routing

- IGP vs. EGP
- Static vs. dynamic
- Next hop
- Understanding routing tables and how they pertain to path selection
- Explain convergence (steady state)

1.7 Compare the characteristics of wireless communication standards

- 802.11 a/b/g/n
    - Speeds
    - Distance
    - Channels
    - Frequency
- Authentication and encryption
    - WPA
    - WEP

- RADIUS
- TKIP

Domain 2.0: Network Media Topologies

2.1 Categorize standard cable types and their properties

Type:

- CAT3, CAT5, CAT5e, CAT6
- STP, UTP
- Multimode fiber, single-mode fiber
- Coaxial
  - RG-59
  - RG-6
- Serial
- Plenum vs. Non-plenum

Properties:

- Transmission speeds
- Distance
- Duplex
- Noise immunity (security, EMI)
- Frequency

2.2 Identify common connector types

- RJ-11
- RJ-45
- BNC
- SC
- ST
- LC
- RS-232
- RG-59
- RG-6

2.3 Identify common physical network topologies

- Star
- Mesh
- Bus
- Ring
- Point to point
- Point to multipoint
- Hybrid

2.4 Given a scenario, differentiate and implement appropriate wiring standards

- 568A
- 568B
- Straight vs. cross-over

- Rollover
- Loopback

2.5 Categorize WAN technology types and properties

Type:

- Frame relay
- E1/T1
- ADSL
- SDSL
- VDSL
- Cable modem
- Satellite
- E3/T3
- OC-x
- Wireless
- ATM
- SONET
- MPLS
- ISDN BRI
- ISDN PRI
- POTS
- PSTN

Properties

- Circuit switch
- Packet switch
- Speed
- Transmission media
- Distance

2.6 Categorize LAN technology types and properties

Types:

- Ethernet
- 10BaseT
- 100BaseTX
- 100BaseFX
- 1000BaseT
- 1000BaseX
- 10GBaseSR
- 10GBaseLR
- 10GBaseER
- 10GBaseSW
- 10GBaseLW
- 10GBaseEW
- 10GBaseT

Properties

- CSMA/CD
- Broadcast
- Collision
- Bonding
- Speed
- Distance

2.7 Explain common logical network topologies and their characteristics

- Peer to peer
- Client/server
- VPN
- VLAN

2.8 Install components of wiring distribution

- Vertical and horizontal cross connects
- Patch panels
- 66 block
- MDFs
- IDFs
- 25 pair
- 100 pair
- 110 block
- Demarc
- Demarc extension
- Smart jack
- Verify wiring installation
- Verify wiring termination

Domain 3.0: Network Devices

3.1 Install, configure and differentiate between common network devices

- Hub
- Repeater
- Modem
- NIC
- Media converters
- Basic switch
- Bridge
- Wireless access point
- Basic router
- Basic firewall
- Basic DHCP server

3.2 Identify the functions of specialized network devices

- Multilayer switch
- Content switch
- IDS/IPS
- Load balancer
- Multifunction network devices
- DNS server
- Bandwidth shaper
- Proxy server
- CSU/DSU

3.3 Explain the advanced features of a switch

- PoE
- Spanning tree
- VLAN
- Trunking
- Port mirroring
- Port authentication

3.4 Implement a basic wireless network

- Install client
- Access point placement
- Install access point
  - Configure appropriate encryption
  - Configure channels and frequencies
  - Set ESSID and beacon
- Verify installation

Domain 4.0: Network Management

4.1 Explain the function of each layer of the OSI model

- Layer 1 – physical
- Layer 2 – data link
- Layer 3 – network
- Layer 4 – transport
- Layer 5 – session
- Layer 6 – presentation
- Layer 7 – application

4.2 Identify types of configuration management documentation

- Wiring schematics
- Physical and logical network diagrams
- Baselines
- Policies, procedures and configurations
- Regulations

4.3 Given a scenario, evaluate the network based on configuration management documentation

- Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure
- Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed

4.4 Conduct network monitoring to identify performance and connectivity issues using the following:

- Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)
- System logs, history logs, event logs

4.5 Explain different methods and rationales for network performance optimization

Methods:

- QoS
- Traffic shaping
- Load balancing
- High availability
- Caching engines
- Fault tolerance

Reasons:

- Latency sensitivity
- High bandwidth applications
  - VoIP
  - Video applications
- Uptime

4.6 Given a scenario, implement the following network troubleshooting methodology

- Information gathering – identify symptoms and problems
- Identify the affected areas of the network
- Determine if anything has changed
- Establish the most probable cause
- Determine if escalation is necessary
- Create an action plan and solution identifying potential effects
- Implement and test the solution
- Identify the results and effects of the solution
- Document the solution and the entire process

4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution

Physical issues:

- Cross talk
- Nearing cross talk
- Attenuation
- Collisions
- Shorts
- Open impedance mismatch (echo)
- Interference

Logical issues:

- Port speed
- Port duplex mismatch
- Incorrect VLAN
- Incorrect IP address
- Wrong gateway
- Wrong DNS
- Wrong subnet mask

Issues that should be identified but escalated:

- Switching loop
- Routing loop
- Route problems
- Proxy arp
- Broadcast storms

Wireless Issues:

- Interference (bleed, environmental factors)
- Incorrect encryption
- Incorrect channel
- Incorrect frequency
- ESSID mismatch
- Standard mismatch (802.11 a/b/g/n)
- Distance
- Bounce
- Incorrect antenna placement

Domain 5.0: Network Tools

5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality

- Traceroute
- Ipconfig
- Ifconfig
- Ping
- Arp ping
- Arp
- Nslookup

- Host
- Dig
- Mtr
- Route
- Nbtstat
- Netstat

5.2 Explain the purpose of network scanners

- Packet sniffers
- Intrusion detection software
- Intrusion prevention software
- Port scanners

5.3 Given a scenario, utilize the appropriate hardware tools

- Cable testers
- Protocol analyzer
- Certifiers
- TDR
- OTDR
- Multimeter
- Toner probe
- Butt set
- Punch down tool
- Cable stripper
- Snips
- Voltage event recorder
- Temperature monitor

Domain 6.0: Network Security

6.1 Explain the function of hardware and software security devices

- Network based firewall
- Host based firewall
- IDS
- IPS
- VPN concentrator

6.2 Explain common features of a firewall

- Application layer vs. network layer
- Stateful vs. stateless
- Scanning services
- Content filtering
- Signature identification
- Zones

6.3 Explain the methods of network access security
Filtering:
- ACL
  - MAC filtering
  - IP filtering
- Tunneling and encryption
  - SSL VPN
  - VPN
  - L2TP
  - PPTP
  - IPSEC
- Remote access
  - RAS
  - RDP
  - PPPoE
  - PPP
  - VNC
  - ICA

6.4 Explain methods of user authentication
- PKI
- Kerberos
- AAA
  - RADIUS
  - TACACS+
- Network access control
  - 802.1x
- CHAP
- MS-CHAP
- EAP

6.5 Explain issues that affect device security
- Physical security
- Restricting local and remote access
- Secure methods vs. unsecure methods
  - SSH, HTTPS, SNMPv3, SFTP, SCP
  - TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2

6.6 Identify common security threats and mitigation techniques
Security threats
- DoS
- Viruses
- Worms
- Attackers
- Man in the middle

- Smurf
- Rogue access points
- Social engineering (phishing)

Mitigation techniques

- Policies and procedures
- User training
- Patches and updates

Domain 1.0 – Network Technologies

Chapter 1

Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5
- Objective 6

1.1 Explain the function of common networking protocols

TCP

TCP is a connection oriented protocol that provides reliable end-to-end delivery service. With TCP establishing a connection involves initiating the three-way handshake process. Before a client can connect with a server for example, the server must first bind to a port and open it for connections.

TCP uses a sequence number for identifying each byte of data it processes. It also makes use of a cumulative acknowledgment scheme. The end-to-end flow control mechanism, known as a sliding window, is used to keep the sender's data from overwhelming the receiver by sending too much at once.

FTP

FTP is a connection oriented file transfer protocol. It differs from TFTP in that FTP uses TCP, while TFTP uses the connectionless UDP protocol for delivery.

UDP

UDP is connectionless protocol that provides very few error recovery services. It is considered to be a "best effort" service. The benefit of UDP is that it offers a very direct way to send and receive datagrams over an IP network. Because of these factors, UDP is faster than TCP. Typically, if your network is very stable, UDP can provide higher efficiency, whereas TCP provides more verification for less stable networks. UDP is often used in time sensitive applications such as video conferencing.

TCP/IP suite

This is the language suite of the internet. Its reference model has four layers, which are the link layer, the network layer, the transport layer, and the application layer. TCP provides reliable, order-specific delivery of data streams. If errors are detected, it will retry delivery. IP, on the other hand, provides unreliable service on a best effort basis, thus there is no guarantee for communications. It does attempt to ensure individual packet headers are error-free via a checksum algorithm.

DHCP

DHCP, or Dynamic Host Configuration Protocol, is a protocol used for assigning dynamic IP addressing information to network devices.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address as this is done automatically.

TFTP
As previously stated, TFTP uses the connectionless UDP protocol for data delivery. Due to its connectionless nature, UDP provides very few error recovery services and instead offers a very direct way to send and receive datagrams over an IP network. Because of this, TFTP is more efficient in terms of performance.

DNS
DNS, or Domain Name System, translates host names to IP addresses. This allows a human to enter a text-based name and have it translated to the corresponding IP address that network devices understand. One easy way to verify whether DNS is working is to use command line utilities such as Nslookup. This allows administrators to display specific information and diagnose problems with the DNS infrastructure.

HTTP(S)
HyperText Transport Protocol is the protocol for moving hypertext files across the Internet. It requires an HTTP client program on one end and an HTTP server program on the other end. This is typically a web server and a web browser. HTTP is the most prevalent protocol used in the World Wide Web (WWW). HTTPS is the Secure and Encrypted form of HTTP. Since HTTP sends data in clear text, HTTPS helps to secure it through SSL encryption.

ARP
Address Resolution Protocol (ARP) translates IP addresses to hardware or MAC addresses. ARP is not an IP-only or Ethernet-only protocol. It can also be used to resolve many different types of network-layer protocol addresses to the corresponding hardware addresses. Reverse ARP (RARP) works the other way by translating Layer 2 (hardware) addresses to Layer 3 (network) addresses.

SIP (VoIP)
The Session Initiation Protocol (SIP) is an application-layer control protocol used in VoIP implementations for signaling. SIP clients rely on either TCP or UDP port 5060 for connecting to SIP servers and endpoints. The benefits of SIP include the facts that it is Lightweight and Transport independent, it is peer-to-peer, and is text based. This makes the protocol more reliable in time sensitive applications.

RTP (VoIP)
Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) are often used together. RTP is for transmitting data and RTCP is for control and QoS monitoring. The cRTP (Compressed RTP) protocol can compress voice packet header to a few bytes. This works on a hop-by-hop basis.

RTP uses dynamic ports, typically in the range of 16384 to 32767. RTCP uses the next highest numbered port from the one chose by RTP. Call setup and tear-down is primarily performed through the SIP protocol. Separate sessions are used for carrying different types of media content.

SSH
Secure Shell (SSH) allows data to be exchanged via a secure channel between two hosts. Encryption allows for confidentiality and integrity of data over the insecure internet. Public-key

cryptography is used for authenticating the remote host and to allow the remote host to authenticate the user as needed.

POP3

Short for Post Office Protocol (version 3), POP3 is a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can also use the newer IMAP (Internet Message Access Protocol). There are two versions of POP. The first, called POP2, became a standard in the mid-80s and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

NTP

Network Time Protocol (NTP) is a protocol mainly for synchronizing the clocks of a group of computer systems over a packet-switched, variable-latency data network. It works via UDP port 123. An example of this protocol in use is the Windows Time Service, which offers the ability to synchronize the local system clock to an NTP server on the network or the Internet.

IMAP4

Short for Internet Message Access Protocol (version 4), IMAP4 is a protocol for retrieving e-mail messages. The latest version of IMAP is similar to POP3 but supports some additional features. For example, with IMAP4, you can search through your e-mail messages for keywords while the messages are still on the mail server. You can then choose which messages to download to your machine.

Telnet

Telnet is a protocol for remote computing on the Internet. It allows a computer to act as a remote terminal on another machine, anywhere on the Internet. This means that when you telnet to a particular host and port, the remote computer (which must have a telnet server) accepts input directly from your computer (which must have a telnet client) and output for your session is directed to your screen.

Telnet transmits instructions and data in clear text and is therefore not considered to be secure.

SMTP

Short for Simple Mail Transfer Protocol, SMTP is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. Because of this both the POP or IMAP server and the SMTP server must be specified when you configure your e-mail application.

SNMP2/3

Simple Network Management Protocol (SNMP) is an application layer protocol for distributed network management. It facilitates the exchange of management information between network devices. Its main function is to manage network performance, find and solve network problems, and plan for network growth. There are currently two versions of SNMP, and standardization of version three is pending.

ICMP

Short for Internet Control Message Protocol, ICMP is defined in RFC 792 as an extension to IP. It operates at layer 3 (network), reporting errors and other information regarding IP packet processing back to the source.

ICMP generates several kinds of messages useful for troubleshooting network problems. They are:

- Destination Unreachable
- Echo Request
- Echo Reply
- Redirect
- Time Exceeded

When a destination-unreachable message is sent out by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet. The four possible types of destination-unreachable messages are network unreachable, host unreachable, protocol unreachable, and port unreachable.

An echo-request message is generated by issuance of the ping command and is used for testing whether a host can be reached across the network. A successfully returned message typically indicates that the target host can be reached.

A redirect message is sent out by a router to the source host to request a more efficient route. The router will still forward the original packet to the destination, but requests that the sender chooses a better path.

A Time-exceeded message is issued by the router if an IP packet's Time-to-Live (TTL) field (which is usually expressed in hops or seconds) reaches zero. This field prevents packets from continuously circulating the network if the network contains a routing loop. In these cases, the original packet is discarded.

IGMP

Internet Group Management Protocol (IGMP) specifies how hosts can register a router in order to receive specific multicast traffic. IGMP is implemented on both the host and router sides. The host side reports group membership to the local router and the router side listens to these reports from the member hosts.

TLS

TLS (Transport Layer Security) is the successor of SSL. It is a cryptographic protocol that provides security and data integrity for communications over the relatively unsecured TCP/IP networks (the internet in particular). TLS is standardized in RFC 2246.

1.2 Identify commonly used TCP and UDP default ports

For the exam, it is a good idea to memorize the ports listed below. Unused well known ports should be blocked to minimize the attack surface. Port blocking is more effective when implemented at the edge of the network. In fact, even Windows Server has a TCP filter facility which allows you to manually block ports (TCP, UDP, or IP) at the interface level.

TCP ports
FTP – 20, 21
SSH – 22
TELNET – 23
SMTP – 25
DNS – 53
HTTP – 80
POP3 – 110
NTP – 123
IMAP4 – 143
HTTPS – 443

UDP ports
TFTP – 69
DNS – 53
BOOTPS/DHCP – 67
SNMP – 161

1.3 Identify the following address formats

IPv6/IPv4
In order to properly communicate on an Internetwork, computers must have unique identifiers for differentiating one computer from another. This is accomplished through IP addressing. Every IPv4 address is a 32-bit or 4 octet, address. An octet consists of 8 bits, with each bit representing a binary value of 128, 64, 32, 16, 8, 4, 2 or 1, with a minimum total numeric value of 0 or a maximum total value of 255. The address is written using dotted decimal format, with each octet separated by a decimal point. For example: 192.78.213.5.

An IP Network is identified by the number of bits in the network mask. The bits masked by this value represent the Network ID. The node address values are assigned using the remaining unmasked bits and are mapped to the physical addresses of the network hosts. The ARP protocol provides this translation from logical (IP) addresses to physical (MAC) addresses. The basic rule of thumb is that every network host has at least one unique IP address, while every router has a unique IP address for every network interface it possesses. All hosts on the same physical network must have the same network prefix (subnet mask) in order to communicate with each others.

In contrast, the IPv6 address space has 128 bits, which is broken down into eight groups of 16 bits. There are two major 64-bit parts: the network prefix that contains the registry, provider, subscriber ID, and subnet values and occupies the higher order groups of bits, and the interface ID that occupies the lower bits.

The three major types of IPv6 addresses are unicast, anycast, and multicast. You may use an IPv4-mapped IPv6 address to identify an IPv4-only node to an IPv6 node. *For purposes of the exam you are not required to know IPv6 implementation*.

MAC addressing

Every NIC is manufactured with a 'unique' identifier called a MAC address. Typically, the first half of the MAC address is the 'vendor ID' and the second half is the unique identifier. Because of this addressing technique, every MAC address on a network is unique. This is necessary to firmly identify each node and can be used to trace the source of a transmission. The MAC address is resolved to an IP address via arp.

1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes

Addressing Technologies

Static address assignment requires that you manually input the IP address for the host. This is usually desirable for servers since servers are always on and you do not want their addresses to keep changing.

For most network clients, DHCP is used for dynamic, or automatic, address assignment. This provides ease of management and saves the time it takes to manually assign each client on the network. Using a DHCP server provides an IP addressing database as well as automatically assigning IP addressing and possibly other information to the client for you.

In the absence of a statically or dynamically assigned IP address, hosts may use APIPA (Automatic Private IP Addressing); a feature of later Windows operating systems. With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server is not available. The IP address range is 169.254.0.1 through 169.254.255.254, with a default class B subnet mask of 255.255.0.0. A host will continue to use the self-configured IP address until a DHCP server becomes available or a static address is assigned.

Subnetting

IPv4 networks can be divided into smaller networks known as subnets. Subnetting refers to the process of dividing a larger network into several smaller subnets for the purposes of extra flexibility and scalability, more efficient use of network addresses, and broadcast traffic containment.

Subnet addresses are usually created by borrowing bits from the host field defined by a standard subnet mask, in which case a custom mask is used. The portion of the IP address that is masked is the subnet ID and the rest is the host ID. The number of borrowed bits will vary according to the subnet mask specified. Note the following:

- Subnet masks always use the same format and representation technique as the regular IP addresses.
- Subnet masks have a binary value of 1 in all bits specifying the network and/or subnetwork portion, and a binary value of 0 in all bits specifying the host portion.
- Subnet mask bits beyond the standard subnet mask values are always borrowed from the left-most bits of the host portion.

The table below shows the binary representation of the subnet masks.

Subnet mask and the binary representations	
Mask	**Binary**
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

The following tables summarize the key information for each address class. There are 5 columns. The first shows the number of bits borrowed from the host portion, the second shows the subnet mask, the third shows the effective number of subnets created, the fourth shows the number of hosts that can be accommodated per subnet, and the last one shows the number of subnet mask bits in CIDR notation.

Class A Host/Subnet Table				
1	255.128.0.0	2	8388606	/9
2	255.192.0.0	4	4194302	/10
3	255.224.0.0	8	2097150	/11
4	255.240.0.0	16	1048574	/12
5	255.248.0.0	32	524286	/13

6	255.252.0.0	64	262142	/14
7	255.254.0.0	128	131070	/15
8	255.255.0.0	256	65534	/16
9	255.255.128.0	512	32766	/17
10	255.255.192.0	1024	16382	/18
11	255.255.224.0	2048	8190	/19
12	255.255.240.0	4096	4094	/20
13	255.255.248.0	8192	2046	/21
14	255.255.252.0	16384	1022	/22
15	255.255.254.0	32768	510	/23
16	255.255.255.0	65536	254	/24
17	255.255.255.128	131072	126	/25
18	255.255.255.192	262144	62	/26
19	255.255.255.224	524288	30	/27
20	255.255.255.240	1048576	14	/28
21	255.255.255.248	2097152	6	/29
22	255.255.255.252	4194304	2	/30
23	255.255.255.254	8388608	2*	/31

Class B Host/Subnet Table

1	255.255.128.0	2	32766	/17
2	255.255.192.0	4	16382	/18
3	255.255.224.0	8	8190	/19
4	255.255.240.0	16	4094	/20
5	255.255.248.0	32	2046	/21
6	255.255.252.0	64	1022	/22
7	255.255.254.0	128	510	/23
8	255.255.255.0	256	254	/24
9	255.255.255.128	512	126	/25
10	255.255.255.192	1024	62	/26
11	255.255.255.224	2048	30	/27
12	255.255.255.240	4096	14	/28
13	255.255.255.248	8192	6	/29
14	255.255.255.252	16384	2	/30
15	255.255.255.254	32768	2*	/31

Class C Host/Subnet Table

1	255.255.255.128	2	126	/25
2	255.255.255.192	4	62	/26
3	255.255.255.224	8	30	/27
4	255.255.255.240	16	14	/28
5	255.255.255.248	32	6	/29
6	255.255.255.252	64	2	/30
7	255.255.255.254	128	2*	/31

Classful vs. classless (e.g. CIDR, Supernetting)

IPv4 addresses are grouped into different classes. INTERNIC is the organization which administers the IPv4 classes and addresses and assigns these to requesting firms in blocks based upon address class.

With the traditional way of subnetting as previously shown, the same subnet mask is applied for all the subnets, meaning each subnet has the same number of available host addresses. In many

cases, having the same subnet mask for all subnets can waste address space as each subnet typically cannot utilize all the available host addresses.

In order to use IP address space more efficiently, Variable Length Subnet Masks (VLSM) can be deployed. With VLSM, you can use a long mask on networks with few hosts and a short mask on subnets with many hosts. This technique is efficient in terms of address space usage, but is considerably more complex. Also keep in mind that in order to use VLSM, you must use a routing protocol that supports it.

With Classless Inter-Domain Routing (CIDR) addressing, each address has a network prefix for identifying either an aggregation of network gateways or an individual gateway. The length of such prefix is also specified as part of the address and can vary greatly depending on the number of bits that are actually needed. A destination address that has a shorter prefix is said to be less specific. A longer prefix, on the other hand, is said to describe a destination gateway more specifically. When performing routing functions, routers are required to use the more specific prefix in the routing table when forwarding packets.

A classless network address should look something like 192.22.25.0 /18, where "/18" designates that the first 18 bits of the address represent the network and the remaining 14 bits represent the specific host addresses.

NAT

Network Address Translation (NAT) allows a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. It helps to secure a network by masking the internal configuration of a private network and makes it difficult for outsider to monitor individual users.

With Dynamic NAT, a private IP address is mapped to a public IP address that draws from a pool of public IP addresses. This can be useful for a large network, whereas static NAT is recommended only for a small user base.

NAT is not without drawbacks and restrictions. The dynamic allocation of IP addresses, in the form of NAT requires state information that may not always be available. This is especially true for UDP traffic which offers almost no mechanism at the packet header level for determining if a packet is part of an ongoing communication session.

PAT

Port Address Translation (PAT) uses port remapping so that a single valid IP address may support source IP address translation for up to 64,000 clients. PAT does not work with applications that have an inbound data stream different from the outgoing control path. Another option would be to use Static translation, which allows you to substitute a fixed external IP address for an internal address, which is useful for servers that require fixed IP addresses.

SNAT
Source NAT refers to the process of network address translation done in a secure way. It involves the translation of the source IP address and/or the source port.

Public vs. private
Formally speaking, Private IP addresses belong to the address space allocated via RFC 1918. These addresses are available for any use by anyone and the same RFC 1918 IP addresses can be reused anywhere without introducing conflicts. However, because these addresses are not routable, they must stay "private" without connecting to the Internet. In fact, for hosts configured with private addresses to access the internet, the Network address translation (NAT) function would be the most desirable configuration.

The formally defined private network address spaces are:

Name	IP address range	Number of IPs
24-bit block	10.0.0.0 – 10.255.255.255	16,777,215
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576
16-bit block	192.168.0.0 – 192.168.255.255	65,535

NOTE: With private addressing hosts are assigned addresses capable of use only within your own network. They are not capable of communicating on the Internet. Technically you are free to set the IP addresses on the hosts as long as they are for your inside use only. If you expect your hosts to talk directly to the Internet you need to use addresses assigned by your ISP (Internet Service Provider).

DHCP (static, dynamic APIPA)
See previous section ***Addressing Technologies***.

Addressing schemes
Class A addresses range from 1.X.X.X to 126.X.X.X, where the first octet identifies the network (the prefix) and the last three octets identify the node. The default subnet mask is 255.0.0.0:

11111111.	00000000	00000000	00000000
Network	node	node	node

Class B Addresses range from 128.0.0.X to 191.255.X.X, where the first two octets identify the network and the last two identify the node. The default subnet mask is 255.255.0.0:

11111111.	11111111	00000000	00000000
Network	Network	node	node

Class C Addresses range from 192.0.0.X to 223.255.255.X, where the first three octets identify the network and the last octet identifies the node. The default subnet mask is 255.255.255.0:

11111111.	111111111	11111111	00000000
Network	Network	Network	node

Addresses that begin with 127 are loopback addresses that represent the local interface (e.g. 127.x.x.x). The contents of the last three bytes are not of any concern when using this for testing purposes. It allows you to verify that a network host can actually send something to itself, meaning the host's TCP/IP stack is still functioning (at least on itself).

Addresses from 224.0.0.0 to 239.255.255.255 are reserved for multicast packets. This address range is known as the Class D address range. The Class E address range (240.x.x.x and above) is also reserved for experimental purposes.

Unicast, Multicast, Broadcast

Unicast transmissions send all packets to a single destination. Broadcast refers to transmitting all packets to all destinations. Multicasting refers to the delivery of information to a group of targets simultaneously, using the most efficient way. IP Multicast is often employed for streaming media and Internet based TV applications.

1.5 Identify common IPv4 and IPv6 routing protocols

Link state

These protocols are either distance vector based or link state based. Distance vector uses the routing tables of all connected routers to determine how many hops it is to a specific destination. Link-state algorithms flood routing information to all nodes in the network. Each router, however, only sends out the portion of the routing table that describes the state of its own links. Through this update process, each router can build up a picture of the entire network in its routing tables.

OSPF

OSPF (Open Shortest Path First) uses a highly complicated link-state algorithm to build and calculate the shortest path to all known destinations, which allows much faster convergence in

large networks. OSPF enables the logical definition of networks where routers can be divided into areas. This limits the explosion of link state updates over the whole network and provides a mechanism for aggregating routes as well as reducing the unnecessary propagation of subnet information. There are a few drawbacks to OSPF; it is complicated to setup and is highly demanding in terms of router processing power.

IS-IS

IS-IS stands for Intermediate System-to-Intermediate System. It is a protocol based upon the routing method of DECnet Phase V routing, in which routers exchange data about routing via a single metric for determining the network topology. It was developed by ISO as part of their OSI model.

Distance vector

Distance vector algorithms call for each router to send all or some portion of its routing table only to its neighbors, not to all routers. Therefore, routers that use Distance vector algorithms can only know what their neighbors know.

RIP, RIPv2

RIP is a distance vector protocol and is fairly easy to set up, but is limited by hop counts. RIPv2 allows more information to be included in RIP packets and provides a simple authentication mechanism that is not supported by RIP. In fact, the primary difference between RIPv2 and v1 is that RIPv2 supports both plain text and MD5 authentication, with plain text authentication being the default.

BGP

Exterior routing protocols are used to exchange routing information between two hosts in a network of autonomous systems that are geographically separated. BGP is an example of an exterior routing protocol.

Hybrid

Hybrid routing involves the use of multiple different routing protocols and/or mechanisms together for better flexibility in the routing process.

EIGRP

EIGRP includes the components neighbor discovery of neighbor recovery, reliable transport protocol, DUAL finite state machine and protocol-dependent modules. Neighbor discovery of neighbor recovery refers to the process that routers use to dynamically learn of other routers on their directly attached networks. The reliable transport protocol is responsible for guaranteed and ordered delivery of EIGRP packets to all neighbors. The DUAL finite state machine embodies the decision process for all route computations. The protocol-dependent modules are responsible for most network layer protocol-specific tasks.

1.6 Explain the purpose and properties of routing

IGP vs. EGP

IGP (Interior Gateway Protocol) is a protocol primarily for exchanging routing information among gateways that reside within an autonomous network. EGP (Exterior Gateway Protocol), on the other hand, is a protocol designed for exchanging routing information between two neighbor gateways in a network of autonomous systems. It is mostly implemented between hosts on the Internet for mutually exchanging routing table information.

Static vs. dynamic, Next hop

With static routes you manually add routing entries. With dynamic routing, routing protocols are used for configuring the routing tables. Static routing is efficient and practical for small networks. Dynamic routing is necessary for large networks with many routes.

A routing entry tells the router where the next hop is, as well as which network interface to use. The "next hop" could be a host on the neighboring network, or another router that needs to forward the packet further down the link.

Understanding routing tables and how they pertain to path selection

A routing table has all the information necessary for forwarding a packet along the best path toward the destination. Each packet has information about its origin and destination. The table also provides instructions for forwarding a packet to the next hop on its route. Path selection works differently with different routing protocols.

Explain convergence (steady state)

Convergence, in the context of routing, refers to the act of all hosts, routes, problems and states of a network being shared with all routing and switching devices. Once all the information has been propagated throughout all the devices, the network is said to be converged. Routing protocols can adapt to changes on the network and detect a failure and then share the necessary update messages throughout the entire network. This process is subject to delay. The formal definition of a routing convergence period is the time period between change detection and the restoration of new path information at all routers.

1.7 Compare the characteristics of wireless communication standards

802.11 a/b/g/n

Speeds, Distance

Bandwidth is the term often used to state the measure of the information-carrying capacity of a medium, though the truly correct term is throughput. Precisely, the information-carrying capacity of a medium is normally referred to in units of MHz/km. In theory, when you have more bandwidth you have more speed. The amount of information that may be transmitted over a medium will change according to distance, even though the relationship is not necessarily linear. This applies to wired and wireless transmission.

Channels, Frequency

The available channels supported by the current wireless products in various countries are not entirely the same. Regulations in the US prohibit using channels greater than 11. For wireless products sold outside the US, the wireless region selection of the software interface would determine the channels that are available for use.

Frequency refers to the communication bandwidth and its cycle, or refresh rate, upon which the data is traveling. This is measured in hertz (Hz). One hertz is equal to one cycle per second. Kilohertz (KHz) is equal to one thousand cycles per second. Megahertz (MHz) is equal to one million cycles per second. Gigahertz (GHz) is equal to one billion cycles per second.

Authentication and encryption

WPA

WPA (Wi-Fi Protected Access) is a stronger form of wireless security. It is stronger because it uses Temporal Key Integrity Protocol to dynamically generate a new key for every packet and generate different sets of keys for each computer. WPA2 (Wi-Fi Protected Access 2) is even more robust as it is based on the final IEEE amendment to the original 802.11 standard and provides very strong encryption through AES (Advanced Encryption Standard).

WEP

WEP (Wireless Equivalent Privacy) is a wireless security protocol that helps protect your information by using a WEP key to encode all network traffic before transmitting it over the airwaves. This helps prevent unauthorized users from accessing the data as it is being transmitted.

WEP is part of IEEE 802.11 which uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. With RC4, the same traffic key is never used twice. Still, WEP is not considered to be strongly secure. This is why WPA was developed, which includes two improvements over WEP. First, there is improved data encryption through TKIP. Next, there is enhanced User authentication through EAP.

NOTE: You may also secure your access points by changing the SSID value from the default and disable SSID broadcasts altogether. You may also implement MAC address filtering which allows only clients with matching MAC addresses in a predefined list to connect.

RADIUS

RADIUS is an access server and a system of distributed security that secures remote access to networks and network services against unauthorized access. Its three components are the protocol, the server and the client.

TKIP

TKIP (Temporal Key Integrity Protocol) is an encryption protocol that has been included as part of the IEEE 802.11i standard for WLANs. It is intended to provide more secure encryption than WEP. It is the encryption method used by WPA.

Domain 2.0: Network Media Topologies

2.1 Categorize standard cable types and their properties
Type:

CAT3, CAT5, CAT5e, CAT6

Twisted pair 10BaseT and 100BaseT are the most common cable types used in networks today. CAT is short for Category. UTP is Unshielded Twisted Pair and STP is Shielded Twisted Pair. To achieve 100Mbps the cables must be at least CAT5. CAT3 supports up to 10Mbps only.

CAT5 cabling has three twists per inch of each twisted pair of 24 gauge copper wires in the cable. CAT5e cabling is made to more stringent standards and is primarily for 1000baseT networks or long distance 100baseTX links that exceed 100m in length (CAT5e can go up to 350m maximum).

CAT6 cabling can transmit voice and data at a rate of up to 155Mbps with a possible maximum transmission frequency of 550MHz. CAT6 cable is backward compatible with the older CAT5, CAT5e, and CAT3 standards.

STP, UTP

Unshielded Twisted Pair (UTP) cabling is made up of four pairs of insulated copper wires. UTP uses RJ45 connectors on each end of the cable for connecting to network devices. Shielded Twisted Pair (STP) includes an extra foil wrap shielding and more twists per inch to protect against interference and crosstalk and is more expensive.

Multimode fiber, single-mode fiber

Fiber Optic cables are the fastest, most expensive cabling option, and made up of an outer sheath, and inner cladding and glass or plastic fibers for the core. Optical fiber transmits data using pulses of light and can carry data at a rate as high as 622Mbbs. Because it uses light instead of electrical impulses, it is immune to crosstalk and EMI. Fiber cabling, however, is the most difficult to implement. It is very costly to install and manage and is therefore not as popular as UTP cabling.

Single-mode fiber has a specific wavelength, while Multi-mode can support many wavelengths.

Coaxial

Following the IEEE 802.3 Standard, coaxial cable is used for 10base2 (thinnet) and 10base5 (thicknet) networks in a physical bus topology. The bus is formed by a 50 Ohm backbone cable which connects all the computers in the LAN. Each segment is terminated at both ends by 50 Ohm resistors. Failure to properly terminate a

coax-based bus network leads to a problem called signal bounce that will flood and effectively shut down a network. Also see RG-59 and RG-6 below.

Serial

Serial ports are usually integrated into the motherboard, but can also be an expansion card. Serial ports are also often referred to as COM ports. Parallel ports are usually integrated into the motherboard, but can be in the form of an expansion card as well. These are often called LPT ports. They were also used for serial communications. Serial cables are usually thinner and have a smaller connector than parallel cables.

Plenum vs. Non-plenum

A plenum cable is a cable which is installed in the plenum spaces of a building. Plenum space is used for air circulation in heating and air conditioning systems and is typically between the structural ceiling and the suspended ceiling, or, under a raised floor. Typical plenum cable is coated with fire-retardant coating (usually made of Teflon) so that in case of a fire it doesn't release toxic gasses and smoke (non-plenum cables may release toxic gas when burnt). .

Properties:

Transmission speeds, Distance

Transmission speed is a performance issue. Distance is more of a scalability issue. Both set limits for different network communication mediums and mechanisms.

Duplex

Full-duplex means the transmission of data in two directions simultaneously. Half-duplex means only one party can transmit at a time. Think of full-duplex like a telephone where both people can talk and half-duplex like a CB radio where only one person at a time can talk.

Noise immunity (security, EMI)

In the context of network communications, noise is the interference (static) that can destroy the integrity of signals on a line. Crosstalk refers to the bleeding of signals carried by one pair of conductors onto another.

EMI is short for electromagnetic interference. It means the electromagnetic field of one device disrupts, impedes or degrades the electromagnetic field of another device by coming into proximity with it. All computer devices are susceptible to EMI as electromagnetic fields are an unavoidable byproduct of passing electricity through a wire. Data lines without sufficient shielding can be highly susceptible to data corruption by EMI.

Frequency

The frequency at which a communication device works makes a difference in the overall design. In the context of wireless communication, a frequency range, or band, refers to a range of wave frequencies in electromagnetic radiation. Many radio and wireless devices operate within a specified frequency range, which limits the frequencies on which transmission is allowed.

2.2 Identify common connector types

RJ-11

An RJ-11 (Registered Jack 11) connector is primarily used in the United States and its surrounding territories. It is not commonly used for data networks, although it can be used in terms of a modem for data transmissions. RJ-11 connectors are most commonly seen and used on PSTN (Public Switched Telephone Network) which is nothing more than the international telephone system based on copper wires carrying analog voice signals to the homes of people worldwide depending on where it's deployed.

RJ-45

RJ-45 is short for Registered Jack 45. This is a cable connector that accommodates eight wire pins. These are the most commonly seen termination type in today's networks. RJ-45's are found on twisted pair cabling and thus in any network that uses this cabling type. They are often confused with RJ-11's, but a side by side comparison makes it easy to distinguish the difference as RJ-45s are wider than RJ11s. The graphic below depicts a typical RJ45.

BNC

A BNC connector is a very popular type of RF connector used for the purpose of terminating coaxial cable. BNC connectors are commonly found on video devices and on older NICs supporting a physical bus topology. In terms of network use it is considered legacy equipment and obsolete.

SC, ST, LC

An ST connector is most commonly found on fiber optic cable. ST stands for 'straight tip' and was formerly the most common fiber cabling connector type. . An ST connector employed a 'screw on' type of locking mechanism that required it to be seated in the receptor with a 'Stick and Twist' motion. 10BaseFL is an older 10 Mbps fiber cabling type that was primarily where you would see ST connectors in use.

The most common fiber connector type in use now is the SC connector. SC stands for 'standard connector'. An SC connector employs a 'click in' type of locking mechanism that requires it to be seated in the receptor with a 'Stick and Click' motion.

A newer type is the LC connector. This is starting to replace the SC connector type in today's implementations. LC stands for "little connector" or "Lucent connector". It basically resembles a small SC connector and is currently mostly seen in high density fiber cabling. It has been standardized as one of the Fiber Optic Connector Intermateability Standards in EIA/TIA-604-10.

RS-232

RS-232 is a telecommunications standard intended for binary serial communications between hardware devices that are commonly referred to as a DTE (data terminal equipment) and DCE (data communications equipment). The most updated designations for the RS-232 protocol have included EIA-232 as well as EIA/TIA-232. In PC applications this is the formerly ubiquitous DB-9 serial port connector. It is a 9-pin D-shell connector with 2 rows of pins; 5 on top and 4 on bottom.

RG-59, RG-6

RG-6 and RG-59 are 2 common types of coaxial cable connectors used in a wide variety of residential and commercial applications. The most common place it is seen is in cable TV connection wires. The connectors are very similar in appearance. Typically and RG-6 connector has a shorter threaded barrel than the RG-59. The connector type is determined by the cabling type used, which have the same code (RG-6 or 59) as the connectors. RG stands for Radio Guide.

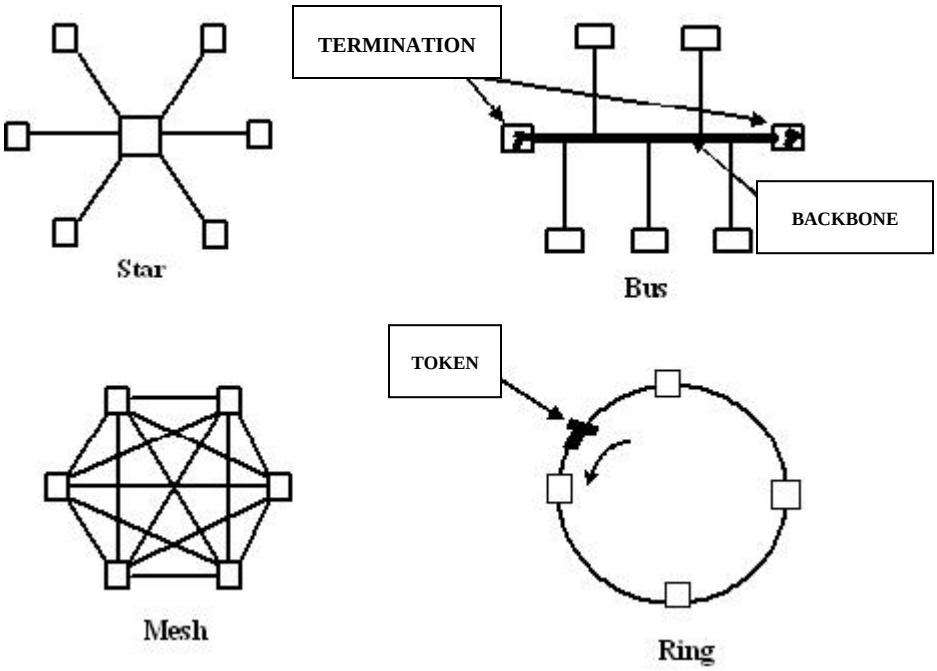
2.3 Identify common physical network topologies

Star, Mesh, Bus, Ring

A physical network topology refers to the geometric arrangement of nodes and cable links in a LAN. The most popular Ethernet configurations are bus and star. A physical bus topology consists of nodes connected to a backbone cable. Nodes tap into the backbone via vampire tap connectors. The nodes use coax thinnet cables to connect to the backbone thicknet cable. The main issue with a bus network is that a cable break anywhere along the bus will cause the entire segment to suffer. An improperly terminated endpoint will cause the entire bus to fail.10base2 and 10base5 networks use the bus topology.

The most popular physical topology today is the star topology, in which access is controlled by a central device; either a hub or a switch. The major advantages of a physical star network are that cable breaks only affect the directly connected node(s) and it is to expand the network as a new node only requires a twisted pair patch cable to connect to the network.

With a ring topology, nodes are connected from one to another as in a ring. A data token is used to grant permission for each node to send message out. Due to the high cost involved in setting up and maintaining ring networks, they are rarely seen in operation today.



A physical mesh topology involves the use of multiple connection paths between nodes A router is typically used to do best path determination for the transmission. Mesh topologies are mostly seen in core network areas, especially in WAN implementations where redundancy is mission critical. Though a mesh topology allows redundancy, it can be very difficult to configure and maintain, especially as the number of connected nodes grows. Mesh networks can also be very costly to implement.

Point to point, Point to multipoint, Hybrid

Broadly speaking, the two basic types of network transmission technologies are Broadcast and point-to-point. Typically, a point-to-point connection is used to connect one specific area to another via wired or wireless means. All communications in this configuration are isolated to the two endpoints.

Point to multipoint is different in that it allows connections to be made with multiple points at the same time. Simply put, a point to multipoint topology allows you multiple locations to be connected for the purpose of sharing network resources.

Hybrid networks deploy connection methods of different types for better compatibility and flexibility. There are many types of communication models that can be combined in this configuration.

2.4 Given a scenario, differentiate and implement appropriate wiring standards

568A, 568B

568A and 568B are the color code schemes used for correctly wiring the RJ45 connectors in twisted pair cabling. These schemes have been approved by ANSI/TIA/EIA wiring standards. Note that there is no difference between these two wiring schemes in terms of connectivity or performance when connecting network devices, so long as the connected devices are wired for use under the same scheme on both ends of the cable.

Straight vs. cross-over

A crossover cable is used to interconnect two “like” devices directly without use of any type of intermediary device. Basically this means connecting ports on two hubs or switched (unless specified as an uplink port), two computer’s NICs or even two routers. If the ports are expecting the same cabling scheme, then a crossover it the correct cable type to use. It works by "crossing over" (i.e. reversing) thee respective PIN contacts, typically pins 1, 2, 3 and 6..

Rollover

A rollover cable is also known as a console cable. These are typically used for connecting a computer terminal to a router or managed switch’s console port. It is typically flat and with a light blue color for easily distinguishing it from the other types of network cabling. It is wired by completely flipping, reversing or rolling over the wiring order on the opposite end of the cable.

Loopback

Loopback cables are used for network testing and basically redirect the output back to the source to test a complete end to end connection for a specific device. They are wired the same way as a crossover cable, but usually only have the 4 wires involved in the crossover switch (1,2,3,6) crimped into the RJ45 connector.

2.5 Categorize WAN technology types and properties

Types:

Frame relay

Frame Relay is a packet-switching protocol for connecting devices on a WAN that can support data transfer rates at 1.544 Mbps and/or 45 Mbps. It uses variable size frames to encapsulate data and transport it.

E1/T1

The T-carrier is a generic designator for digitally multiplexed telecommunications carrier systems, originally developed by the Bell Labs and are deployed in North America, Japan, and Korea. A T1 line contains 24 64Kbps channels for a total throughput of 1.544Mbps. A T1 is also referred to as a DS1, with each channel called a DS0. The E-carrier system ('E' stands for

European) is not compatible with the T-carrier, although they are similar in usage. The E1 circuit contains 32 channels total, with 2 used for line management. Its total throughput is 2.048Mbps.

Though E carriers and T carriers are not directly compatible, they can be linked using translational intermediaries. The E carrier also has multiple level lines such as the T carrier's T3.

ADSL, SDSL, VDSL

xDSL refers to all types of Digital Subscriber Lines, including ADSL (Asymmetric Digital Subscriber Line), SDSL (Symmetric Digital Subscriber Line), and VDSL (Very high bit rate Digital Subscriber Line). The basics of these are as follows:

- ADSL basically means the upload and download rates are not the same. It supports downstream rates of 1.5 to 9Mbps and upstream ranges from 16 to 640kbps. The implementation must be located within a distance of 18,000ft from the central office DSL switching equipment. It is typically delivered over copper twisted pair. This is the most common home consumer DSL implementation.
- SDSL means that the upload and download speeds of the connection are the same rate. It can deliver various levels of speed, with a max of 1.544Mbps upload and download. It uses a single copper twisted pair to deliver the service. The implementation must be within a distance of 10,000ft from the central office DSL switching equipment. This type is usually seen in commercial and small business implementations.

VDSL is an attempt to use DSL technology to deliver very high speed data lines, mostly for use in commercial applications.. It can provide data transmission up to 52 Mbps downstream and 12 Mbps upstream. The distance limitations vary with VDSL, but typically fall between 1000ft for the fastest speeds to 4500ft for a reduced rate, both from the central office switching equipment. VDSL can provide many services at once and is often seen in bundled service implementations. More recently it is starting to be seen in home rollouts in the form of VoIP phone service and HDTV.

Cable modem

Cable modems use the existing cable TV lines to provide high speed internet access for both home and commercial customers. More recently they are also used to provide bundled services such as VoIP phone. The cable modem provides access to what is essentially a big Ethernet network connected to the cable TV network.

NOTE: Hybrid Fiber-Coaxial (HFC) is for two-way access using fiber optics together with coaxial cable. The network extends from a central location to each end user. These are then connected to hub site in which the fiber optic node provides services for up to 2000 nodes.

Satellite
Internet gateways can be accessed via geostationary satellites also known as GEOs. These systems are not optimized for TCP/IP and Internet use and can be quite expensive. The time delay in data transport can be problematic for Voice over Satellite as well.

Practically speaking, this kind of connection would work only if you have a clear sky environment. In a place with a lot of tall buildings or inclement weather , satellite is typically not a reliable choice.

E3/T3
A T3 line basically combines 28 T1s into a single line. It contains 672 channels operating at 64Kbps for an aggregate throughput of 43.008Mbps. These are typically WAN backbone implementations. They are also referred to as DS3 lines. The E3 is the European version of this and contains 512 channels for a total throughput of 34.368Mbps.

OC-x
OC stands for Optical Circuit and is a set of standards defining transfer rates over high throughput fiber optic lines. OC-x lines are used primarily in SONET and ATM implementations. The most common designations and rates are OC-1 at 51.84Mbps, OC-3 at 155.53Mbps, OC-48 at 2.488Gbps and OC-192 at 10Gbps. There are other OC-x levels and the speed of the line can be determined by multiplying the number after OC by 51.84Mbps.

Wireless
Wireless LAN is a type of local-area network that uses high-frequency radio waves to communicate between nodes. There is no need for cabling between client nodes. Instead, Access Points are used to act as the communication hubs for the wireless clients to connect to a wired LAN.

ATM
ATM stands for asynchronous transfer mode. It is a dedicated-connection switching technology that operates at Layer 2. It organizes digital data into fixed 53-byte cell units for transmission. It is often seen in the same types of implementations as Frame Relay.

SONET
SONET stands for synchronous optical networking and is a ring based technology that provides extremely high throughput rates. SONET employs OC-x lines usually and is often used as s large scale backbone. SONET is a multiplexing protocol and uses multiple signal streams via lasers or light-emitting diodes over fiber optic media.

NOTE: Since SONET uses time division multiplexing (TDM) for offering permanent connections, packet mode communication is never involved and is therefore considered to be a physical layer technology.

MPLS
MPLS stands for Multi-Protocol Label Switching. It is a protocol independent way of creating end to end connections across multiple platform types. In an MPLS network, a label is attached to each data packet and routing decisions are based upon the label, not the packet. This helps to eliminate dependence upon a single Layer 2 transport technology.

ISDN BRI, ISDN PRI
ISDN stands for integrated services digital network and defines an international communications standard for sending voice, video, and data over digital or normal telephone lines and is commonly seen in business implementations. The primary benefit of ISDN is that it allows a remote location to connect on a dial-in basis to a central network and be treated as an extension of that network, with all service types provided. Also, it is delivered on a 'call initiated' and 'call terminated' basis so you only pay for what you use. Once the call is deemed over due to inactively, the call is ended and so is the billing for that usage.

ISDN supports data transfer rates of 64 Kbps per data channel. These are called B channels. ISDN also uses a management, or D channel to build and tear down the call. These concepts are the basis for most digital connection technologies, such as a T carrier. There are two ISDN service levels: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI uses two B and one D channels for a maximum rate of 128Kbps. PRI uses 23 B channels one D channel fro a rate of 1.544Mbps. This is basically a T1 that can be used on an on-demand basis. The European version of PRI uses 30 B channels and one D channel for a throughput of 2.048Mbps.

POTS
POTS stands for plain old telephone service and refers to the original voice telephone service. This utilizes the PSTN (public switched telephone network) and provides a dedicated 64Kbps circuit for end-to-end calling during the call duration. The network implementation of this would be use of a dial-up modem for Internet access.

PSTN
Public switched telephone network (PSTN) refers to the network of public circuit switched phone networks in the world. Originally this network was analog based, but is now mostly digital with the implementation of fiber optic lines. It also includes cellular based voice technology. The PSTN is the core network that provides voice services.

Properties:

Circuit switch, Packet switch
Circuit switching refers to connections that require verified circuits to be opened from end to end before transmission can take place. Packet switching emulates circuit switching in that it requires a path to be made available, but the data can be broken into many smaller pieces and take different routes, each opening a circuit for its individual delivery. A good example of a circuit switching scenario is a telephone call that requires a verified, dedicated line for the duration of transmission. An example of packet switching is sending or receiving data via the Internet.

Speed, Transmission media, Distance

Speed refers to the rated throughput of a connection, such as the T1 speed 1.544Mbps. Transmission media refers to the type of physical medium used, such as fiber optic lines in SONET. Distance refers to the linear length that a technology can deliver its signals, such as the 18000ft limitation of ADSL.

2.6 Categorize LAN technology types and properties

Types:

Ethernet

Ethernet is a LAN architecture originally developed by DEC, Intel and Xerox in 1976. This original standard was called DIX Ethernet. The finalized and modern implementation of Ethernet is defined by the IEEE 802.3 standard. Ethernet is by far the most ubiquitous LAN technology in use today.

Some key features of Ethernet include:

- Uses contention based communication standard CSMA/CD
- Ethernet networks are prone to data collisions which absorb network throughput
- Ethernet uses frames to encapsulate data and contain the destination address, source address, type field, data payload and checksum field for error checking
- An Ethernet or MAC address is 6 bytes, with each being unique and preset in the factory.
- Every network device listens for Ethernet frames with a wild card destination address of "FF-FF-FF-FF-FF-FF", which is a broadcast address
- All equipment and devices on the network must be Ethernet compatible

The following table lists several of the Ethernet LAN standards and their specifications. Any of these could be potentially covered on the Network+ exam.

Name	Cable Type	Max Distance	Throughput Rate
10baseT	Copper twisted pair	100m (330ft)	10Mbps
100baseTX	Copper twisted pair	100m (330ft)	100Mbps
100baseFX	Fiber optic	2km (1.25mi)	100Mbps
1000baseT/TX	Copper twisted pair	100m (330ft)	1000Mbps or 1Gbps
10GbaseT	Copper twisted pair	100m (330ft)	10Gbps
1000baseSX	Fiber optic`	550m (1800ft)	1000Mbps or 1Gbps
1000baseLX	Fiber optic	100km (62.5mi)	1000Mbps or 1Gbps
10GbaseSR	Fiber optic	300m (990ft)	10Gbps
10GbaseLR	Fiber optic	10km (6.25mi)	10Gbps
10GbaseER	Fiber optic	40km (25mi)	10Gbps

10GbaseSW, 10GbaseLW and 10GbaseEW are the WAN versions of the corresponding 10GbaseSR, 10GbaseLR and 10GbaseER LAN technologies. These standards allow their companion LAN fiber Ethernet implementations to be more seamlessly connected to an OC-x

based WAN connection. Even though considered WAN technology in purpose, these standards are still technically a type of Ethernet LAN.

All 10 Gigabit Ethernet implementations are full-duplex and fiber-only, thus eliminating the need for using CSMA/CD. Besides this difference, 10 Gigabit Ethernet is highly similar to the original Ethernet model.

Properties

CSMA/CD

Ethernet uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) as the network access method. This is also known as contention based transmission because all nodes contend for access. To understand CSMA?CD, you must break it down into three separate statements. Carrier Sense means that all connected nodes are listening, or sensing, the wire and waiting for an opening to transmit. Multiple Access means that all nodes have equal access and are not required to have a special piece of code to do so, as in the case of Token Ring. Collision Detection means that all nodes have the ability to sense when a data collision has occurred. This characteristic of Ethernet creates what is called overhead and absorbs some of the possible aggregate throughput of the network. This is why it is a good strategy to segment collision areas, or domains; to make an Ethernet network more efficient. A switch or router provides this function, whereas hubs do not.

Broadcast

A broadcast is when a transmission is sent to all nodes that are connected. This can be done to discover other nodes or services or to advertise them. Since broadcasts basically flood packets onto every corner of the connected network, it is a good strategy to segment broadcast sections, or domains; to make an Ethernet network more efficient. Bridges, switches and routers can provide this functionality.

Collision

A collision is when more than one node attempt to transmit simultaneously. The result is multiple overlaying signals that come out as scrambled and unreadable. When this happens all Ethernet nodes generate a random number via the backoff algorithm that determines how long it will wait until it tries again to transmit or retransmit.

Bonding

Ethernet channel bonding is a tactic of binding multiple Ethernet channels together to get better throughput from a server computer. It is now a very popular technique in the Linux community.

Speed, Distance

Ethernet speeds vary from 10Mbps to 10Gbps in today’s networks. The most common speeds are 10, 100 and 1000Mbps. When a group of interconnected nodes are operating at different speeds, the actual speed is determined by the slowest node due to the fact that Ethernet is a logical bus topology and all nodes see all traffic. Distance limitations are very important to consider, especially when designed a new network layout and the underlying cabling plant. The general

rule of thumb with Ethernet is 100m (330ft) total, end to end, with out any type of repeating device. This is due primarily to the fact that Ethernet is mostly twisted pair cabling based or in higher speed fiber that the cabling is restricted to shorter distances to maintain the higher speeds.

2.7 Explain common logical network topologies and their characteristics

Peer to peer, Client/server

Peer to peer networks are also known as Workgroups. Older physical bus Ethernet networks were almost exclusively peer to peer. Logically, peer to peer provides basic printer and file sharing and limited basic password security. In this scenario, all modes are both a client at times and a server at times. Each node hosts its resources and shares them with the other connected nodes. Peer to peer is not considered to be secure by today's standards.

Client/server is the most common model used in businesses. In this scenario, a client connects to a server for both authentication to the network and for use of resources. This requires some type of client software to log into the server, which then applies various security models or policies to the client, thus defining the functions the client can perform on the network. Nodes can still share files with each other as in the peer to peer model, but are much more limited in their server functions. The client/server model is considered to be much more secure and allows many levels of access permission granularity, as well as the ability to more easily isolate security breaches if and when they occur.

VPN

VPN stands for virtual private network. A VPN uses public lines to create a private, encrypted tunnel between two sites. The two common types of VPNs are:

- Remote Access – Also called a Virtual Private Dial-up Network (VPDN), these are typically used for an individual user to connect to their LAN remotely.
- Site-to-Site - This type is typically used to connect multiple fixed sites through the use of dedicated equipment to each other. A good example is a branch office connected to the main headquarters of a company.

The major encryption and tunneling protocols supported by Windows based VPNs are MPPE + PPTP and IPSec + L2TP. MPPE and IPSec are the encryption protocols and PPTP and L2TP are the tunneling protocols. Pre-Windows 2000 computers support PPTP. Windows 2000, XP, 2003 and 2008 computers use L2TP. L2TP uses UDP port 1701 and PPTP uses TCP port 1723. L2TP is considered to be more secure than PPTP.

VLAN

A Virtual LAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. Also, they are used to further segment a larger LAN section. VLANs are based on logical connections, and are extremely flexible in terms of configuration and application. However, they require network layer services to route between VLANs.

2.8 Install components of wiring distribution

Vertical and horizontal cross connects, Patch panels, 66 block, 110 block

Vertical cross-connects (VCC) and Horizontal cross-connects (HCC) are used to interconnect a patch panel to the backbone cabling. A patch panel is a concentrated group of connector ports that is wired directly to the core network cabling. They are usually found in the wiring closet and allow multiple nodes to use a patch cable to connect to the network. A 66 block is a device for connecting wires in a phone system and usually hosts a 25 pair telephone connection from the voice provider. A 110 block is a similar and newer device for serving the same purpose, but can also be used with Cat5 cabling. With both of these, the wires are connected using a punch down tool that forces the wires into metal clips that terminate the connection.

MDFs, IDFs

IDF stands for intermediate distribution frame. It is a cable rack that can be used to interconnect and manage your telecommunications wiring between an MDF and other workstation devices. MDF stands for main distribution frame. These interconnect telecommunications wiring between themselves and the IDFs.

25 pair, 100 pair

25-pair defines both a wire type and color coding for that wire and is the most commonly provided wiring by most telephony providers. It has 50 individual wires within it. A 100-pair cable is the same thing as a 25 pair, but has 200 individual wires within it. Both are primarily used in telecommunication applications.

Demarc, Demarc extension, Smart jack

A demarcation point is the point at which the local phone company network ends and connects with the wiring at your own premises. These are implemented by professionals typically due to the specialized knowledge necessary to properly terminate the circuit. All cabling and connections past the point of the demarc are the responsibility of the customer.

A demarc extension is wiring connected to the demarc and run into the customer premises to allow the internal LAN to connect to the telecommunications service provided. A smart jack is the device that connects directly to the demarcation point via the demarc extension and provides a connection port for the internal network devices, such as a router. Smart jacks are also known as a network interface unit (NIU) or network interface device (NID).

Verify wiring installation, Verify wiring termination

This is a wire crimper, which are used to properly terminate cabling wires:

This is a tone generator:

These are sometimes also called time-domain reflectometers (TDR) or a fox and hound. They are used to verify proper installation and termination of cabling and wiring. This is done by introducing a tone, or current, to the wire pairs to verify the circuit is complete from end to end. They can also be used to determine the point of a cable breakage or sever interference.

Volt-ohm meters and digital multimeters can also be used to measure physical layer parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity.

Domain 3.0: Network Devices

Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5
- Objective 6

3.1 Install, configure and differentiate between common network devices

Hub

A hub is a concentrating device that allows multiple nodes to connect to a simulated bus network via twisted pair patch cabling. The hub replaced the thicknet backbone and thinnet client connections by simulating the bus backbone and vampire tapped client connections with its internal wiring and external RJ45 ports. This gave birth to the physical star networks seen in most Ethernet implementations today.
A hub is basically a multiport repeater. They are also the predecessor of the switch. There are two basic types of hub: active and passive. An active hub has its own power supply and thus regenerates signals that pass through it, effectively extending the reach of a network. A passive hub is simply a connecting device and does not regenerate signals that pass through it. In either case, a hub works by flooding the signals it receives to all ports which have a node connected. It knows this because the ports is terminated when a node is connected. Since a hub floods all packets to all active ports, it does not restrict the boundaries of either collision or broadcast. Due to the overheard generated by this and the fact that the internal wiring of the hub is actually a physical bus, hubs both lose throughput and split it evenly to all connected ports. For example, if a hub is a 100Mbps hub and has 4 connected nodes, each node is effectively accessing a 25Mbps connection. Hubs operate at the physical layer.

Repeater

A repeater is a network extending device. It helps allow the linear length of a transmission path to circumvent the distance limitations by re-strengthening signals that pass through it. Repeaters are not as common as they used to be, and were mostly replaced by hubs in LAN implementations. They are still seen in large payload core network applications and in older LANs that have not been converted to newer standards. Repeaters operate at the physical layer.

Modem

The term modem is an amalgamation of the two terms modulator-demodulator and are devices that allow a computer to transmit data over telephone lines. Basically a modem acts as an analog to digital signal converter. Modems at one time were the most common form of Internet access, but have been supplanted by the availability of home broadband such as DSL and cable modem. Modems operate at several layers of the OSI with their highest function being at the session layer.

NIC

A Network Interface Card, often called a NIC for short, is one of the most commonly used and preferable methods of attaching devices to a network. A NIC is nothing more than an expansion board for your PC that provides an interface to the

local network. They are also often referred to as a network adapter. A lot of PCs now come with on-board NICs, though it still quite common to see them as an expansion board that requires installation. There are a few things to consider when procuring a NIC. First the speed should match the advertised speed of the network to which you are connecting. Some NICs come as variable speed and will be noted as such (e.g. 10/100/1000 Mbps). Also, you must get a NIC compatible with the type of network, such as Ethernet or Token Ring. Another feature of modern NICs that many administrators find appealing is PreBoot Execution (PXE) compliant support. This allows a NIC to wake a computer from sleep mode or to even power a computer on to allows for remote installations, patching and imaging. All NICs come with a hardware or MAC address (sometimes also called an Ethernet address) hard wired or "burned" into them. This is a 48bit (6byte) hexadecimal address that uses the XX-XX-XX-XX-XX-XX format. The first 3 pairs (24bits or 3bytes) of numbers represent the manufacturers address and are typically the same in a group of NICs. This address is assigned to the manufacturer by governing bodies. The last 3 pairs are unique to each device. The combination of assigned vendor numbers and unique device numbers provides each NIC with a completely unique hardware address. This allows transmissions to be traced back to a specific device for communication or even security purposes. NICs operate at more than one OSI layer, with their highest functions being at the network layer.

Media converters

Media converters are devices that convert LAN signals to different media formats. For example, signals from a coaxial cable can be converted to fiber optic signaling or twisted pair cabling can be converted to coaxial signaling. These are especially useful for expanding networks that do not want to completely replace their infrastructure at once.

Basic switch

Switches are data link layer devices that enable multiple physical LAN segments to be interconnected. They have supplanted hubs as the concentrating device of choice in most LANs. Switches regenerate signals like active hubs and provide the segmenting and translational abilities of a bridge. Because they have the ability to separate collision and broadcast areas or domains, they can be used to divide a network into more manageable sections. They use a table of MAC addresses to determine where a node is located. Switches also have fully dedicated circuit paths to each node connection port. This means that if the network is 100Mbps, each switch port provides a 100Mbps connection. Replacing hubs with switches is a way to instantly speed up a network. Basic switches operate at the data link layer, but newer switches have network layer and above functions.

Bridge

A Bridge is a device that connects two LANs or two segments of a LAN in order to segment it and/or provide translation services between different network types. Bridges have this capability because they operate using hardware addresses, which are used in all network types. Bridges use a table of MAC addresses to know where to forward a packet. Since they segment nodes based upon their connection to the bridge, this separates the collision domain. Bridges, however, do not separate broadcast domains like a switch. Bridges operate at the data link layer.

Wireless access point
A wireless access point (WAP or AP) is basically the switch of the wireless LAN. They operate by reading the MAC address of a wireless NIC. They provide a point for wireless clients to connect to the wired LAN. A basic WAP operates at the data link layer.

Basic router
A router is a device that forwards data packets to the appropriate network path. It does this using several types of information, the most of which is the IP address of the intended node. They can also weigh network traffic, line speed and many other factors into routing decisions. Routers can also act as a gateway to another network, with this function most commonly seen as the connection to Internet access. Routers can also perform bridging and switching type functions, but do not forward either collision or broadcast traffic. One exception to this rule is the forwarding of BootP traffic, which is associated with PXE installations and DHCP traffic. Routers keep a table of logical addresses to determine where a node is located. Routers are generally considered to be network layer devices, but some newer models now have transport layer functionality.

Basic firewall
A firewall prevents unauthorized access to or from a private network by examining each message and blocking those that do not meet the specified security criteria. It may be implemented in hardware or software, or a combination of both. Routers are often used as firewalls as most have the ability to build an access list of acceptable traffic types and nodes.

Basic DHCP server
A DHCP server provides automatic addressing information to clients via the dynamic host configuration protocol. In order for this to work, the node must be configured to be a DHCP client. Configuration settings provided by a DHCP server can include IP address, subnet mask, gateway address and DNS or WINS server addresses. The assignment of DHCP information to clients is done through a type of handshaking process called D-O-R-A. The client sends out a DISCOVERY message looking for a server. The server sees the request and responds with an OFFER of configuration information. The client then sends a REQUEST to take the offered information back to the server. Finally, the server then sends an ACKNOWLEDGEMENT that the client can use the information. DHCP greatly reduces the amount of administrative effort in network addressing.

3.2 Identify the functions of specialized network devices

Multilayer switch
As previously stated, switches have the ability to operate at multiple layers of the OSI. These types of switches are called multilayer switches and combine layer 2, 3 and 4 capabilities. Layer 3 switching is the ability to make routing type decisions based upon IP addressing information. This capability also allows for VLANs to be implemented without a router. Layer 4 switching involves using the TCP or UDP port numbers found in the TCP/IP packet header to make routing

and traffic flow decisions. Though layers 3 and 4 have traditionally been the territory of routers, switching is becoming more prevalent at these layers because by nature it is much faster than routing. Multilayer switches use much more detailed tables than the traditional switches to make predefined decisions for forwarding data. Services that are more concerned about speed of delivery over error checking and flow control benefit the most from layer 3 and 4 switching.

Content switch

Content switches are sometimes referred to as layer 4-7 switches, content services switches, web switches or application switches. These are specialized devices that can make switching decisions based on application level criteria. They are often used for load balancing for servers by performing basic security and other prequalification actions. They can be used to perform NAT functions and SSL certificate services. They also have the ability to associate a source address with a specific resource host and reuse the association. Most of these functions can be performed at switch speeds, which can dramatically speed up services.

IDS/IPS

Intrusion detection system (IDS) / Intrusion Prevention System (IPS) is a software or hardware based device that can detect many types of attacks on a network. It can be broadly classified into the following:

- In a network-based IDS system, individual packets that flow through a network are analyzed.
- In a host-based IDS system, activities on each individual computer are individually inspected.
- In a passive IDS system, the IDS detects potential security breaches and raise alerts proactively.
- In a reactive IDS system, the IDS reactively responds to any suspicious activity through logging off the involved user and blocking network traffic from the suspected source.

One weakness of an IDS/IPS is that it does not generally have the ability to detect an attack disguised in encrypted traffic.

Load balancer

Load balancing is the use of hardware, software or both to evenly distribute traffic, service requests and workloads in a network. Primarily it is used to help distribute workloads across servers and to keep traffic flow balanced. Load balancers are often used to spread out HTTP, HTTPS and/or VPN traffic. In fact, it can be used for most applications that are based upon TCP/IP traffic. Load balancing often involves the use of NAT in order to disguise which server is actually processing the requests.

Multifunction network devices

Multifunction devices, in general, are devices capable of performing multiple functions. In terms of networking this could be switching, caching, routing and filtering. It could be voice and data traffic delivery. Usually these types of devices are deployed to save time, money and administrative effort. Sometimes, but not always, they may not do as complete of a job addressing some of the functions with which they are tasked versus a stand alone, dedicated

device. This trade off should be weighed and considered before implementation of a multifunction or singular function device.

DNS server

DNS stands for Domain Name System. DNS creates mappings between host names and IP addresses. This give the user the ability to find a node by name rather than memorize its IP address. A good example of this is simply typing a Web address into a browser and pressing enter. Because of DNS, the Web site's name will be resolved to the registered IP address of that resource. To verify DNS operability, there are several tools available. The most useful is NSLOOKUP. This is a command line utility and requires that the PC issuing the command has TCP/IP installed. Below is sample output from NSLOOKUP:

```
C:\>nslookup www.examreview.net
Server:
Address:  192.168.2.1

Name:    www.examreview.net
Address:  75.126.94.74
```

DNS server information can be manually entered in a network adapter's TCP/IP settings or can be delivered to hosts dynamically via DHCP. DNS can be thought of a distributed database of host information, with the keepers of the information being the name servers. A top level name server is referred to as a root server. DNS resolvers are name servers that start the resolution process on the client side. Authoritative servers are name servers that answer the forwarded requests from resolvers, though due to caching a resolver may be able to answer the query itself. There are two basic types of query: recursive and non-recursive. A recursive query is one that is answered in full by a name server, usually for a new resource not queried before. A non-recursive query is one that is partially answered by the name server, or when an error is returned.

Bandwidth shaper

Bandwidth or traffic shaping is the technique of limiting throughput consumption based on predefined criteria. Shaping does not drop packets as policing techniques do, but rather uses strategies to control the amount of traffic that passes through the network. This can be done by throttling, which defines amount limits during specific time periods, by rate limiting, which defines the speed at which traffic can be sent, or by complicated algorithms that use several factors to determine the best combination of techniques to control traffic volume.

Proxy server

A proxy server intercepts all messages entering and leaving the network. It is primarily used as an intermediary for Internet traffic. The primary benefit of a proxy server is in security as it makes outgoing requests on behalf of internal clients so they are never exposed to external risks

directly. When proxy services are in use, the client's Web browser must be configured with the proxy server's address.

CSU/DSU

A CSU/DSU is a hardware device for converting data frames from the communications technology used on the LAN into frames suitable for the WAN connection and vice versa. The CSU transmits and receives signals to and from the WAN line and also provides a barrier for electrical interference. The DSU manages line control and converts input and output signals. CSU stands for Channel Service Unit and DSU stands for Data Service Unit. A CSU/DSU can also act a type of bridge in relation to the media types in use. A good example of this is connecting a copper twisted pair based LAN to a fiber optic based WAN connection.

3.3 Explain the advanced features of a switch

PoE

Power over Ethernet (PoE) is the ability of some switches to provide a constant supply of DC power to the network via Ethernet cabling. This can be useful in areas where it is difficult to implement power or to save the total amount of wiring for the location. Very little configuration is necessary to implement this feature and it requires little maintenance.

Spanning tree

The Spanning Tree Protocol (STP) is a link management protocol that implements the spanning tree algorithm for providing path redundancy while preventing undesirable loops in a network that are created by multiple active paths between hosts. This addresses both traffic loops and events of link failure. Spanning tree is defined in the IEEE 802.1d standard.

Bridging loops can occur when there are multiple paths between hosts. In order to establish proper path redundancy without introducing endless loops, STP creates a tree that spans all of the switches in the network and forces redundant paths into a standby, or blocked state.

STP allows only one active path at a time between any two hosts for the purpose of loop prevention. The redundant links are established as standby backup paths. If STP costs change or if a network segment in the STP becomes unreachable, the spanning tree topology is reconfigured with a standby path activated.

VLAN, Trunking

VLANs were described previously, Please refer back to section 2.7.

A VLAN can contain many types of hosts, all of which are combined into a single logical broadcast domain. Trunking is the technique of combining several VLANs into a single port for transmission. Without this feature, a port is restricted to a single VLAN. In order for this to be implemented, the devices must support VLAN Trunking Protocol (VTP). Trunking is defined in the IEEE 802.1q standard.

Port mirroring, Port authentication

Port mirroring is the technique of sending a copy of all packets on one switch port to another switch port that has network monitoring tools in use. This allows traffic to be examined for problems and potential security risks.

Port authentication is the strategy of restricting specific ports on a switch. This determination of restriction can be based on several factors, such as MAC or IP address. A good example of this would be restricting access to a specific server connected directly to a switch based on a set of MAC addresses. If the requesting host does not match the acceptable set of MAC addresses, it will be denied access.

3.4 Implement a basic wireless network

Install client

The installation of a basic wireless network is very similar to the implementation of a basic wired network, with a few exceptions. A wireless client must be using a compatible version of wireless technology (e.g. 802.11a, 802.11g, etc.) to communicate on the wireless network. This functionality is usually contained within the wireless NIC, but may also require a piece of client software to make the connection. This is the first step in enabling a node to connect to the wireless infrastructure.

Access point placement

Determining the number and placement of access points to provide adequate coverage throughout the facility is crucial in implementation of a wireless network. Without a string signal, clients will have limited or no connectivity. An RF site survey is performed prior to implementation to determine the best placement of the access points. As a general rule of thumb, access points usually need to be mounted high, towards or inside the ceiling plenum area.

Install access point

When installing an access point, the following configurations must be made:

- Appropriate encryption type
- Set channels and frequencies
- Set SSID and beacon

An improper configuration of these settings will cause wireless network connectivity to fail. The clients must also be configured with the same settings as determined on the access point

Verify installation

There are several ways to verify and test the installation of a wireless network. The most obvious test would be whether clients can see the wireless network. This verifies that the network is being advertised as available. Next, verification of the client connection to an access point ensures that the configuration of the wireless settings is correct on both sides. Generally, speaking, the final test is whether or not a client can access resource via the wireless network. This could be a shared folder or printer, a server based application or even basic Internet access.

A failure in any of these areas indicates an issue. The actual are of the issue can be logically determined by where in the trail of events the breakdown occurs. For example, if a client cannot see the network at all, it is not likely that the issue is related to the external Internet connection.

Using the technique of first verifying the installation will help to mitigate most common problems. It is not a good practice to just assume that it will work if you plug it in and power on the device.

If a problem arises, troubleshooting a wireless network should be done in the same logical, modular fashion as any type of network. Verify the basics first and then move on to more technically advanced possibilities.

Domain 4.0: Network Management

Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5
- Objective 6

4.1 Explain the function of each layer of the OSI model

The OSI Layers

The OSI (Open Systems Interconnect) model is a reference model that describes the top to bottom process of network communications. The OSI model is an ISO standard and defines a networking framework for implementing protocols in seven layers. Each defined layer provides services to the one above it and the one below it. It is also used by programmers to determine the steps involved in making a reliable application that uses network resources. For the Network+ exam, you must know the layers and their function, resident devices and protocols, by both name and number.

The Application Layer (Layer 7) is best described as the user interface. This is where a human spends their time when working on a computer. Protocols such as HTTP, SMTP and FTP work at this layer.

The Presentation Layer (Layer 6) is responsible for the formatting of data. Services such as data compression, decompression, encryption, and decryption are provided here. The protocols at this layer are not often thought of as such, but are protocols by the strictest definition of the word. Usually these are seen as file formats. Some of these include JPEG, MPEG, MIDI, PICT, Quick Time, and TIFF.

The Session Layer (Layer 5) is responsible for coordinating communication between network nodes. In simplest terms, it handles dialog control between the connection endpoints. Session layer protocols include SCP, RPC and SSH. Some protocols that are associated primarily with other layers have functions that are handled at layer 5. A good example of this is L2TP.

The Transport Layer (Layer 4) is responsible for flow control and error correction. When speaking of connection oriented resources, it is layer 4 that ensures the reliable end to end connection. The segmentation of data also occurs at the transport layer. Some transport layer protocols include TCP, UDP, SCTP and SPX. Layer 4 is also considered to the intermediary layer between the software layers (5-7) and the hardware layers (1-3). At this layer you begin to associate hardware devices with it, such as layer 4 routers and switches.

The Network Layer (Layer 3) is where logical addressing occurs. Its primary responsibility is sending data packets from the source to the destination using logical addressing information. Routing occurs at this layer as well as Internet addressing. Packetization of data occurs at this layer. Some layer 3 protocols include IP, IPX, IPSec, DNS, and ICMP. Network layer devices include routers and layer 3 switches.

The Data Link Layer (Layer 2) is responsible for host to host packet delivery as well as hardware addressing. It is divided into two sub-layers; the upper Logical Link

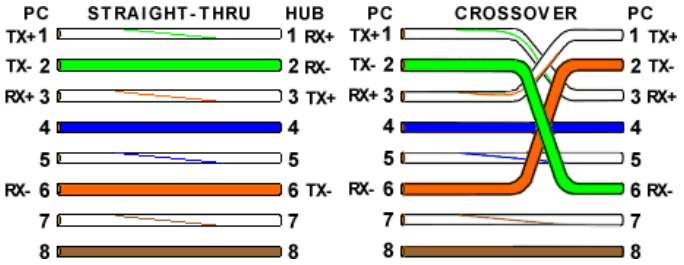
Control (LLC) and the lower Media Access Control (MAC). The LLC sub-layer handles tasks such as error control, flow control and framing, while the MAC sub-layer handles access to shared media. LLC provides the translation service between the hardware and logical addressing. Framing and encapsulation of data occurs at this layer. Layer 2 protocols include Frame Relay, ATM, ARP, RARP, Ethernet, 802.2, 802.11, PPP, L2TP, PPTP and Token Ring (802.5). Data Link layer devices include bridges, switches, and Frame Relay or ATM switches.

The Physical Layer (Layer 1) is where the actual electrical flow of signals takes place. As the name indicates, this is actual media and connections that can be physically touched and seen. Layer 1 defines the signaling type in use as well as device types needed for transmission. The conversion of data into a pure bit stream occurs at this layer. Physical layer protocols include RS232, V.92, cabling standards, ISND and DSL. There are many devices at this layer as any hardware has a function at this layer in some respect. Pure layer 1 devices include modems, hubs, repeaters, concentrators, cabling and even electrical wiring.

4.2 Identify types of configuration management documentation

Wiring schematics

Wiring schematics can represent various aspects of a network such as the cable plant, wiring of a custom hardware interface or even as basic as the pin out scheme for network cables. The key is to recognize one when seen. Below is a schematic of crossover versus straight cable wiring.



Physical and logical network diagrams

Physical diagrams deal with physical hardware placement and connections, while logical diagrams deal with logical network connections. They serve to supplement each other, even though a network's logical topology is often different from its physical topology.

A physical network diagram is primarily used for representing the physical layout of a network including the placement of devices and cabling. A logical network diagram represents how network connections are made in regards to transmission of data. The IP addressing scheme is considered to be part of the logical diagram.

Baselines

Baselines allow comparisons of network performance and effectiveness to be made. By establishing a baseline, or normal level of operations at a given time, current operations can be compared to determine if the network runs more efficiently or needs improvement. This could be after implementation of a new technology or devices or perhaps to determine if certain steps

should be taken.

NOTE: When devising the baseline, take into account both peak and non-peak usages. However, when monitoring usage, make sure you do not interrupt regular network activities.

Policies, procedures and configurations, Regulations

Network documentation is not limited strictly to schematics of the network and baselines. There are many other factors involved in a network management scenario that must be documented. Some these could include, but are not limited to:

- Password policies
- Hardware disposal procedures
- Due diligence for purchasing policies
- New employee hire policies
- Administration and management policies
- Stated goals for future growth
- Implementation or rollout plans
- Government regulations
- Company policy/regulations

The point to keep in mind is that all things related to the management, growth and operations of a network, both directly and logistically should be documented and available to the appropriate staff. These types of documents help to clarify overall goals of network growth and usage as well as to clarify policy confusion. They also provide accountability and remove deniability of compliance. In the event of a staff member leaving, their function is documented and can be easily handed over to a new employee.

In short, documentation is the “Rosetta stone” of a network’s operational procedures and expectations. In many cases, documentation is not only a good idea for management and planning, it is legally required.

4.3 Given a scenario, evaluate the network based on configuration management documentation

Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure; Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed

Review the previous section for explanation of the various documentations types. Using these documents can greatly reduce the difficulty of determining many types of issues, network growth patterns, areas of weakness and improvable sections. These issues, plus ones that cannot be foreseen, are why it is critical to maintain excellent documentation.

It is also critical to keep documentation up to date. Having documents that represent the network 5 years ago are not helpful, unless no changes have been made during that time. Typically, there is a document that describes documentation update procedures. These usually have to be approved by management after update.

4.4 Conduct network monitoring to identify performance and connectivity issues using the following:

Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)

Network monitoring utilities are used to mitigate issues and determine the source of problems once they occur. They work by examining network traffic and reporting any irregularities back to the user. They can be used to determine network efficiency, network attacks, traffic patterns and many other aspects of overall network security and performance. There are many off the shelf products available for these purposes.

System logs, history logs, event logs

Log files are used to determine the source of an issue or other after-the-fact information about network or host activity. Log files create an audit trail which can be reviewed to determine the source of issues, appropriate actions or even to mitigate potential future problems.

System logs are typically associated with the internal workings of a device's software. History logs can be many things and are usually in relation to a specific area or piece of software. Web browser history is a good example of a history log. Event logs record specific events and their success or failure. These usually come with a default set of parameters, but can be customized to track user defined events.

4.5 Explain different methods and rationales for network performance optimization

Methods:

QoS, Traffic shaping

The goal of implementing QoS (Quality of Service) is to make network performance relatively more predictable and also to allow bandwidth utilization to be more effective. QoS involves classifying traffic by assignment of class of service values to frames at incoming interfaces on core networking equipment like routers and more advanced switches. You seldom do this at the outgoing interfaces. The primary focus of QoS is to provide more predictable network performance.

A typical QoS configuration provides dedicated bandwidth for delay sensitive traffic such as voice and video. There are queuing mechanisms for congestion avoidance and congestion management as well as network traffic shaping procedures. These processes typically require traffic classification.

Classifying traffic helps to ensure that time sensitive traffic can receive appropriate priority. To properly define each traffic class the current applications and their unique parameters must be determined. Future growth and deployments must also be considered whenever possible.

Traffic shaping is an integral part of most QoS implementations. Review section 3.2 for a more detailed explanation of traffic/bandwidth shaping.

Load balancing, High availability, Caching engines, Fault tolerance

Load balancing is the technique of evenly distributing workloads across network resources. For a more detailed explanation review section 3.2.

High availability is related to fault tolerance. Basically it means to ensure that a network resource is available for access as much as possible. This can be done in many different ways and the techniques will vary greatly according to the resource type and unique factors involved. An example of a high availability solution is server clustering or printer pooling.

Caching engine can mean a few different things. It could be a caching server that saves copies of recently accessed Web pages or internal Web content, or a switch or router that caches resource location information. In any case, the intent is the same: to provide greater speed in accessing resources.

Fault tolerance is the technique of providing an alternative to a resource should it become unavailable. This is typically done by creating redundancy in resources. An example of this could be a secondary DNS server, authentication server or core networking hardware device. Typically, implementation of redundancy means higher costs.

Reasons:

Latency sensitivity, High bandwidth applications

The intention of the previously mentioned strategies is to provide a more reliable and robust delivery of network resources. Many resources have latency, or timely delivery, sensitivity. Good examples of this are Voice over IP (VoIP), video conferencing and IP-based television. Latency can cause poor quality of performance and even failure in these types of applications.

Another major factor that these strategies address is the fact that some applications require a significantly higher amount of bandwidth to operate properly. By assigning values, traffic shaping and ensuring quality of service, higher bandwidth applications can be ensured the resources they need to deliver their services more reliably and accurately.

Uptime

Uptime is always a concern for a network administrator and often times it a factor in evaluation of their performance. Uptime basically means the percentage of time that a resource is available for use. A Service Level Agreement (SLA) usually defines an expected or promised uptime. This is a contract between the customer and the provider and is usually legally binding. Though they are increasingly combined, voice services and data services historically have had different expectations of uptime; with voice requirements being much more stringent.

4.6 Given a scenario, implement the following network troubleshooting methodology

When confronting a problem in the world of networking, few things serve a technician better than a good strategy for troubleshooting the issue. The best practice is to have a logical set of steps that cover the possibilities from simplest to most complex. This is important because often times problems have a simple causality and thus a simple solution. Also, the information obtained from checking the basics first is usually required to investigate a more complex set of circumstances. The best rule of thumb is to use modular techniques. This means to break the whole situation into the parts from which it is made and examine each one for integrity. The following list is a good basic methodology to use:

- Information gathering – identify symptoms and problems
- Identify the affected areas of the network
- Determine if anything has changed
- Establish the most probable cause
- Determine if escalation is necessary
- Create an action plan and solution identifying potential effects
- Implement and test the solution
- Identify the results and effects of the solution
- Document the solution and the entire process

In the real world, there is no single rigid approach as most problem solving processes are tailored to the environment. Another good thing to keep in mind is the OSI model. Its layers provide a

logical breakdown of the end to end communication process and can often help to isolate an issue.

NOTE: The OSI's 7 layer model can be used as a guide for systematic network troubleshooting. Remember these facts:

- A layer 1 problem means a physical connectivity problem.
- A layer 2 problem usually means a problem with the LAN, often times an issue with switching.
- A layer 3 problem usually means a problem associated with IP addressing or routing.
- A layer 4 or above problems are typically related to applications, but could be related to traffic issues or flow control problems.
- Layer 7 issues almost always involve the end user applications.

In the end, some issues are solved because of past experience with that specific issue. When a technician or administrator knows their environment and has excellent documentation of the network and its resources, as well as past problem resolutions, this can help facilitate a more timely solution to the current dilemma. Many problems are related and occur in the same area, though their solution may vary slightly. This is one reason why it is important to isolate what the issue is and where it is occurring.

4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution

Physical issues:

Cross talk, Near-end cross talk, Attenuation

Crosstalk is a phenomenon in which a signal transmitted on a channel creates an undesired effect in another channel. Such phenomenon is usually caused by undesired capacitive, inductive or conductive coupling from one channel to another. Near-end crosstalk refers to an error condition that may occur when connectors are attached to a twisted pair cabling that has crossed or crushed wire pairs. Attenuation refers to reduction in signal strength that can occur with digital or analog signal, usually due to the distance the signal has traveled. Extent of attenuation is commonly expressed in units of decibels (dBs).

Collisions

Collisions occur when more than one network host attempts to transmit simultaneously. This is an extremely common occurrence in Ethernet networks and is responsible for a large amount of the overhead loss of bandwidth. Replacing hubs with switches segments the network into collision domains to help reduce the impact.

Shorts
Shorts or broken wires can be identified with a cable tester. A short will stop communications cold and lead to data and connectivity loss. Usually it is best to replace a shorted or broken cable rather than repair it. This depends on where the short or break is and the resources at hand.

Open impedance mismatch (echo)
Impedance is the resistance of current flow based upon the pure resistance and the inductance and is expressed in ohms (Ω). Impedance matching involves two connections being at the same impedance level. When they are mismatched, this causes a signal reflection and can cause several problems. This is due to the fact that the receiver or sender cannot tell which is the actual data and which is the reflection. With wireless communications, an antenna's impedance should match that of its connecting transmission line.

An example of an issue caused by open impedance mismatch is echo. This is primarily seen in voice applications. This is where the voice heard on the line seems to echo back like in a tunnel. In the case of VoIP technology, this can be seen as chatter or signal loss.

Interference
Interference can come in many forms. In terms of networking, the most common type is electromagnetic interference (EMI). When electricity is conducted over a metal carrier, a magnetic field is generated around the medium. When one of these fields disrupts the flow of electricity in another medium it can disrupt the flow on that medium. When this happens to a wire transmitting data, it can disrupt the transfer completely and effectively stop communications.

Logical issues:

Port speed, Port duplex mismatch
Port speed refers to the throughput rate at which the port is operating. The most common are 10Mbps, 100Mbps and 1000Mbps. A speed mismatch can cause a bottleneck in the network, possibly leading to performance issues. These are usually caused by incompatible hardware, but can be a result of manual configuration. Port duplex refers to the communication type of the port. This could be half or full duplex. When the duplex is mismatched, this will cause significant communication issues. Small transfers will not seem to be effected, but when a large transfer is attempted, the network will slow to a crawl. Duplex mismatches usually result from an incorrect manual configuration.

Incorrect VLAN, Incorrect IP address
With incorrect VLAN settings the logical VLAN connection will fail to be established and the host will be effectively isolated from the network. This is tantamount to assigning the wrong network to a host. With an incorrect IP address the device will fail to communicate with other devices even though physical connection is error free. Again, the host is effectively isolated from the rest of the network.

Wrong gateway, Wrong DNS, Wrong subnet mask

When a host has an incorrect default gateway assigned, it will not be able to communicate with devices outside of its subnet, including, usually, the Internet. When a host has an incorrect subnet mask, it will effectively be in a different subnet and will not be able to communicate with devices with in its subnet. When a host has incorrect DNS settings, it will not be able to use host names to connect. It can still connect using the IP address, however.

Here are some issues that should be identified, but escalated:

- Switching loop
- Routing loop
- Route problems
- Proxy ARP
- Broadcast storms

Switching loops can occur when you have more than one path between two switches in a network. Routing loops can happen when there are multiple paths to a destination. Proxy ARP refers to the technique of using ARP to provide for an "ad hoc" routing mechanism, which can produce problems under an already problematic routing configuration. Broadcast storms are usually the result of hardware errors and can saturate a network to the point of cessation in communications.

Wireless Issues:

Interference (bleed, environmental factors)

Sources of RF interference may include microwave ovens, wireless phones, Bluetooth enabled devices and other wireless LANs. The introduction of other signals into the wireless LAN is called signal bleed. To mitigate this, it is a good idea to analyze the potential for RF interference in the area where the wireless LAN is in operation. Preventing the interference will provide more adequate wireless coverage and operation. Environmental factors must also be taken into account. There are many things that this encompasses and it is not limited to natural factors such as weather. It can also include the physical environment. Areas with large amounts of concrete infrastructure may give wireless LANs problems, for example.

Incorrect encryption

Incorrect encryption settings can result in connection failure. The encryption type to be used is part of the build and tear down cycle of a connection and must be the same on both ends.

Incorrect channel

Incorrect channel settings can result in connection failure. The client must use the exact same channel for communication as the server.

Incorrect frequency

Incorrect frequency settings can result in connection failure. Both the client and the server must communicate over the exact same frequency range. In the United States, the FCC decides who may use which frequencies for which purposes. Megahertz refers to "millions of cycles per

second". Kilohertz refers to "thousands of cycles per second". All FM radio stations transmit in a band of frequencies between 88 megahertz and 108 megahertz. AM radio is confined to a band from 535 kilohertz to 1,700 kilohertz.

ESSID mismatch, Standard mismatch (802.11 a/b/g/n)

The ESSID must be the same on the AP and the rest of the wireless network. A mismatch can lead to communication failure. Standard mismatch refers to the 802.11 iteration in use. The common types are 802.11a, 802.11b, 802.11g and the newest 802.11n. Typically the newer standard will be able to communicate with previous standards, but not the reverse.

Distance

Distance is always a concern with wireless networks. The closer a client gets to the edge of the coverage area, the more the signal will degrade. This can be mitigated by using high gain antennas and wireless bridges to extend the signal range. Most basic implementations of wireless LANs use Line of Sight to transmit. This requires that the path between the two points be clear. This must be taken into consideration when extending a network range.

Bounce

Bounce occurs when the wireless signals hit and scatter from a reflective surface. Windows and mirrors are prime examples of things that can cause bounce. In an enclosed environment, this may not cause too much of an issue, but in an area that is close to the edge of the range, this could cause loss of communications.

Incorrect antenna placement

As before mentioned, most wireless LANs require clear communication paths between antennas. When decisions are made for antenna placement, line of sight is critical in determining the optimal spot. Many things can cause line of sight blockage including trees, mountains, poor weather and many man made objects. The elliptical shaped area of the line of sight pat his called the Fresnel zone. It often varies in thickness depending on the length of the signal path as well as the frequency of the signal.

Domain 5.0: Network Tools

Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5
- Objective 6

5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality

Traceroute

Traceroute is a utility that sends an ICMP packet from the issuing node to a user input destination and displays information about what is happening to the packet on each point along the path. It is very useful in determining where a network outage is occurring, testing connectivity and determining bottlenecks in traffic. The command for Unix systems is traceroute, whereas on newer Linux systems the command is tracepath. Current Windows based machines use the command tracert. Windows NT used the pathping command for similar functionality.

Ipconfig, Ifconfig

The Ipconfig command displays network interface information in Windows machines. The /all switch added to the command shows more detailed information for all installed interfaces. It is useful to determine IP addressing information as well as the protocols in use on the interface. The graphic represents a snippet of the output from an ipconfig /all command:

```
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 00-15-58-B1-37-4E
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.123.130
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.123.254
        DNS Servers . . . . . . . . . . . : 203.198.23.208
```

If DHCP is in use on the network, Ipconfig can also be used to purge and reapply the IP addressing information. To clear the addressing information issue the command ipconfig /release. To obtain a new address or to renew the current address use ipconfig /renew.

On a Linux system, the comparable command is ifconfig. It serves some of the same functionality as ipconfig, but has more features. It even has a configuration file associated with it that can have persistent settings added to it.

Ping, ARP ping

The ping command uses ICMP to send echo requests from one host to another for the purpose of testing connectivity. It can also be used to test the host's local interface by pinging its loopback address. Ping works by either host name or IP address. This is usually the most basic step in troubleshooting most connectivity issues. ARP ping is basically the same thing except that it uses the ARP protocol instead of ICMP. This allows it to ping based upon layer 2 addressing information.

ARP

The arp command resolves IP address to MAC address. It displays the entries in the local interface's ARP table. This is a table with all of the recent hosts that the node has contacted. The –a switch will display all entries, the –s switch manually adds an entry and the –d switch deletes an entry.

> NOTE: The ARP table is not static. It is cleared when the system is rebooted.

NSLOOKUP, Host, Dig, Mtr

NSLOOKUP is the Windows based DNS utility as previously mentioned. Dig is the Unix/Linux version of this command. These utilities are especially useful when the suspected issue is DNS resolution errors or DNS functionality. These utilities create a session with the DNS server directly and allow host names and IP address to be resolved, as well as testing different services on the network, such as the mail server and even communications with other DNS servers.

Host is a Unix/Linux utility that allows DNS queries for a designated host name or the in the reverse for a specified IP address. The Unix/Linux based mtr command combines the functionality of traceroute and ping into one single network diagnostic tool. It is useful for testing connectivity and path determination, as well as to determine downed links along a path or high congestion areas.

Route

You use the route command to manipulate the routing table. For example, route print is the command for displaying the entire routing table, as shown here:

```
G:\Documents and Settings\Administrator.NEWSETUP>route print

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 15 58 b1 37 4e ...... Realtek RTL8139 Family PCI Fast Ethernet N

===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  192.168.123.254  192.168.123.249     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
    192.168.123.0    255.255.255.0  192.168.123.249  192.168.123.249     20
  192.168.123.249  255.255.255.255        127.0.0.1        127.0.0.1     20
  192.168.123.255  255.255.255.255  192.168.123.249  192.168.123.249     20
        224.0.0.0        240.0.0.0  192.168.123.249  192.168.123.249     20
  255.255.255.255  255.255.255.255  192.168.123.249  192.168.123.249      1
Default Gateway:   192.168.123.254
===========================================================================
Persistent Routes:
  None
```

Nbtstat

You use this command to review protocol statistics and to perform name resolution of NetBEUI over TCP/IP. This obviously makes this a Windows-only utility. The –n switch can be used to show all local entries as shown in the graphic:

```
Node IpAddress: [192.168.123.130] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    YCT-98B0A682613<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    YCT-98B0A682613<20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
```

Netstat

You use the netstat command to find out about all of your active connections. It is useful in determining if a session is being established and too see if unauthorized clients are connecting. Here is a sample output:

```
C:\Documents and Settings\ycthk>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    yct-98b0a682613:1181   localhost:27015        ESTABLISHED
  TCP    yct-98b0a682613:27015  localhost:1181         ESTABLISHED
  TCP    yct-98b0a682613:2841   63.150.131.166:http    CLOSE_WAIT
  TCP    yct-98b0a682613:2849   63.150.131.166:http    CLOSE_WAIT
```

With the –a switch all active ports and their status information will be shown:

```
C:\Documents and Settings\ycthk>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    yct-98b0a682613:epmap  yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:microsoft-ds  yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:1025   yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:2869   yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:smtp   yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:pop3   yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:1026   yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:1181   localhost:27015        ESTABLISHED
  TCP    yct-98b0a682613:10110  yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:27015  yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:27015  localhost:1181         ESTABLISHED
  TCP    yct-98b0a682613:netbios-ssn  yct-98b0a682613:0      LISTENING
  TCP    yct-98b0a682613:2841   63.150.131.166:http    CLOSE_WAIT
  TCP    yct-98b0a682613:2849   63.150.131.166:http    CLOSE_WAIT
  UDP    yct-98b0a682613:microsoft-ds  *:*
  UDP    yct-98b0a682613:isakmp  *:*
```

NOTE: The Linux netstat command allows querying of IP addresses and interfaces to which the several daemons are listening. By using the netstat and grep commands for the proper port, IP addresses that a given daemon are listening to can be found. Alternatively, you may rely on the -a option for the ifconfig command to display verbose network information on all interfaces.

5.2 Explain the purpose of network scanners

Packet sniffers

Packet sniffers, also known as protocol analyzers, are software utilities that capture network traffic and allow it to be analyzed on a bit by bit basis if desired. They are useful tools for determining network issues and their causes. They can however also be used for many nefarious purposes such as identity theft and to gain information to launch a network attack. The usage of these must be monitored closely and only allowed when necessary.

Intrusion detection software, Intrusion prevention software (IDS/IPS)

IDS/IPS Sensors detect network intrusions based on signatures. Signatures define the types of network intrusions to be detected by the sensor. Existing signatures can be modified or new ones can be defined as needed. Network sensing involves real-time packet capture and analysis as well as the monitoring of logged traffic. If an IDS/IPS detects an attack, it can generate alarms or IP session logs, and may even deny entry to a specific network host or network through dynamically reconfiguring and reloading a network device's ACL if present. This technique is known as shunning.

Port scanners

Port scanners are used to find open software ports in a network or a specific host. From the standpoint of administration, they are handy tools to determine weaknesses in network security. However, they can also be used to determine the weak spot in a network for an attack. Port scanning is determining open ports on a specific host. Port sweeping is checking all hosts for a specific port number.

NOTE: You can deter scanners by limiting the number of access attempts. Failed login attempts are good indicators of scanning activities. Attempts that exceed the pre-defined limits may result in long delays that discourage the scanning process.

5.3 Given a scenario, utilize the appropriate hardware tools

Protocol analyzer

Protocol analyzers are valuable tools to evaluate your security setup. One example is determining if a firewall is blocking port scans from outside the network. They can also be used to identify the sender of stealth port scans as well as detect the true source IP address when a spoofed IP connection is used.

Cable testers, Certifiers, TDR, OTDR, Multimeter

Cable testers can be used to test and report on cable conditions such as basic connectivity, near-end crosstalk, attenuation, and noise. Certifiers are basically the same as a cable tester, but can determine whether your network sufficiently meets specific ISO or TIA standards.. A TDR (time domain reflectometer) introduces pulses on a line and measures the flux in impedance. These are handy for measuring many of the same things as a cable tester. An OTDR is the optical version and is used for testing fiber optic cables for connectivity as well as correct light spectrum distribution. Multimeters are used to measure physical layer parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity.

Toner probe, Butt set

A toner and probe is a handy tool for identifying a single cable or wire pair set amongst a bundle of cabling or wiring. These are especially handy when installing the initial cabling at a site or to determine a problematic cable. These tools can disrupt traffic in the network and should be used only when necessary during operational hours. A Butt Set is a special type of telephone handset for installing and testing local loop telephone lines. These are usually seen in use by voice installers and repair technicians.

Punch down tool, Cable stripper, Snips

A punch down tool is a small screwdriver-like tool that is usually spring loaded at the tip and is used for connecting wiring to a punch down block. They work by pushing the wire between two metal contact points that are sharp and cut into and make contact with the wire. Below is a picture:

A cable stripper is used to pull the plastic sheathing that wraps individual wires so that metal to metal contact can be made. For instance, be fore an RJ-45 connector can be crimped to a Cat5 cable, the wire must be exposed using a stripper. Most crimp tools have strippers built into them, but stand alone ones can also be found, as seen in this graphic:

Snips are scissor-like tools used to cut the wires themselves or sheets of metal. These are handy to make the ends of a set of cable wires even before inserting them into a connector..

Voltage event recorder

Voltage event recorders are hardware devices that are plugged into the electrical system of a site and record various events. Some of these events include sags, swells, transients, outages and frequency variations on line voltage at the receptacles. They typically come equipped with and interface for administration and software to configure various parameters such as event types and thresholds for the events. They are extremely handy for determining if network problems or outages are due to variations in the power supply.

Temperature monitor

Temperature monitors are basically complex thermometers with integrated thermostats. These can be configured to send alarms to an administrator in the event of extremes in temperature. These are typically deployed at remote sites that are not readily available physically. These can also send real time data involving the temperature at a given site.

Domain 6.0: Network Security

Quick Jump To:

- Objective 1
- Objective 2
- Objective 3
- Objective 4
- Objective 5
- Objective 6

6.1 Explain the function of hardware and software security devices

Network based firewall, Host based firewall

Remember that a firewall is a piece of hardware, software or both that shields a network from the outside. A network based firewall is a firewall that protects an entire network. This is the typical deployment in most business environments. A host based firewall is exclusive to a single node and protects the local system from attack. This is a typical desktop and home implementation of a firewall.

IDS/IPS

Intrusion detection system (IDS) / Intrusion Prevention System (IPS) is a software or hardware based device that can detect many types of attacks on a network. The primary security function this provides is a packet by packet analysis of traffic it captures. The primary function of an IDS/IPS is to detect and prevent network attacks and obfuscation of data.

VPN concentrator

A VPN concentrator is a hardware device that hosts the VPN connection for the network while at the same time combining the administration functions required to host a VPN. These greatly centralizer and simplify maintenance of the VPN while providing higher levels of filtering, connection services and encryption. By combining all of these functions in a single interface they provide a better response to network attacks as there are not several interfaces.

6.2 Explain common features of a firewall

Application layer vs. network layer, Stateful vs. stateless

Application layer firewalls are more like a proxy server than a true firewall, except that they can reject traffic based upon certain criteria. Network layer firewalls actually perform routing functions and filter based upon network layer addressing information. Stateful firewalls have the ability to inspect packets and determine if the packet is accepted based on a wide set of criteria. Stateless firewalls simply make decisions on source and destination addressing and lack the ability to detect if a packet is not what it says it is.

Scanning services

In regards to a firewall, there can be many types of scanning services. The types and range of services depends on the type of firewall implemented. Some have the ability to perform port scanning, data packet scanning for integrity and authenticity and even the ability to scan for certain attack types and spoof the source of the attack.

Content filtering

Filtering content involves examining traffic at the firewall for certain types of data and denying access to types that do not meet the acceptable criteria. This could be adult content, certain keywords, specific URLs and even applications. This is essentially a proxy service but has the added capability of rejecting traffic, notifying the user and logging the event. These parameters are typically set via graphical user interface and are often browser-based utilities.

Signature identification

Signature identification means the firewall is checking for specific digital patterns, or signatures, in the data. These patterns of binary information are compared against a database of known malicious software signatures and rejected as needed.

Another possible definition of signature identification is the use of application layer firewalls to check for digital certificates that have verified digital signatures. This is typically associated with secure Web sites and VPN authentication. In either type of signature verification, a database is used to store the acceptable or banned signatures.

Zones

Firewall zones are a new concept introduced by Cisco. This provides a way of defining areas protected by a firewall and which application and types of actions can be performed in each zone. Zones require a security policy to be defined and these policies to be associated with certain zones and actions. These are called policy maps. Class maps must also be defined for the traffic types. By combing the class and policy maps and then assigning them to zones, a more detailed level of traffic filtering to specific hosts or groups of hosts. This also makes the network more secure as only acceptable actions can be performed.

6.3 Explain the methods of network access security

Filtering:

ACL

An ACL is an access list. These are implemented typically on a router and provide the capability to restrict traffic flow to and from specific hosts or software ports. The ACLs filter based upon addressing information or port numbers. By restricting access to a specific group of hosts or ports, connections that have been identified as dangerous can be blocked from communications.

MAC filtering, IP filtering

MAC filtering involves examining the MAC address in a packet and allowing or denying access based on a defined list of acceptable addresses. This type of filtering takes place at layer 2. IP filtering involves examining the IP address in a packet and allowing or denying access based upon on a defined list, usually an ACL. This type of filtering takes place at the network layer.

Tunneling and encryption**:**

SSL VPN

Tunneling and encryption are typically associated with a VPN. Basically, tunneling is the act of creating a virtual tunnel via a series of virtual circuit connections and allow a portal for data to traverse through a public network such as the Internet. In order to secure the tunnel data stream, encryption is usually implemented so that data is not easily read in the case of a tunnel breach. Secure Sockets Layer (SSL) is a protocol designed to enable encrypted, authenticated communications across the Internet. SSL involves the use of IPSec. An example of SSL is a Web address that use HTTPS in the URL. An SSL VPN utilizes IPSec to establish a tunneled external connection to a network. This provides an extra layer of security to a VPN and further helps to ensure sensitive data and communications cannot be easily stolen. SSL usually involves the use of digital certificates which allows connections to be filtered based upon the acceptance or rejection of a certificate.

VPN

A VPN is a virtual network created between a remote user and a LAN. These provide a tunneled, encrypted data transport for secure communications. This allows a remote user to access network resources as if they were directly connected to the network.

L2TP

L2TP is a layer 2 tunneling protocol that uses IPSec to provide secure communications and authentication. This is used in the context of a VPN and thus provides filtering based by not allowing suspicious connection from taking place.

PPTP

PPTP is similar to L2TP. The main difference is that PPTP's encryption does not use IPSec and is not considered to be as secure as L2TP. In regards to filtering, again this is employed with remote access or VPN clients and provides a vehicle to filter suspicious connections

IPSec

IPSec is a framework for securing IP based communication sessions. It works by encrypting and/or authenticating each IP packet in transit. There are two modes available – the fully routable transport mode and the more secure tunnel mode.

Remote access:

RAS

Remote access is the method of providing off-site access to approved users. By creating a list of acceptable user accounts or hardware or network addresses, connections can be filtered. Remote access is typically associated with either dial-in access or VPN.

RAS is the remote access server. This is the server that provides the dial-in or VPN access The RAS maintains the filtering list for acceptable connections and accepts or denies traffic and/or connections based upon these lists.

RDP
Remote Desktop Protocol (RDP) is a special protocol that allows a user to connect to a computer via terminal services. This allows a virtual desktop session to be established. To the end user it looks like they are sitting directly at the console to which they are connected. RDP uses TCP port 3389 by default.

PPPoE
PPPoE (Point to Point Protocol over Ethernet) is a network protocol that encapsulates PPP frames inside Ethernet frames. It is very common with ADSL services. The two distinct stages are PPPoE discovery and PPP session.

PPP
Point-to-Point Protocol (PPP) is one method of connecting a computer to a remote network. It works at the data link layer, is more stable than SLIP and has error checking features included. PPP negotiation consists of three phases: Link Control Protocol (LCP), Authentication, and Network Control Protocol (NCP). Note that both SLIP and PPP encapsulate datagrams and other network-layer protocol information over point-to-point links.

VNC
Virtual Network Computing (VNC) is a desktop sharing system which uses a special protocol to transmit keyboard and mouse events from one computer to another. This allows remote desktop and control sessions to be established. This is very similar to using RDP and terminal services, but requires the VNC client software to be installed on the target machine.

ICA
ICA (Independent Computing Architecture) is the Citrix Systems proprietary protocol used by Citrix based application server systems. This allows remote control and desktop session to be performed without regard to system platforms. It also has the capability to create remote sessions with specific applications.

6.4 Explain methods of user authentication

PKI
A public key infrastructure (PKI) is a system of digital certificates, Certificate Authorities, and other registration authorities for verifying and authenticating the validity of the parties involved in an Internet transaction. The user must have the public key as well as the certificate that contains the private key. By requiring both keys, establishing a connection is much more secure and it is much more difficult to provide fake credentials and be authenticated.

Kerberos
Kerberos is a network authentication protocol. It is designed to allow two parties to exchange private information across the network. It works by assigning a ticket to each user which is then embedded in messages to identify the sender. Windows 2000/2003/2008 use Kerberos for authentication within the domain.

AAA
AAA is a framework for creating a security model, usually on a router. It is actually three components: Authentication, Authorization and Accounting. Authentication refers to the process of validating the claimed identity of an end user or a device. Authorization refers to the act of granting access rights. It gives you the ability to limit network services to different users via dynamically applied access lists. Accounting refers to the methods to establish who (or what) performed a certain action. In fact, the accounting function may be used for connection time billing. It may also be used to track suspicious connection attempts into the network.

RADIUS
Remote Authentication Dial-In User Service (RADIUS) refers to an authentication and accounting system for remote access. When a user dials in to a network they must enter their username and password for validation by the RADIUS server for access authorization. Modern remote authentication is typically implemented through RADIUS and TACACS+.

TACACS+
Terminal Access Controller Access Control System (TACACS) refers to an authentication protocol that allows a remote access server to communicate with an authentication server for determining if the user has access to the network. TACACS+ is a new protocol that is not compatible with TACACS.

Network access control, 802.1x
Network access control is a set of rules or requirements that control access to a network at the connection endpoints. If the host attempting to connect does not satisfy the requirements, it is denied access. IEEE 802.1X is port-based Network Access Control. In this case, port refers to the connection to the LAN itself, not necessarily a software port. 802.1X provides authentication services for network connections. If the criteria is satisfied, a point to point connection from the host to the LAN is established. If the criteria is not met, the connection is denied.

CHAP, MS-CHAP
CHAP (Challenge Handshake Authentication Protocol) is a method of forcing a host to identify itself to a resource to which it is attempting to connect. This is carried out using hash algorithms and creating unique sets of identifiers that the connecting node must supply to be authenticated for a session. CHAP is now an obsolete standard and was used primarily by PPP. The newer standard in use is MS-CHAP (Microsoft CHAP). MS-CHAP currently comes in versions 1 and 2 (MS-CHAPv1; MS-CHAPv2). It uses the same basic concept, but takes it a step further by requiring the proof of identity to be performed by both sides of the connection. This helps to ensure a remote node is not compromised by establishing a connection to a false resource. MS-CHAP can also be used with RADIUS for dial-in and VPN clients.

EAP
Extensible Authentication Protocol (EAP) is a security framework that acts as an extension of the security procedures already in place. It is not a protocol in the same way that TCP/IP is, for instance. Rather it is a set of rules for formatting the security messages. Each protocol that uses EAP encapsulates the EAP information within its own packets, using its own method. EAP works with many protocols and is considered to add another layer of security.

6.5 Explain issues that affect device security

Physical security

Physical security is an integral part of any comprehensive security policy. In cases where data is highly sensitive or classified, actual physical access to the storage media, servers, clients and various pieces of hardware that connect to a network must be monitored and secured.

Physical security can come in many forms. It starts with restricting physical access to sensitive areas or devices. This could be security gates, keycard or biometrically controlled locks and surveillance equipment. Once inside the sensitive area, another layer of security can be implemented in the form of things such as locked server racks, floppy-less workstations or biometrically controlled access.

There is no one key answer to security and it is often said by professionals that access may be close to impossible, but must always be treated as if the resources are still vulnerable. In the end, it is due diligence, understanding the threats and continued perseverance that are the best methods to create a secure physical environment.

Restricting local and remote access

As mentioned in the previous section, devices must be physically secured as well as logically secured. When securing against unauthorized local access there are really two concerns. First, physical console access to a device must be addressed as previously mentioned. Also, local logical access must be secured. This includes both physical access to connect any type of interface cable or hardware to the device as well as the internal logical security, such as username/password requirements and data tokens (e.g. digital certificates).

Securing remote access is primarily a logical implementation, but has some concerns regarding physical access. For example, easily accessible backbone cabling could be a potential physical risk. Another popular type of physical remote security is the use of hardware tokens. These are often keychain type devices that must inserted into a USB port in order for a connection to be made when a user attempts to logon remotely. These can also come in PC Card form, though the key fob design is by far the most popular. Logically, there are many methods to securing device access. These include, but are not limited to VPNs, digital certificate requirements, use of encryption and implementation of strict security designs, such as those based upon IPSec.

Secure methods vs. unsecure methods

Secure methods typically involve the use of encryption to protect the transmitted data and high level authentication to protect from unwanted access. Methods that are considered to be unsecure typically have few authentication requirements and usually transmit data in clear text.

Unsecure methods create a problematic landscape to which security technicians and administrators must constantly attend. In cases where the level of sensitivity of the data is very low, unsecure methods are often used, When the network is a mixed bag of public and highly sensitive data, however, areas that do not employ more secure methods can be a risk to allow access to more sensitive areas. This must be taken into consideration when designing the security infrastructure.

Secure methods provide a level of integrity to the network operation, but can never be said to be perfect and impenetrable. By requiring encrypted data and strong authentication, logical security can be maintained with a much higher rate of success. Physical access control must be a part of any secure methodology as well. This includes properly training staff in addition to locking down access to the devices and network.

NOTE: In regards to logical methods, the following protocols are some, but not all, that are considered to be secure: SSH, HTTPS, SNMPv3, SFTP and SCP. These protocols, among others, are considered to be unsecure: TELNET, HTTP, FTP, RSH, RCP and SNMPv1/2.

6.6 Identify common security threats and mitigation techniques

Security threats:

DoS

Denial of service (DoS) attacks involve rendering a network or resource unusable by saturating it with traffic. A Distributed denial of service (DDoS) is the same basic thing but employs a larger number of hosts in the attack. There are many ways a DoS attack can be manifested. Attackers can deny service to individual victims or they may overload the capabilities of a machine or network and block all users altogether. These types of attack are very hard to prevent and stop while occurring because the behavior of the entire network must be analyzed.

Viruses

Viruses are among the most common type of attack. These are pieces of malicious code designed to infect and impede normal operations in applications and ultimately the network. They come in many forms and levels of complexity and can be easily passed from host to host when undetected. They attach themselves to applications and replicate using the processes of the application typically.

Worms

Worms are pieces of malicious code that insert themselves into a system and carry out various forms of attack against the system. They differ from a virus in that they are self replicating and can distribute themselves through the system without the help of a host. They also run independently of other applications, whereas viruses attach themselves to other applications.

Attackers

Attackers are people with malicious intent. These were usually called hackers in the past. The term hacker has come to mean a person that can break through a system's security. With the advent of ethical hackers, the term no longer immediately has negative connotations. Basically a hacker with harmful intentions is an Attacker.

Man in the middle
A man in the middle attack involves intercepting electronic messages in a public key exchange, then retransmitting them by substituting a false public key for the requested one. In this scenario, the attacker must fool each side of the connection that they are indeed the trusted party. These are also sometimes called bucket brigade or Janus attacks.

Smurf
Smurf attack is a form of denial of service attack which makes use of spoofed IP broadcast ping messages for flooding a target system. Simply put, it disables a system through bandwidth consumption.

Rogue access points
A rogue access point is a Wi-Fi access point which has been installed into a secure network without authorization. This allows an attacker access to a LAN without having to first beat the perimeter security. A typical use for one is to carry out a man in the middle attack.

Social engineering (phishing)
Social engineering is the act of manipulating a human into providing access or sensitive information that allow a hacker to carry out an attack or gain information or access. There are several types of social engineering. The most common is phishing. This usually involves email or a website that is disguised as a legitimate correspondence or site. The end user is asked to provide some type of private or personal information that is in turned used to perform the malicious acts. False emails from a trusted sender are the most common type of phishing and are often involved in identity theft. A hoax is another type of social engineering that involves convincing an end user that a false scenario is real. A good example of this is overseas fake lottery and money transfer scams. Keep in mind that while these types of attacks are typically seen in general public emails and areas, the techniques they employ to derive sensitive information can be applied to a business network setting as well.

Mitigation techniques:

Policies and procedures
The first step in mitigating the multitude of possible network attacks is good, sound security policies. The companion to strong policies is strong procedures for dealing with an attack in progress and the aftermath. By defining these sets of rules, this allows the team that deals with attacks to function more efficiently and to know all hands are on the same page during critical times.

A good policy to implement is classification of corporate information based on business risk, data value, or other criteria. This makes determination of which security measures should be implemented to protect the various types of data. Redundancy of data and servers is also very helpful in ensuring that resources are still available during an attack. One method is to reserve a private set of IP addresses and hardware devices that are not exposed to the network usually and can be quickly implemented in the event of availability loss.

Preventing attacks is difficult and may not meet with 100% success, even if all possible measures are taken. Security policies regarding things such as password complexity will help, especially with DoS attacks. Typically, a combination of several types of defenses along with diligent monitoring for attacks is the best policy.

In addition to security involving the network hardware and software, policies and procedures should also include rules for personnel. This includes defining classes of employees and to which data classes they have access. In organizations that have highly sensitive information to protect, the hiring process should also be affected by these policies. An example of this would be strict background checking for perspective new hires.

It only makes sense to have policies and procedures that define security for a network. Without these protocols attempting to deal with security issues and their implications would be disorganized and most likely ill fated. It could be said that not having a good set of policies is a security risk in and of itself.
.

User training

User training is very valuable in terms of mitigating attacks, especially social engineering. User training is not limited to end users only. Making sure the network team and administrators understand the threats and how to handle them is key to a successful infrastructure and its availability. Additionally, educating users on the way that attacks are carried can be very helpful in the users not allowing themselves to be utilized in an attack.

Patches and updates

Patches fix specific issues in a software product or operating system. Updates are basically the same thing, but usually involve a set or sets of patches. Patches and updates must be managed, however, as they can also be disguised and used to attack a system. Additionally they can cause problems within a system or network if not properly applied and tested. Typically an administrator has approved groups of users that are allowed to apply patches or updates. Patch and update management is especially important with antivirus software. By installing on all connected nodes and keeping the virus definitions up to date, most viruses can be mitigated.

NOTE: Patch and update application must be done in a consistent manner. Failing to patch even a few computers leaves the overall network vulnerable. Again, patches and updates should be thoroughly tested before deployment into the live environment.