EXAM N10-004

Network+

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.

PrepLogic

Be Prepared. Be Confident. Get Certified.

PrepLogic, Inc. • 1300 N. Westshore Boulevard, Suite # 125 • Tampa, Florida 33607
Phone: (813) 769-0920 (800) 418-6789 • Fax: (813) 769-0926 • Website: www.preplogic.com

Network+ (N10-004) Mega Guide

Copyright © 2010 by PrepLogic, LLC.
Product ID: 012040
Production Date: July 20, 2010

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

PrepLogic offers favorable discounts on all products when ordered in quantity. For more information, please contact PrepLogic directly:

1-800-418-6789
solutions@preplogic.com

International Contact Information

International: +1 (813) 769-0920

Australia: (02) 8003 3878

South Africa: (0) 11 083 9973

United Kingdom: (0) 20 8816 8036

Table of Contents

1.0 Network Technologies

1.1 Explain the Function of Common Networking Protocols

TCP

Transmission Control Protocol (TCP), a Transport layer protocol, is a host-to-host, connection-oriented protocol. It enables two hosts to establish a connection and exchange network data. Unlike IP, TCP guarantees data packet delivery and reassembles packets back into the same order in which they were sent.

TCP's connection-oriented properties set it apart from similar protocols, such as UDP (covered next). TCP provides error detection and recovery, flow control, and guaranteed, reliable delivery of data. Network applications that require reliable, guaranteed, error-free delivery use TCP. But TCP does this at a price. The TCP header contains 20 bytes, which means it has more overhead than UDP. Because it has more overhead, it's slower than UDP. To choose between TCP and UDP, decide whether you want speed (UDP) or reliability (TCP).

FTP

The File Transfer Protocol (FTP) is an Application layer protocol that allows a user to upload or download files between hosts. FTP is the simplest way to exchange files between computers on the Internet, and is used on the Web to download files. It's often compared to HTTP, which transfers Web pages, and to SMTP, which transfers e-mail.

FTP operates as a protocol when used by applications. However, FTP also can operate as a program. Users can use FTP to access directories and files and to perform directory operations such as relocating directories or files. FTP is limited to listing and manipulating directories, typing file contents, and transferring files between computers. FTP cannot execute remote files as programs. When paired with Telnet, FTP allows for seamless login to an FTP server for file transfers. FTP also offers authentication security.

UDP

User Datagram Protocol (UDP), also a Transport layer protocol, is a streamlined, economy class version of TCP, earning it the nickname "thin protocol," which means it doesn't take up much bandwidth on the network. UDP is a connectionless, unreliable, low overhead protocol but is faster than TCP. UDP doesn't offer the assurances of TCP, but does do a very good job of getting data from one host to another using lower bandwidth and fewer network resources to do so. It's a good choice to use if guaranteed delivery is not required. UDP is also used when it is paired with a service, such as Network File System (NFS), that contains its own reliability checks. You, for example, would choose UDP for transport for applications such as streaming audio and video. If a packet here or there is lost, by the time TCP retransmitted, it is a moot point.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is used by devices to request an IP address and local network configuration parameters. These most common parameters include an IP address, default gateway, and the DNS server IP address(es). If there is no DHCP server in a network, devices are typically statically configured with this information.

TFTP

Trivial File Transfer Protocol (TFTP) is also similar to FTP in that it facilitates file transfer between computers. The difference between FTP and TFTP is speed. FTP uses TCP, which is reliable but has high overhead, and TFTP uses UDP, which uses much less bandwidth, offering greater speeds but less reliably.

TFTP is a more primitive, simpler version of FTP. TFTP only transfers files. It does not allow the user to browse files in a directory, and there is no security for authentication. TFTP is the protocol of choice for users who know the file location and exactly what files they want. Because TFTP lacks security, it is seldom-used by users. It is, however, used in other applications by system administrators for activities such as downloading a new Internetwork Operating System (IOS) to a Cisco Router.

DNS

The Domain Name Service (DNS) translates and resolves IP addresses into host names or the reverse: resolves host names to IP addresses.

HTTP(S)

Hypertext Transfer Protocol (HTTP) is a control protocol used on the Web to transfer files from a Web server or client PC to a Web browser. When you select a URL, HTTP is the protocol that opens a Web page, no matter where that document is located. HTTP resides in the Application layer of the OSI model, uses little bandwidth, and supports the use of both text and graphics

Hypertext Transfer Protocol Secure (HTTPS) is the secure version of HTTP. HTTPS was developed by Netscape using Netscape's implementation of SSL. HTTPS offers secure message-oriented communications and is designed for use with HTTP. HTTPS allows browsers and servers to sign, authenticate, and encrypt an HTTP network packet. HTTPS uses the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols for security. If you use Internet Explorer as your Web browser and a gold colored lock appears at the bottom of the Web page, you are visiting a secure Web site. If you use Firefox, the address field containing the URL is white with a yellow background. Also, Secure Web sites are also identified by a URL that begins with https:// instead of http://.

ARP

Address Resolution Protocol (ARP) is a Network layer protocol that resolves network (IP) addresses into hardware (MAC) addresses. ARP uses the address resolution cache table built into every network interface card (NIC). This table maps IP addresses to MAC addresses on the network. Whenever a node needs to send a packet, it checks the address resolution cache table to see if the MAC address information for the destination is there. If so, that destination address will be used. If not, an ARP broadcast request is issued. ARP is built into most network operating systems such as Windows, UNIX, and Novell and is executed at a command prompt.

Reverse Address Resolution Protocol (RARP) uses a host MAC address to discover its IP address. The host broadcasts its MAC physical address and a RARP server replies with the host's IP address.

SIP (VoIP)

The Session Initiation Protocol (SIP) is a VoIP call control protocol which is rising in popularity. SIP takes advantage of already used Internet schema; this is because SIP uses a URL to address a specific endpoint (i.e. sip:test@user.com). SIP supports not only VoIP services but also Video over IP, instant messaging and presence.

RTP (VoIP)

The Real-Time Transport Protocol (RTP) is used by most VoIP signaling protocols to transport voice traffic between endpoints. RTP uses UDP to transport this traffic but adds both time-stamping and packet sequencing which do not exist within UDP.

SSH

Secure Shell (SSH) is an application program used to log into another computer on a network, execute commands, and transfer files back and forth. SSH offers secure data transfers as compared to using rlogin, telnet or FTP. Actually, SSH is a suite of protocols; slogin, ssh and scp and requires that the server and client are both running SSH software. It uses strong authentication methods and secure communications. Because the entire session is encrypted, SSH protects against network attacks. SSH use the RSA public-key encryption technology authentication method and can be used on Windows, UNIX, and Mac computers.

POP3

Post Office Protocol version 3 (POP3) is an Application layer protocol used to retrieve e-mail files from an e-mail server. Whenever you connect to a POP3 e-mail server, all messages addressed to your e-mail address are downloaded into your e-mail application. Once e-mail files are downloaded, you can view, modify, and/or delete the messages without further assistance from the POP3 server. POP3 can be used with or without Simple Mail Transfer Protocol (SMTP).

NTP

Network Time Protocol (NTP) is an Internet standard application protocol that sets computer clocks to a standard time source, usually a nuclear clock maintained by the U.S. Naval Observatory Master Clocks. An NTP designated server on a LAN is often deployed to periodically connect to an NTP server on the Internet, assuring accurate synchronization of the LAN NTP server's time clock down to the millisecond. The LAN NTP server then checks and, if necessary, adjusts, all other servers and client computers time clocks assuring accurate time and date stamping of client files.

IMAP4

Internet Message Access Protocol version 4 (IMAP4) is similar to POP3, but supports additional features. IMAP4 allows you to download e-mail, look at or download the message header, store messages in hierarchical structure, and link to documents and Usenet newsgroups. It also provides search commands that allow you to locate messages based on their subject, header, or content. IMAP4 also allows users to manipulate their e-mail and e-mail folders while disconnected from their main messaging system and to synchronize to their message store once the connection is reestablished. IMAP4 also contains authentication components, which support the Kerberos authentication method.

Telnet

Telnet stands for Telephone Network, so called because most Telnet sessions occur over a dial-up network. Telnet is a terminal emulation program often used to connect a remote computer to a Web server but can connect to any kind of server. Once the connection is established, you enter and execute commands using a command prompt. Telnet depends on TCP for transport services and reliable delivery. To start a Telnet session using a Telnet client, you must log onto a Telnet server by entering a valid user name and password.

SMTP

As its name implies, SMTP is used to send e-mail. One thing to remember is how SMTP compares with POP3, which can be used with or without SMTP. SMTP sends e-mail whereas POP3 receives e-mail.

SMTP uses the spooled, or queued, method to deliver e-mail. An e-mail is sent to a destination and is spooled to a hard disk drive. The destination e-mail server regularly checks the spooled e-mail queue for new e-mails, and when it finds new e-mails, forwards or sends them to their destinations.

Most Internet-based e-mail services use SMTP to send e-mails along with either POP3 or IMAP to receive e-mails. SMTP is generally used to send messages between mail servers. This is why you need to specify both the POP3 and the SMTP server IP addresses when you configure your e-mail application.

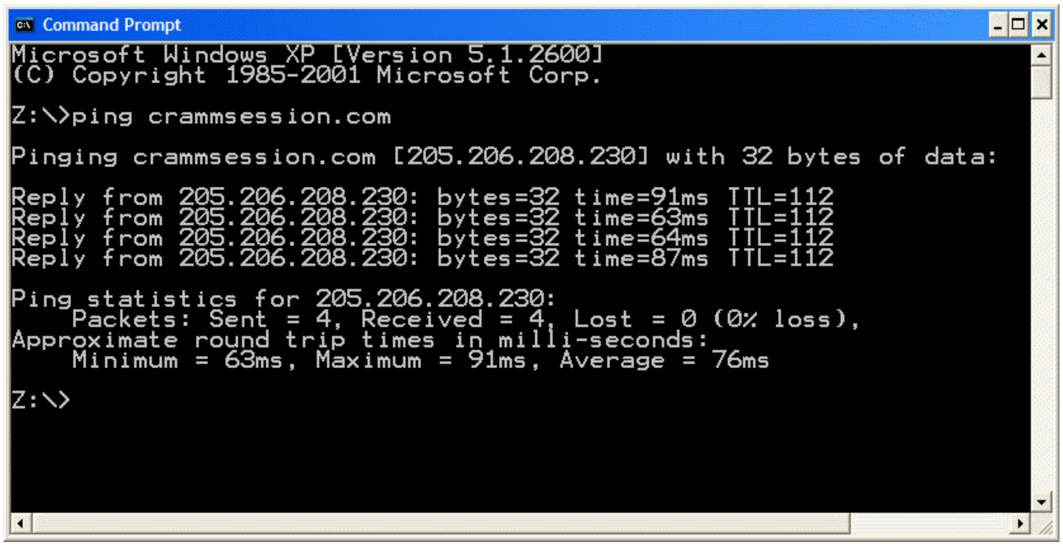
SNMP2/3

Simple Network Management Protocol version 2 and 3 (SNMP2/3) monitors the network and network devices. SNMP sends messages to different parts of a network. SNMP agents store and return data to the SNMP requesters. It uses Management Information [Data] Bases (MIB) to define what information is available from a managed network device.

ICMP

Internet Control Message Protocol (ICMP) works with IP at Layer 3 to provide Network layer management and control. Routers send ICMP control messages in response to undeliverable datagram's. The receiving router places an ICMP message into an IP datagram and sends the datagram back to the source.

ICMP provides feedback about network connectivity problems and the processing of datagram's but does not guarantee reliable delivery. ICMP is built into most network operating systems such as Windows, UNIX, and Novell, and can use packets containing error control. The ping command, for example, uses ICMP to test an Internet connection. When you ping a network device with an IP address, the ICMP part of that host's TCP/IP stack responds to the request.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\>ping crammsession.com

Pinging crammsession.com [205.206.208.230] with 32 bytes of data:

Reply from 205.206.208.230: bytes=32 time=91ms TTL=112
Reply from 205.206.208.230: bytes=32 time=63ms TTL=112
Reply from 205.206.208.230: bytes=32 time=64ms TTL=112
Reply from 205.206.208.230: bytes=32 time=87ms TTL=112

Ping statistics for 205.206.208.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 91ms, Average = 76ms

Z:\>
```

Figure 1 - Ping Command Results

IGMP

Internet Group Management Protocol (IGMP) is a Network layer protocol that is used by an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows an Internet computer to send content to multiple computers. Multicasting is used to send out company newsletters to an e-mail distribution list, and to broadcast high-bandwidth programs using streaming media to a multicast group membership audience.

TLS

Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL) (HTTPS) in providing a secure method for transferring data from server to client. TLS works in a basically similar manner to SSL and supports several different encryption options.

1.2 Identify Commonly Used TCP and UDP Default Ports

Port Number	Services and Protocols	Transport Protocol	Function
20	FTP	TCP	Transfers FTP data when in active mode
21	FTP	TCP	Provides flow control and FTP signaling
22	SSH	TCP	Executes commands and moves files (Remote login protocol)
23	Telnet	TCP	Connects a remote computer to a server
25	SMTP	TCP	Delivers e-mail between e-mail servers
53	DNS	TCP/UDP	Translates host names into IP addresses
67	DHCP	UDP	Listens for DHCP address requests
68	DHCP	UDP	Responds to DHCP address requests
69	TFTP	UDP	Transfers data (simple FTP)
80	HTTP	TCP	Opens a browser connection to a Web page
110	POP3	TCP	Delivers e-mail between a mail server and client
119	NNTP	TCP	Views and writes news articles for various newsgroups
123	NTP	UDP	Sets computer clocks to a standard time
143	IMAP4	TCP	Downloads e-mail or e-mail headers; stores, searches messages from newsgroups
161	SNMP	TCP/UDP	Used to manage configured SNMP devices
443	HTTPS	TCP	Allows browsers and servers to sign, authenticate, and encrypt HTTP network packets (uses SSL)

Table 1 - Commonly used TCP/UDP ports

1.3 Identify the Following Address Formats

IPv6

The 32-bit Internet Protocol version 4 (IPv4) addressing scheme can only produce about 3.7 billion unique IP addresses. With the increasing popularity and use of the Internet and World Wide Web, it soon became apparent that the number of available IPv4 addresses would not be enough. Based on Classless Inter-Domain Routing (CIDR), IPv6 was standardized in 1994 to overcome these limitations and is beginning to be implemented.

An IPv6 address looks very different from an IPv4 address. IPv6 uses a 128-bit addressing scheme that can produce 79 octillion IP addresses! IPv6 uses eight octet sets of four hexadecimal digits. IPv6 is backward compatible with the older IPv4, allowing for gradual upgrades. It is designed to run well on high speed Gigabit Ethernet networks while still providing efficiencies for low bandwidth networks, such as wireless networks. The 128-bit IPv6 address is divided into eight 16-bit hexadecimal numbers separated by colons (":"). The format is represented by xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, If part of the address is expressed as :0000: or several sets of zeros, the "shorthand" version will look like this:

2342:0000:1F1F:0100:0010:0100:11B0:AFFF

The first 64 bits are used for the network prefix whereas the last 64 bits are used to identify the interface ID, which is the host. The first 24-bits in the interface ID represent the company ID, and the last 40 bits represent the extension ID that creates a larger address space for the NIC manufacturer to use. Another key difference between IPv4 and IPv6 addressing is in the way IPv6 configures hosts. Instead of an IP address, subnet mask, and default gateway that IPv4 uses, each node on an IPv6 network is required to have three different addresses. The host receives an address from the upstream supplier, a local address, and a link local address.

IPv4

TCP/IP networks use IP addressing to identify computers and other networking devices. Networks using the TCP/IP protocol route messages based on the IP address of the destination device. IPv4 employs a 32-bit addressing scheme. IPv4 uses four 8-bit binary coded numbers written in decimal dot notation. In an IPv4 address, each byte, or octet, uses a number that ranges from 0 to 255. Each eight-bit decimal octet contains a decimal value based on its position. For example; 192.168.10.235 represents an IP address on a private network.

Using a private LAN, you can assign random IP addresses as long as each one is unique and as long as each IP address is on the same subnet. Connecting a private network to the Internet, however, requires using a unique, registered IP address to avoid identical IP addresses that would result in unreliable communications. The number of unique, unassigned IPv4 addresses is presently in short supply. A new classless scheme called Classless Inter-Domain Routing (CIDR) is gradually replacing the out-dated (see section 2.6 below) IPv4 addressing system. It is called IPv6.

MAC Addressing

Media Access Control (MAC) addresses are given to every Ethernet interface at the factory and all publically conform to a six octet address (MAC-48). These addresses are identified by splitting the address into two parts with three octets each. The first three octets are used to signify the Organizationally Unique Identifier (OUI) which is assigned to each hardware vender. The second set of three octets is Network Interface Controller (NIC) specific and is given by the originating vendor. There are two main ways these addresses are written. The most common is using the colon (:) between each octet (01:23:45:67:89:00) and the second groups the address into three sections of two octets each separated by a period (0123.4567.8900). In these examples the 01:23:45 is the OUI and the 67:89:00 is the NIC specific identifier.

1.4 Given a Scenario, Evaluate the Proper use of the Following Addressing Technologies and Addressing Schemes

Addressing Technologies

The class of the network determines how many networks and hosts (computers) you can have. The four numbers, or octets as they are commonly called, in an IPv4 address are used in different ways to identify a particular network and a host. In general, higher order bits (left most) bits make up the network portion of the IP address whereas lower order (right most) bits make up the host portion. The host portion can be further divided into subnets. In the following example, the network portion of the IP address is red color and the host portion is blue:

172.143.36.248

Examining this IPv4 address reveals that it is a Class B address. You know this because the first octet, 172, falls within the Class B range of 128 to 191. Class A addresses have a first octet range of 1 to 126 whereas Class C addresses have a range of 192 to 223. Anything greater than 223 is reserved. In the preceding example, the first two octets, in red, are the network portion of the address. The last two octets make up the host portion. Internet addresses—address ranges and supported hosts and networks—are assigned from the following three classes.

- **Class A** - 1.0.0.0 to 126.255.255.255 - supports 16,777,214 million hosts on each of 126 networks
- **Class B** - 128.0.0.1 to 191.255.255.255 - supports 65,534 hosts on each of 16,000 networks
- **Class C** -192.0.0.0 to 223.255.255.255 - supports 254 hosts on each of 2 million networks

Routers use subnet masks to determine and separate (mask) the network and host portions of the IP address. There also is a class D address range, which is used for Multicast and a Class E address range that is experimental.

Class A networks have a binary value of zero and a decimal number from 1 to 126. The first eight bits represent the network portion of the subnet mask ID whereas the remaining 24 bits represent the host portion of the subnet mask ID. Class A networks use the following subnet mask: 255.0.0.0 where 255 represents the network ID and 0.0.0 the host. Represented as binary, a Class A address is 11111111.00000000.0000000.00000000.

Class B networks have a binary value of 10 and a decimal number from 128 to 191. Class B networks use the first 16 bits to represent the network ID and the last 16 bits represent the host. Class B networks use the following subnet mask: 255.255.0.0; where 255.255 represents the network ID and 0.0 the host. Represented as binary, a Class B address is 11111111.11111111.0000000.00000000.

Class C networks have a binary value of 110, and therefore decimal numbers from 192 to 223. Class C networks use the first 24 bits for the network ID and the remaining 8 bits for the host. Class C networks use the following subnet mask: 255.255.255.0; where 255.255.255 represents the network ID and.0 the host. Represented as binary, a Class C address is 11111111. 11111111.11111111.00000000.

Note that 127.0.0.0 represents a loop back address and is reserved. Also network address 0 is reserved for routers and the network address 255.255.255.255 is used to broadcast network signals. Another way classful networks can be identified is total bits for network versus host, as follows:

- **Class A** - 8/24 = 8 bits network and 24 bits host
- **Class B** - 16/16 = 16 bits network and 16 bits host
- **Class C** - 24/8 = 24 bits network and 8 bits host

Subnetting

Subnetting is the process of subdividing an assigned IP address into smaller networks or subnets. For example, let's assume that you need to isolate several individual networks within a company's IP address space by department or branch offices. If you are assigned one IP address only, you could use subnetting to connect five networks to the Internet. To continue this example, you are assigned 224.151.131.89 for your only IP Public address with a subnet mask of 255.255.255.0. Because this is a Class C address and only the last octet represents the host portion, you can only change the last octet by borrowing bits from the host ID. The following formula is used to calculate the number of available subnets:

- 2 to the x power minus 2 = the number of available subnets, where x = the number of bits used from the node portion of the IP address to make subnets.

In the example, because you want five networks, you take three bits from the last octet to use for subnets by using the following formula:

- 2 to the third power minus two = six subnets (more than enough)

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

The difference between Classful and Classless is most used when differentiating IP routing protocols. A classful routing protocol is limited to only using the major class boundaries. If a protocol is classful it cannot support subnetting or supernetting. A classless routing protocol is able to use any legal bit boundary within the IP Address. If a protocol is classless it CAN support subnetting and supernetting.

Classless Inter-Domain Routing (CIDR) or supernetting is a method for joining together a number of networks into one large routing table entry. CIDR uses a notation which signifies at which bit number this joining starts. For example, if you wanted to join together two class C networks (192.168.2.0 and 192.168.3.0) this could be done by advertising a summary of 192.168.2.0 with a mask of 255.255.254.0. This would be notated by CIDR by using /23 signifying a summary starting at the 23rd bit. Using /23 you would summarize 192.168.0.0 through 192.168.1.255, 192.168.2.0 through 192.168.3.255, 192.168.4.0 through 192.168.5.255 and so on.

NAT/PAT

Network Address Translation (NAT) was created as a solution to both protect the inside of a network and to provide a solution which will enable the use of limited public IP addresses for multiple internal (private) IP addresses. NAT enables the ability to have only a few public IP addresses which map internally to a network to private addresses. This mapping can be done on a one-to-one basis (NAT) as well a one-to-many basis (PAT). For example, a network can use 128.118.50.0 network as an outside address range (which is public) and have all internal machines addressed using the 192.168.1.0 network. NAT provides a translation that will map traffic coming from an inside address (192.168.1.50) to an outside address (128.118.50.5). All public devices would see the traffic as coming from the public IP of 128.118.50.5 but the traffic is translated for use on the internal network to 192.168.1.50.

Port Address Translation (or overloading) takes NAT to the next level by allowing the mapping of a limited number of public IP addresses to many internal private addresses. This is done by not only mapping the public IP address to the internal private IP address but also assigns a specific port number for all requests coming from a specific internal IP address. For example, most people's home internet connection works by providing one public IP address which is then translated by the router/gateway (think Linksys). What this does is it allows a number of internal devices to use only one public address. This device keeps track of each internal device by sending out traffic publically on a specific source port number which is tracked by the router. All traffic coming back to the router from a public server will return to that specific port number which allows the router to differentiate between the traffic for each individual internal device.

SNAT

Static Network Address Translation (SNAT) simply allows a user to configure a static translation between a public IP address and a private internal IP address. For example, a user could statically configure an external IP address of 128.118.1.50 to always be translated to an internal IP address of 192.168.1.100.

Public vs. Private

The difference between a public and private network is a public network, such as the Internet, sits in front of a firewall and does not offer protection. Private IP addresses are not publically routable. A private network sits behind the firewall, and offers protection from malicious attacks from the Internet. The gateway router will discard any packets with a private source address into the bit bucket. So, you need to be sure to install your firewall on the outer edge of your network to protect your private Intranet. Private networks have a Class A, Class B, or Class C range of private addresses that are non-routable and therefore excluded from the Internet. They are as follows:

- **Class A** - Private address range: 10.0.0.1 to 10.255.255.254
- **Class B** - Private address range: 172.16.0.1 to 172.31.255.254
- **Class C** - Private address range: 192.168.0.1 to 192.168.0.254

With the shortage of available "classful" IP address ranges, CIDR is used extensively for public IP addressing so that entire blocks of IP addresses do not have to be purchased when you just need a few. All of the other Class A, Class B, and Class C addresses are public, routable, IP addresses and are assigned to companies through the InterNic authority or a company that the InterNic authority appoints to sell registered IP addresses.

DHCP (static, dynamic APIPA)

- **Static** - An IP address, subnet mask, DNS, and gateway address that is manually configured in the TCP/IP configuration options on client operating systems. Static IP addresses are usually assigned to *shared* network devices such as servers and printers. All modern NOS servers using TCP/IP are manually configurable.
- **Dynamic** - An IP address that is automatically assigned to network clients from a pool of addresses residing on a Dynamic Host Configuration Protocol (DHCP) server. DHCP servers reduce administrative efforts by eliminating the tedious task of manually setting IP address information on clients. DHCP servers can also automatically assign other IP address information, such as the default gateway and DNS server IP addresses.
- **Self-assigned** - Automatic Private Internet Protocol Addressing (APIPA) is used by Windows 2000 and Windows XP NOSs when a client is unable to obtain an IP address automatically from a DHCP server APIPA automatically configures itself with an IP address using a range of addresses from 169.254.0.1 to 169.254.255.254. Since this is a Class B address, the APIPA client also configures itself with a default Class B subnet mask of 255.255.0.0. An APIPA client uses the self-configured IP address and can communicate to other APIPA clients until a DHCP server becomes available. Peer-to-Peer networks can also use APIPA effectively to communicate and share network resources without the aid of a DHCP server.

Addressing Schemes

Unicast

Unicast transmission is what is used by most users of the Internet. It is simply the transmission from one single address to another single address. Most normal Internet protocols use unicast as the intended receiver is only a single device. For example, if you opened a web browser and went to google.com the resulting page would only need to be sent to your machine and not a group of machines.

Multicast

Multicast transmission is used when a single transmission is intended to be sent to multiple parties at the same time. This of course could also be done via unicast but the server would need to setup communications which each endpoint individually which takes allot of resources. When using multicast the server sends out one transmission which is sent to a specific multicast address, all receivers who want to listen only listen to that specific address. Un-interested parties simply don't listen to that port so then don't receive the transmission.

Broadcast

Broadcast transmission sends the traffic to all devices on a specific network. Typical IP broadcasts are limited to the local network segment and do not pass over layer 3 boundaries (router).

1.5 Identify Common IPv4 and IPv6 Routing Protocols

Link State

A link state routing protocol gathers information about the cost or metric of a specific path through a network. When making a path selection these costs are added for the length of the proposed path and the decision is based on the lowest cost. Link state protocols also typically send partial updates as the network topology changes. Link state protocols are more complex than distance vector protocols because each device needs to be aware of the complete topology of the network to make routing decisions. Link-state protocols calculate the cost based on the information in the topology table.

OSPF

Open Shortest Path First (OSPF) is one of the most common link state protocols which are run on networks today. It provides classless IP support and supports complex hieratical configurations allowing it to scale to very large networks. OSPF does this by grouping together parts of the network into areas. All OSPF networks must have at least a backbone area number 0 which is meant to be the center of the network. All areas created must have a direct connection to the backbone area. OSPF metric mechanism by default calculates the cost of a specific network link by dividing 100,000,000 by the bandwidth of the link. This calculation is then put into the OSPF database and the path with the lowest cost is advertised into the routing table. The lowest cost of a specific path is calculated using the Shortest Path First algorithm which is also known as Dijkstra's algorithm.

IS-IS

Intermediate System – Intermediate System (IS-IS) as a protocol is very similar to OSPF. They both use the same SPF algorithm for path selection and are designed to scale well to large networks. IS-IS does not however use areas in the same way as OSPF. IS-IS separates a network using L1 areas; each of the devices in a L1 area can only speak to other devices in that L1 area. L2 devices are used to communicate between L1 areas. Typically, a specific device(s) is specified as being a L1 and a L2 device and is used as a gateway between different L1 areas.

IS-IS is an advantage over OSPF because it does not send traffic between devices using IP. IS-IS uses the Connectionless Network Service (CLNS) which allows IS-IS to support multiple routing protocols (i.e. IP and IPv6) at the same time.

Distance Vector

Distance vector protocols are much simpler than link-state protocols. Each distance vector device sends out their view of the network and what networks they can reach. This information is sent typically in complete updates to all other distance vector devices. Each distance vector device does not need to be aware of the topology of the network; distance is assumed correct coming from their neighbors. The metric or cost used by distance vector protocols is not calculated by every router it is figured on the advertising router and advertised.

RIP

Routing Information Protocol (RIP) is the oldest of the modern routing protocols and is not typically used on any network outside of testing situations. RIP sees the network in terms of hops; a specific destination is routed based on the lowest number of hops to get there. RIP is limited to a total of 15 hops. RIP is also a classful routing protocol meaning it is not able to support subnetted networks; this is because RIP updates do not include mask information.

RIPv2

RIP version 2 is basically the same as RIP version 1 except that it has a couple of main additions. RIP version 2 is a classless routing protocol and does support subnetted networks. It also makes use of multicast for communication between RIPv2 devices instead of using broadcast which was used with version 1. RIP version 2 also has support for authentication which was not supported in version 1.

BGP

Border Gateway Protocol is used as an External Gateway Protocol to bridge between various Internet Gateway Protocols. The most common implementation of BGP is the Internet. All traffic which goes over the Internet is routed by BGP, this is typically done only between the various larger carriers (AT&T, Verizon…) but companies also have the ability to connect via BGP to the public internet to make better routing decisions.

Hybrid

EIGRP

EIGRP is considered to be a hybrid protocol because it has traits of both distance vector and link-state protocols. EIGRP does not send link-state updates but passes distance-vector type updates which include the reachability information of each router and the cost from each router. This information is then used to calculate the cost of the end-to-end path. Updates are only sent when EIGRP is starting up and when topology changes occur. EIGRP is also classless and has native support for both IP and IPv6. EIGRP's only main downside is that it is Cisco proprietary.

1.6 Explain the Purpose and Properties of Routing

IGP vs. EGP

An Internal Gateway Protocol (IGP) is intended to be used for routing inside a single autonomous system. An autonomous system is typically limited to the inside of one company or carrier. An External Gateway Protocol (EGP) is intended to be used for routing between autonomous systems. Most of the commonly known routing protocols are IGP's: OSPF, IS-IS, EIGRP, RIP. While the most used EGP is eBGP,

Static vs. Dynamic

When statically routing a network all reachable destinations must be specified within one of the routing entries or the path will not be reachable. Static routes are typically used on branch routers where there is only one main connection to other parts of the network. Dynamic routing is what routing protocols are used for. With dynamic routing the routing protocols devices communicate between each other and find all the reachable destinations.

Next Hop

The next-hop is the next IP hop (or routing device) which is closer to the destination.

Understanding Routing Tables and How They Pertain to Path Selection

The routing table is a list of all the reachable networks and the current cost or metric which is given by the specific routing protocol. Routes which are put into the routing table are the selected on a most specific basis. Meaning the routing entry that best matches the destination network will be matched, if a summary exists of a whole network and a route exists for a specific network inside that network the route for the more specific network will be used.

Explain Convergence (steady state)

Convergence is a state where all of the peers within a routing protocol have been synchronized between each other with the most up to date information. For example, when RIP is converged that means that all of the reachable networks within the scope of the RIP domain have been communicated to all RIP routers. With OSPF this means that the link state of all the links within a network have been communicated between OSPF routers.

1.7 Compare the Characteristics of Wireless Communication Standards

802.11 a/b/g/n

	802.11a	**802.11b**	**802.11g**	**802.11n**
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4 & 5 GHz
Channels	12	11	11	12
Non-Overlapping Channels (20 MHz)	12	3	3	3 (2.4 GHz) & 12 (5 GHz)
Speed	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	1, 2, 5.5 and 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps	6.5 Through 300 Mbps
Distance (Est.)	< 200ft	< 350 ft	< 300 ft	<400 ft (2.4GHz) & < 250ft (5 GHz)
Modulation	OFDM	DSSS	DSSS/OFDM	DSSS/CCK/OFDM

Table 2 - 802.11 a/b/g/n

Authentication and Encryption

WPA

Wi-Fi Protected Access (WPA) adds another layer of security, working with Wi-Fi devices that use Wired Equivalent Privacy (WEP). It offers improved data encryption and user authentication using the wireless devices hardware-specific MAC address as a means of ensuring that only authorized users access the network. The current version WPA2 provides stronger encryption than WPA1 using Advanced Encryption Standard (AES). Both WPA1 and WPA2 use 802.1x and Extensible Authentication Protocol (EAP) for authentication.

The largest security problem with the 802.1x family of wireless technologies is users and consumers not activating their wireless security along with not changing the default password. Although implementing some form of wireless security decreases your speed and overall performance, not doing so leaves your data open to network vulnerabilities and hackers. Both WEP and WPA wireless security should be enabled using the wireless access point software included, usually accessed via a Web browser. You should disable SSID broadcasts and enable MAC address filtering as well. Make sure to also change the default wireless group name along with the default wireless access point browser login password.

WEP

WEP (Wired Equivalent Privacy) is the current 802.11b standard protocol that encrypts and protects data packets over radio frequencies providing a similar level of security as wired Ethernet networks. WEP provides either 64- or 128-bit encryption. WEP does not, however, offer end-to-end security because it uses the lower level layers in the OSI model: the Physical and Data link layers. Because the WEP encryption algorithm is weak, another Wi-Fi standard, WPA was recently developed.

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is used as an authentication and accounting server. RADIUS servers are typically used to store username and password combinations for use with a variety of different services. When used for wireless services RADIUS is typically used in conjunction with 802.11i to authenticated pre-shared wireless keys.

TKIP

The use of the Temporal Key Integrity Protocol (TKIP) was introduced as Wi-Fi Protected Access (WPA). It was designed to be a replacement for WEP; it provided a stronger encryption mechanism and was able to be used on most existing WEP equipment.

2.0 Network Media and Topologies

2.1 Categorize Standard Cable Types and Their Properties

Types

CAT3, CAT5, CAT5e, CAT6

- **Category 3** – Used in 10BASE-T networks and transmits data with speeds of up to 10 Mbps.
- **Category 5** - Used in Fast Ethernet (100BASE-T) networks offering data speeds of up to 100 Mbps.
- **Category 5e** - Used in both Fast Ethernet (for future upgrades) and 1000BASE-T networks running at speeds up to 1 Gbps (1000 Mbps).
- **Category 6** - Transmits speeds of up to 1000 Mbps, and is comprised of four pairs of 24-gauge copper wire.

STP, UTP

Bundled pairs of twisted, insulated copper wire are used for telephone lines and Ethernet computer networks throughout the United States and elsewhere. Twisted-pair media cable carries a signal a maximum distance of 100 meters. Twisted pair cable comes in two types: Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP). STP contains a metal foil sheath to reduce signal degradation, crosstalk, EMI (electromagnetic interference) and RFI (radio frequency interference) and is a better choice than UTP in industrial settings where high-voltage machinery operates. UTP is used to wire Ethernet, Fast Ethernet, and 1000Base-T LANs and is somewhat susceptible to electromagnetic interference and crosstalk. Twisted-pair cabling is the most common type of cabling in use today. Both STP and UTP cable are inexpensive.

Multimode Fiber, Single-mode Fiber

Fiber-optic cable uses pulses of light instead of electrical signals to transmit data. Fiber-optic cable includes a center core containing the glass fibers surrounded by a glass cladding composed of varying layers of reflective glass that refract light back into the core. An outer layer of PVC and inner layers of protective buffer material protect the inner glass core. Using fiber-optic cable, maximum cable lengths of 25 kilometers and data transmission rates are up to 2Gbps are possible. Fiber-optic cable carries laser light encoded with digital signals, and is capable of reliably transmitting billions of bits of data per second. It also offers greater security (much more difficult to tap), emitting no EMI or RFI. Several connectors are used to connect fiber to networking devices. The most common connector used is the SC connector. Fiber's main disadvantage is its expense. The cable itself is more expensive to buy, more expensive to install, and more expensive to maintain.

There are two types of fiber-optic cable:

- **SMF (single mode fiber) -** SMF permits only one mode or wavelength of light to penetrate through the fiber. The central core contains one strand of very pure glass allowing light pulses to travel long distances, up to 50 times more than multimode, making SMF more expensive than MMF. SMF is sometimes used in 1000BASE-LX networks.
- **MMF (multimode fiber) -** MMF permits multiple modes or wavelengths of light to propagate through the fiber up to distances of 2 kilometers (1.2 miles). MMF optic fiber is used in most Gigabit and 10 Gigabit point-to-point networks. Light waves are dispersed into multiple paths, or modes, as they travel through the cable's core that is typically 850 nanometers or 1300 nanometers in diameter. Multimode fiber core diameters are 50, 62.5, and 100 micrometers.

Coaxial

RG-8 & RG-58

Coaxial cable today is used mostly in telephone and cable television systems. In the past, coaxial cable was used in 10Base5 (Thicknet/RG-8) and 10BASE2 (Thinnet/RG-58) Ethernet networks. Coaxial cable uses BNC connectors. The heavy shielding offered by coaxial cable helps protect data offering longer maximum cable lengths than the more prevalent Cat 5 cable. However, coaxial cable is expensive and the connectors are harder to make. For longer communication distances and higher data transfer rates, fiber-optic cable is used today.

RG-59/RG-6

Coaxial RG-59 cable was typically used for cable television installations and has the same physical properties of other coaxial cable types. In today's cable networks however RG-6 is typically used because it offers a larger amount of shielding over RG-59 thus allowing it to transmit a signal longer without degradation. RG-6 is also used almost exclusively for cable modem installations.

Serial

Serial cables are typically split into two main categories: RS-232 and USB. Serial cables provide a medium for serial communications between two devices. RS-232 was typically used to connect computer equipment to a modem or other low speed devices. RS-232 has been almost completely replaced by Universal Serial Bus (USB) which is used to connect a variety of different devices in the current market from hard drives to memory sticks.

Plenum vs. Non-plenum

The difference between Plenum and Non-plenum cables is based on how the cable reacts in a fire. Non-plenum cables are a large fire hazard because they can burn easily and when burnt these cables release toxic gases. As many cables in buildings are run in the space between floors which is also used for return air to the HVAC system any fire with this type of cable will become serious very quickly. Plenum cables are constructed of materials which provide a safer alternative to Non-plenum cables and do not release toxic gas when burnt. The National Fire Protection Association (NFPA) requires that when cable is run in these areas a plenum rated cable be used. Plenum cables however are more expensive than Non-plenum cables.

Properties

Transmission Speeds

The transmission speed of these cables ranges considerably. RS-232 cables are limited to a max speed of around 230 Kbps. Fiber on the other hand has a relatively unknown maximum transmission speed, at present fiber is limited to about 160 Gbps but this changes frequently with technological evolution.

Distance

The distance a signal can be transmitted over a cable is greatly affected by the cables susceptibility to interference which can change a signal enough to make the signal unrecognizable. Unshielded cables like UTP are most prone to this interference and thus are more susceptible, thus making the cable limited to shorter distances. Shielded copper cables like STP and coaxial type cables are less likely to be affected by interference because of their shielding. This does not mean they are not affected but simply that the interference signal must be stronger in order to affect the signal inside the shielding. Fiber cables are not susceptible to interference the same as copper cables so they are most useful in noisy environments or over longer distances. Fiber cables are more susceptible to breaking as they are more fragile than copper.

Duplex

Duplex is split into two groups: half-duplex and full-duplex. When a device is in half-duplex mode the device can either send or receive at the same time but not both. A device which is in full duplex mode is able to both send and receive a transmission at the same time.

Noise Immunity (security, EMI)

The noise which is created by all copper cables introduces a couple of issues. One, the transmission inside the copper cable is done using an electrical signal and is susceptible to outside electromagnetic interference. This makes the signal which is being transmitted able to be changed by outside sources inadvertently. These outside sources can be anything from a power cord to a paralleling cable.
Two, because the signal is electrical it is possible to tap this type of wire without much trouble and without much disruption in the signal. This of course makes any type of copper signal very susceptible to outside security threats.

Frequency

The frequency range which is allowed on each type of cable varies considerably. Twisted pair cables vary depending on the category of the cable: Category 5 & Category 5e cables are rated up to 100 MHz, Category 6 cables are rated up to 250 MHz and category 7 cables are rated up to 600 MHz. Both RG-59 and RG-6 cables are rated to around 2.3 GHz but RG-6 cables are better shielded and thus are less susceptible to outside interference and signal loss.

2.2 Identify Common Connector Types

RJ-11

RJ-11 stands for Registered Jack-11. This is a four-wire connector used mainly to connect telephone equipment in North America. A phone circuit uses two wires; the RJ-11 jack uses four wires. The RJ-11 connector looks very similar to the RJ-45 connector. Be careful not to confuse the RJ-11 with the RJ-45 connector, which holds eight wires and is slightly larger. The RJ-11 connector is used in computers to connect a phone line to a computer modem.

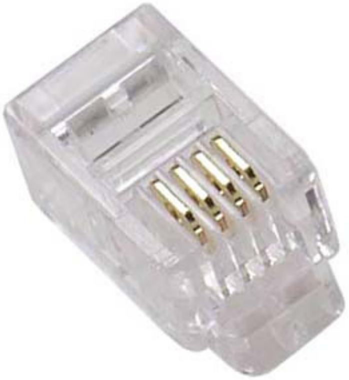


Figure 2 - RJ11 Connector

RJ-45

RJ-45 connectors are used on 10BASE-T and 100BASE-T networks and are defined in IEEE 802.3 standard. The RJ-45 connector is used with CAT 5, CAT5e, and CAT 6 cables. RJ-45 connectors connect computers in LANs to hubs and switches. If your computer is attached to a standard Ethernet network, disconnect the RJ-45 cable in the back of your computer and have a look. The RJ-45 is a connector for digital transmission over 4-pair copper wire, either untwisted or twisted. The interface has eight wires or pins.

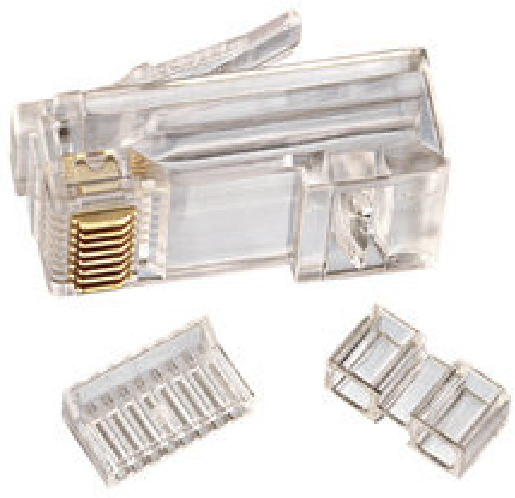


Figure 3 - RJ45 Connector

BNC

A BNC connector is a threaded, coaxial signal connector typically used in consumer applications, such as a coaxial cable connection to a TV or VCR. A BNC media connector is inexpensive because the pin of the connector is actually the center conductor in the coaxial cable.

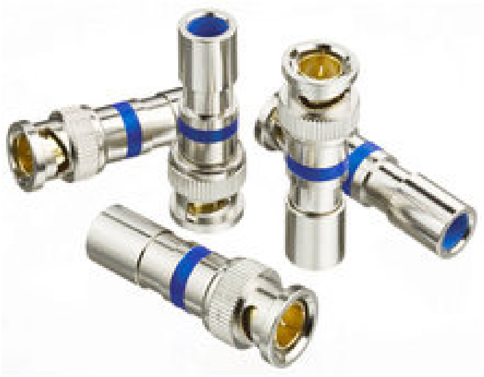


Figure 4 - BNC Connector

SC

SC stands for standard connector or subscriber connector. This fiber-optic cable connector is sometimes called a square connector because of its shape. SC connectors are latched and require a button or release to disconnect it. SC connectors work with both single-mode and multimode optical fibers and last for around 1,000 connections/disconnections. Although not as common as ST connectors, they are seeing increased use in 1000BASE-CX and 1000BASE-LX LAN connections.

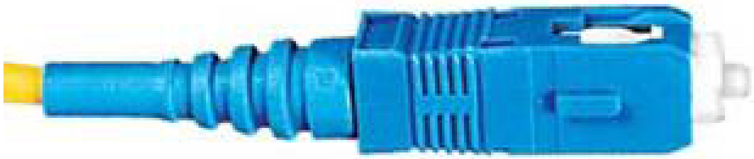


Figure 5 - SC Connector

ST

ST stands for Straight Tip. This is a fiber-optic cable connector you'll see in 100BASE-FX networking environments. This is one of two commonly used fiber optic connectors. It uses a BNC attachment mechanism much like what you see in F-Type cable connectors.

Figure 6 - ST Connector

LC

Fiber-optic LC connectors have an RJ-45 push-pull style housing and latching mechanism. LC connectors are half the size of standard connectors and are used on private and public Ethernet networks. Fiber patch cords using LC connectors are used to connect fiber optic Ethernet network devices.

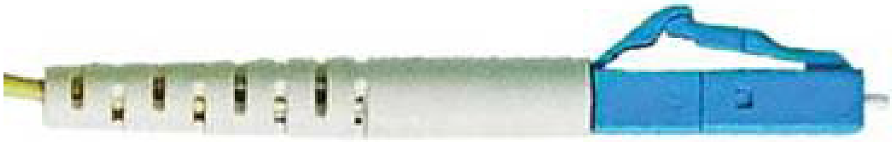


Figure 7 - LC Connector

RS-232

The Recommended Standard 232 (RS-232) is used to connect between low bandwidth devices like modems. For the most part it has been overtaken by USB as a serial connection. RS-232 devices connect via either a DB-9 or DB-25 style connection.

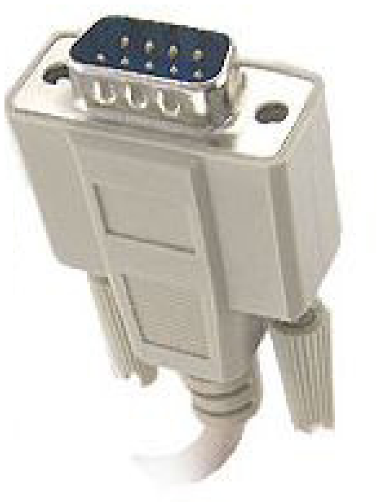


Figure 8 - RS232 Connector (9-pin)

2.3 Identify Common Physical Network Topologies

- Star
- Bus
- Mesh
- Ring
- Point to Point
- Point to Multipoint
- Hybrid

Star Topology

A star physical topology is used on a LAN (Local Area Network) and usually doesn't look like a star, except on paper. The focal point of this topology is what you'll find at the center, namely a centralized hub or switch to which all the network's nodes/devices are connected. Network devices are easily connected or disconnected to the central hub or switch using network media, such as UTP (Unshielded Twisted Pair) cable. This topology is commonly used for 10BASE-T, 100BASE-TX, or 1000BASE-T networks.

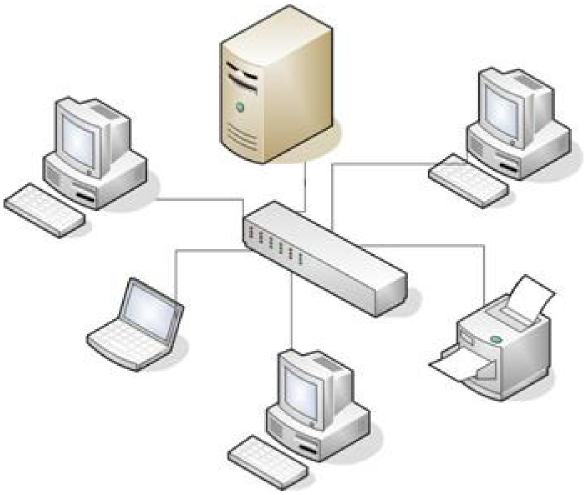


Figure 9 - Star Topology

Advantages

- Cabling is inexpensive and easy.
- Reliable and easy to administer and maintain.
- Locating and repairing bad cables is straightforward.
- Network growth is easily accommodated.

Disadvantages

- All nodes on the network receive the same signal, dividing the bandwidth.
- The maximum number of computers is 1,024 on a LAN.
- If a central media attachment device, such as a switch, fails, the entire network on the switch fails.
- The maximum UTP network cable length is 100 meters (about 330 feet).

Bus Topology

A bus physical topology connects all network devices to a common backbone or bus. PC's connect to the bus by using network cable that attaches or "taps" into the backbone directly. Network signals are sent along the bus in both directions on most buses. This topology was commonly used for 10BASE5 and 10BASE2 networks and is seldom used today.

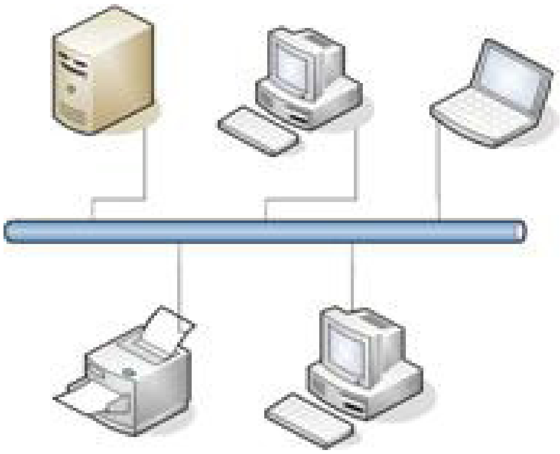


Figure 10 - Bus Topology

Advantages

- Simple to set up. Good for small networks and for quick or temporary LAN installations.
- Additional devices can be added anywhere on the bus.
- Bus topology requires less cable than a star topology.

Disadvantages

- In a physical bus topology, when the network media on one node fails, the entire LAN fails.
- This topology is very difficult to troubleshoot. Locating a break in the cable, or the device causing the fault, when the entire network is down can be time-consuming.
- The length of the bus is limited by cable or signal loss.
- The bus must be terminated at both ends to prevent signal bounce.

Mesh Topology

In a mesh physical topology, every device on the network is connected to every other device on the network. Partial mesh networks don't incur quite the same expense in terms of cabling but, of course, lose some of the redundancy. This topology is most commonly used in WAN (Wide Area Network) configurations for redundancy and maximum fault tolerance.

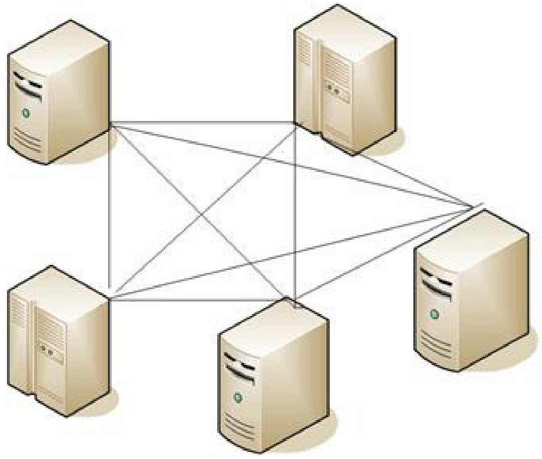


Figure 11 - Mesh Topology

Advantages

- Provides redundancy and fault tolerance. If one device fails, one of the other backup devices takes over with no loss of data.
- A mesh network is reliable. It's easy to find a quick route through the network.
- Can work over great distances.

Disadvantages

- Expensive and complicated, both of which make implementation difficult.

Ring Topology

In a ring physical topology, network devices are wired and connected in a conceptual circle. A ring topology is almost always implemented in a logical ring topology on a physical star topology. Each device is attached to two other devices and uses the same network transmission signal, forming a path in the shape of a ring. Network data flow is unidirectional, and a controlling device, such as a hub or switch, intercepts and manages the data flow to and from the ring. Each device has a NIC (Network Interface Card) that contains a network transceiver, which both sends and receives signals. This topology uses network token-passing access methods referred to as Token Ring. Token Ring is the most common type of ring network.

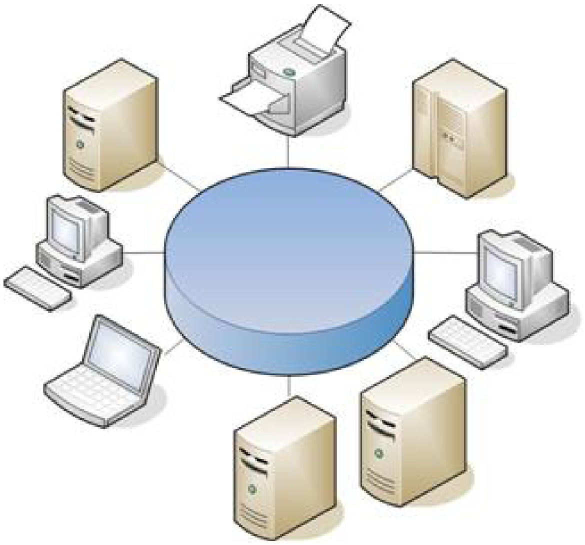


Figure 12 - Ring Topology

Advantages

- Signal degeneration is low.
- Only the device that holds the token can transmit packets of data, which eliminates network packet collisions.

Disadvantages

- Difficult to troubleshoot and locate the problem cable in a network segment.
- Hardware is proprietary and expensive.

Point to Point

A point-to-point topology is one of the simplest as it simply goes from one point to one other point.

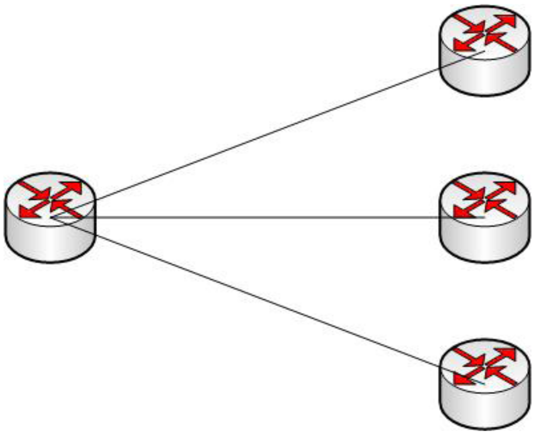


Figure 13 - Point-to-point topology

Advantages

- Simplest of all topologies

Disadvantages

- Point to point connection would be expensive if used between all devices; typically they are only used between WAN sites.

Point to Multipoint

A point to multipoint connection connects one device to multiple other devices through one physical connection. This type of connection is typically used with technologies like frame-relay.

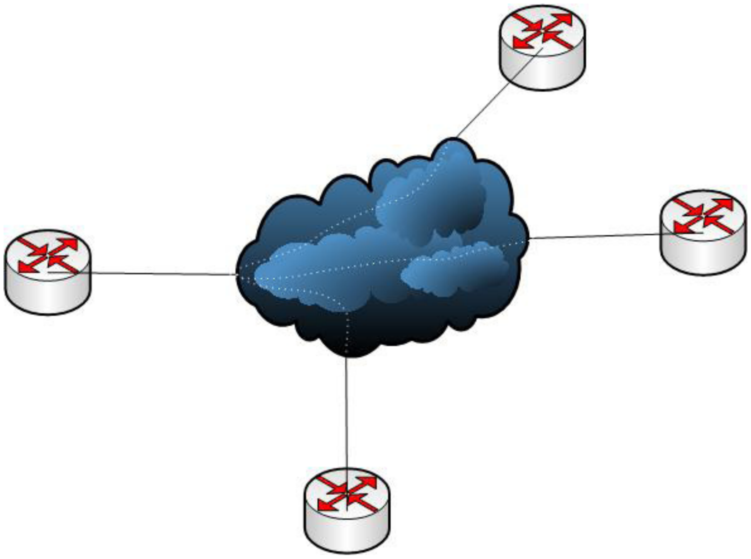


Figure 14 - Point-to-Multipoint Topology

Hybrid

A hybrid topology is simply a combination of several of the other topologies. Typically this topology is used in most networks because the requirements for connectivity between inside devices are different than the connectivity between external sites. The internal networks might use a star topology while the connectivity between remote sites might be point-to-point.

2.4 Given a Scenario, Differentiate and Implement Appropriate Wiring Standards

568A / 568B

568A and 568B standardize on the pinouts of how a twisted pair cable is terminated. The only difference between the two is four wires are reversed. When 568A or 568B is used for a patch cable it does not matter which termination is used within the end connector. 568A is typically used for inside presence wiring. Twisted pair cables typically include four pair of copper conductors and are color coded: Orange-White/Orange, Green-White/Green, Blue-White/Blue and Brown-White/Brown. The pinout differences are shown in the following figure:

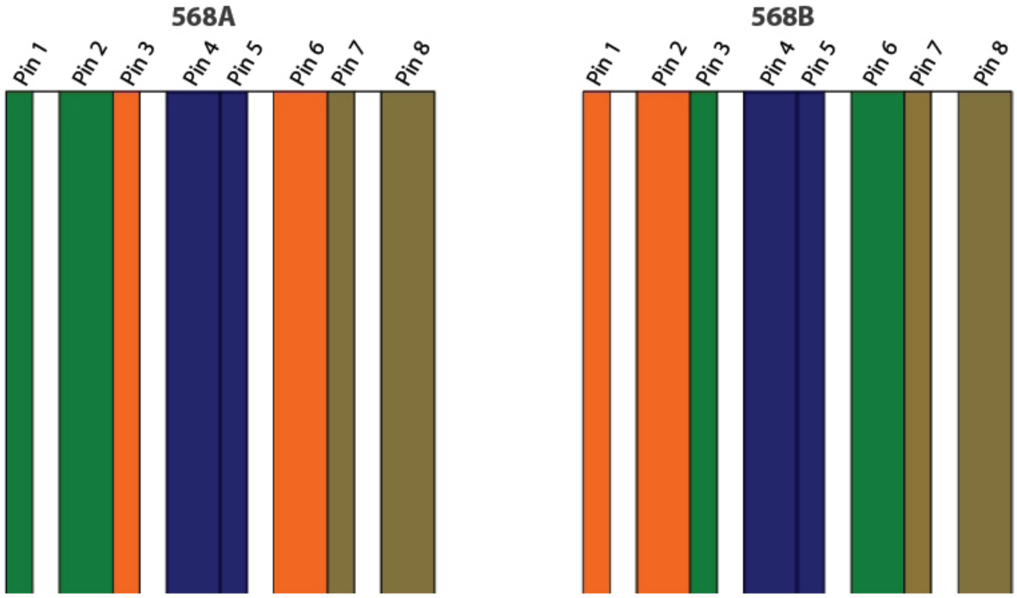


Figure 15 - 568A & 568B Pinouts

Straight vs. Cross-over

A straight through cable is simply a cable which has its pins laid out on both side of the cable in the same order. This can include a 568A to 568A cable or a 568B to 568B cable. These types of cables are typically used when connecting end devices to routers or switches. When connecting two of these types of devices together router to router or switch to switch it is typical for a cross-over cable to be used. A cross-over cable simply reverses the transmit and receive pairs inside the cable. This type of cable is typically a 568A to 568B or 568B to 568A cable. On normal Ethernet connections only pins 1, 2, 3 and 6 are used.

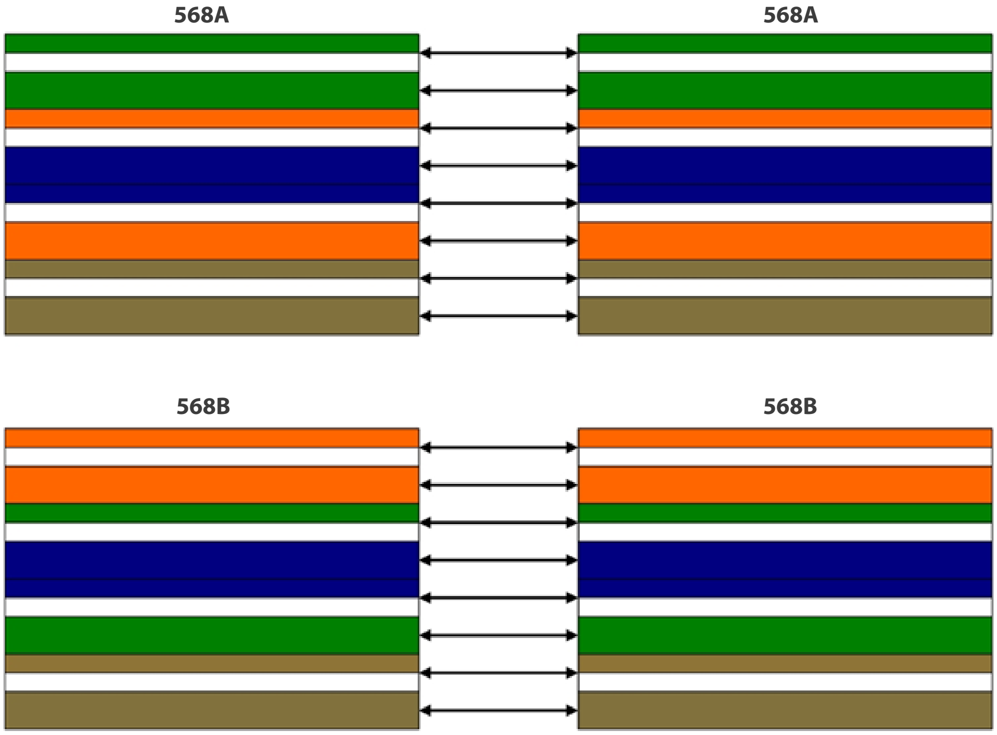


Figure 16 - Straight through Cable

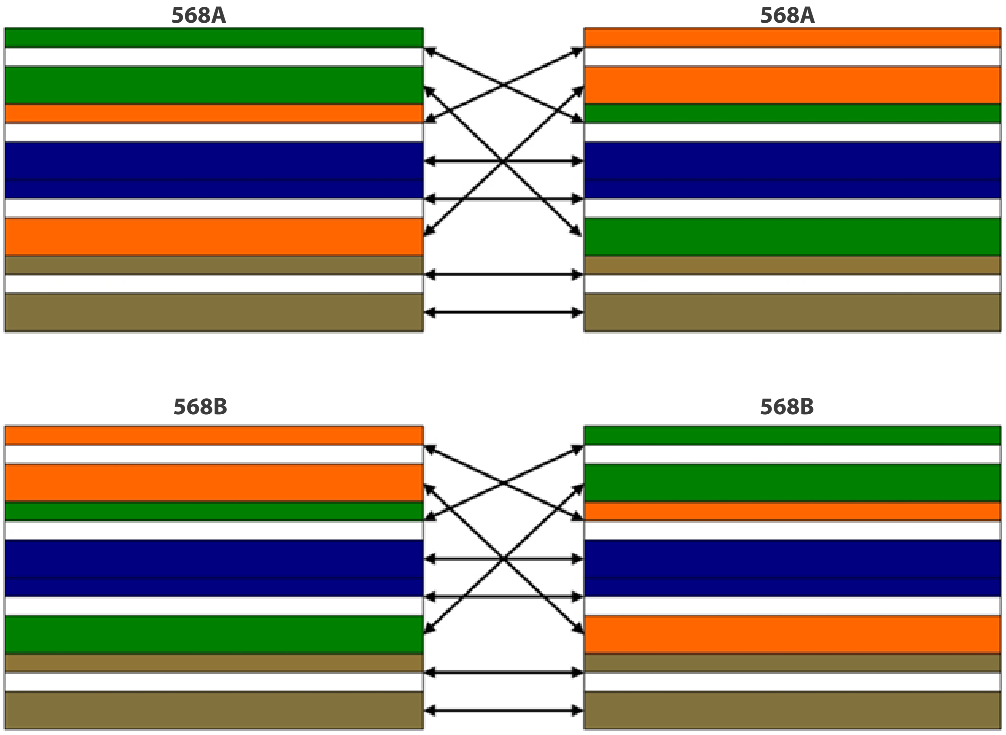


Figure 17 - Crossover Cable

Rollover

A rollover cable is typically used for Cisco console cables. This type of cable does an exact swap of all 8 pins inside the cable.

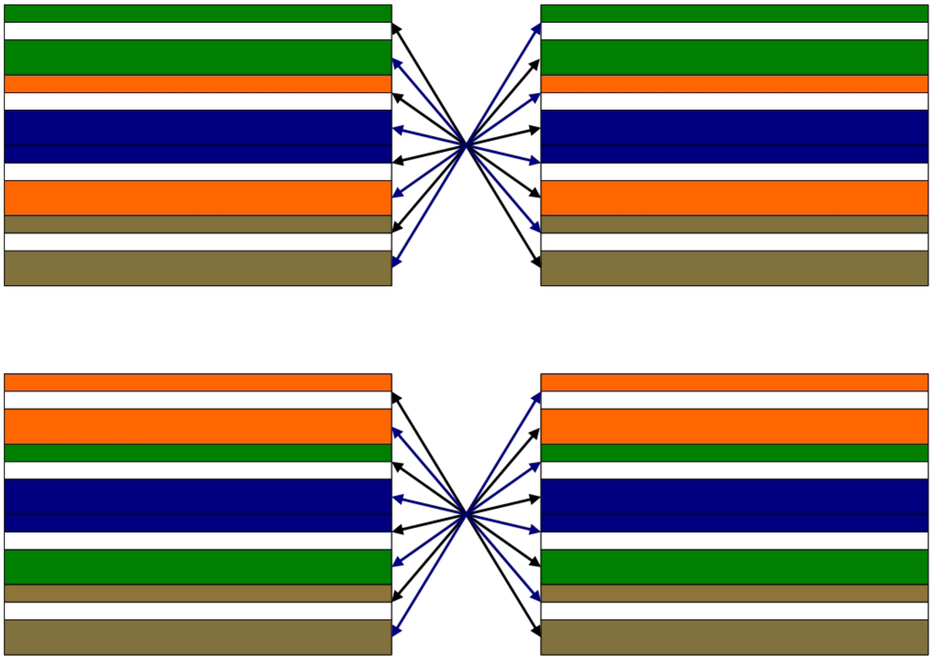


Figure 18 - Rollover Cable

Loopback

A loopback plug is simply a physical connection which reverses the transmit and receive pins back into the same plug. This is typically used for testing purposes.

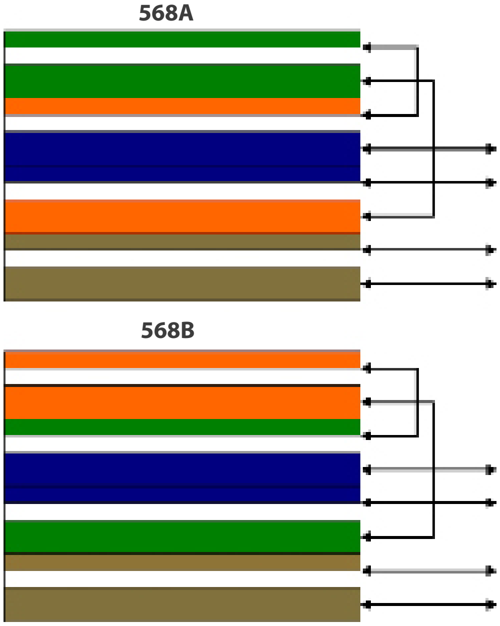


Figure 19 – Ethernet Loopback Plug

2.5 Categorize WAN Technology Types and Properties

Types

Frame Relay

Frame Relay is a packet switching technology which is typically used as a replacement to leased lines. This is because frame relay connections are more cost effective. A frame relay connection is able to virtually connect to a number of different remote sites through point-to-point and point-to-multipoint connections. These connections are called Virtual Circuits (VC). Frame relay is typically provisioned with a Committed Information Rate (CIR) which is the maximum amount of data bandwidth which is guaranteed by the frame relay provider. This does not however mean that higher bandwidth is not possible only that the CIR is guaranteed. Many providers offer a certain amount of burst ability to their customers; this burst capability depends greatly on the capacity of the providers network and the current frame relay network demand. Each individual VC inside the physical frame relay network connection is identified with a Data Link Connection Identifier (DLCI).

E1/T1

The T-series connections are digital carrier transmission systems introduced in the United States by the Bell System in the 1960s. ISPs and medium to large companies are likely to employ either T1 or T3 transmission lines for access to the Internet. Both T1 and T3 lines are leased from a phone service provider.

T-series connections can use standard copper pair cables found in most telephone services, or a fiber optic backbone line. Today, T-1 is often used on fiber optic media. T-series connections currently use Time Division Multiplexing (TDM), which divides the bandwidth of their line into 24 channels each operating at 64 Kbps and each containing a control line. Most telephone companies allow you to purchase just some of these individual channels, which is called fractional T-1 access.

Common T-series lines and their speeds include:

- T1 operates at1.544 Mbps using 24 voice channels
- T3 operates at 44.746 Mbps using 672 voice channels
- E1 operates at 2.048 Mbps using 30 voice channels
- E3 operates at 34.368 Mbps using 480 voice channels
- J1 operates at 1.544 Mbps using 24 voice channels
- J3 operates at 32.064 Mbps using 480 voice channels

E1 or E3 indicates the European counterpart of a T series line. E-series lines do not generally run at the same speeds as their T-series counter parts. Likewise **J1** and **J3** carriers are variants of the T1, T3 transmission lines are used exclusively in Japan.

DSL

Digital Subscriber Line or DSL is a high-speed Internet access technology carrying both digital voice and digital data and is used by businesses and consumers. Transmitting digital data allows the phone company provider to produce greater bandwidth using multiple channels in higher frequency ranges (greater than 3200Hz) than regular voice phone calls. This bandwidth can also be divided into an analog signal so you can still use your analog voice phone while using DSL to access the Internet. A signal splitter provided by the phone company is often required to accomplish this, although emerging technologies such as DSL Lite and G. Lite don't use a splitter.

DSL technologies use several different modulation schemes to transmit data over copper wires. The two most common are Discrete Multitone Technology (DMT) and Carrierless Amplitude Modulation (CAP). The type of media used and/or the thickness of the phone line copper wire affect the maximum range of transmission. In general, copper lines can transmit data up to 5.5 kilometers (18,000 feet) without the use of a repeater. Using fiber optical cable can further extend phone loops. The telephone company uses a Digital Subscriber Line Access Multiplexer (DSLAM) to connect multiple loops of DSL users to its high-speed backbone gigabyte network, xDSL is the term used that refers to several types of DSL technologies. Asymmetric Digital Subscriber Line (ADSL) and Symmetric Digital Subscriber Line (SDSL) discussed earlier, are the two primary types. Other types include:

- HDSL (High-bit-rate DSL)
- VDSL (Very high DSL)
- CDSL (Consumer DSL from Rockwell)
- DSL Lite
- RADSL (Rate-adaptive DSL)
- G. Lite (an emerging xDSL technology)

xDSL, often compared to ISDL because it also uses copper as a medium along with POTS, offers greater transmission speeds than ISDN. xDSL uses up to 32 Mbps for uploading data, and from 32 Kbps to more than 1 Mbps for downloading data at a maximum distance of about 5.5 km or 18,000 feet.

The following table lists the types of xDSL, maximum distance, data upload and download rates, along with characteristics and use.

xDSL Name	Distance Range	Download Speed	Upload Speed	Characteristics Use
ADSL	18,000 ft	1.544 to 6.1 Mbps	126 to 640 Kbps	Most popular type. Used for access for Web access, streaming audio and video, and with remote access
SDSL	12,000 ft	1.544 (U.S.) 2.048 Mbps (Europe)	1.544 (U.S.) 2.048 Mbps (Europe)	T1/E1 LAN or WAN connection from company network server to phone company
HDSL	12,000 ft	1.544 duplex 2-twisted pair 2.05Mbps duplex 3-twisted pair	1.544 duplex 2-twisted pair 2.05 Mbps duplex 3-twisted pair	T1/E1 LAN or WAN connection from company network server to phone company
IDSL (ISDN DSL)	18,000 ft	12 Kbps	128 Kbps	Transmits data only. Similar to ISDN BRI
CDSL	18,000 ft	1 Mbps	Less than 1 Mbps	No splitter necessary. Used in home and small business; similar to DSL Lite
DSL Lite / G. Lite	18,000 ft	1.544 to 6.1 Mbps	Less than 1.544 Mbps	No splitter ADSL type that produces less speed due to lack of splitter in home or small business
RADSL	n/a	640 Kbps to 2.2 Mbps	270 Kbps to 1.1 Mbps	Same as ADSL
VDSL (Very high DSL)	1000 ft to 4500 ft	1.6 Mbps to 53 Mbps	1.5 Mbps to 2.3 Mbps	ATM networks using fiber optic cable

Table 3 - DSL Technologies

Cable Modem

Broadband cable, used by businesses and consumers, also provides high-speed Internet access technology carrying digital data. Using coaxial cable for the installation media, cable modems convert analog signals into digital data. Cable operators deliver the bandwidth using copper lines and for greater distances, fiber optic cable. Cable companies offer a range of bandwidths from 256 Mbps to 1024 Mbps upload speed to 512 Mbps to 3 Mbps download speed. Cable modems are popular and compete favorably with DSL.

A representative schematic diagram of an ADSL and cable Internet installation appears below.

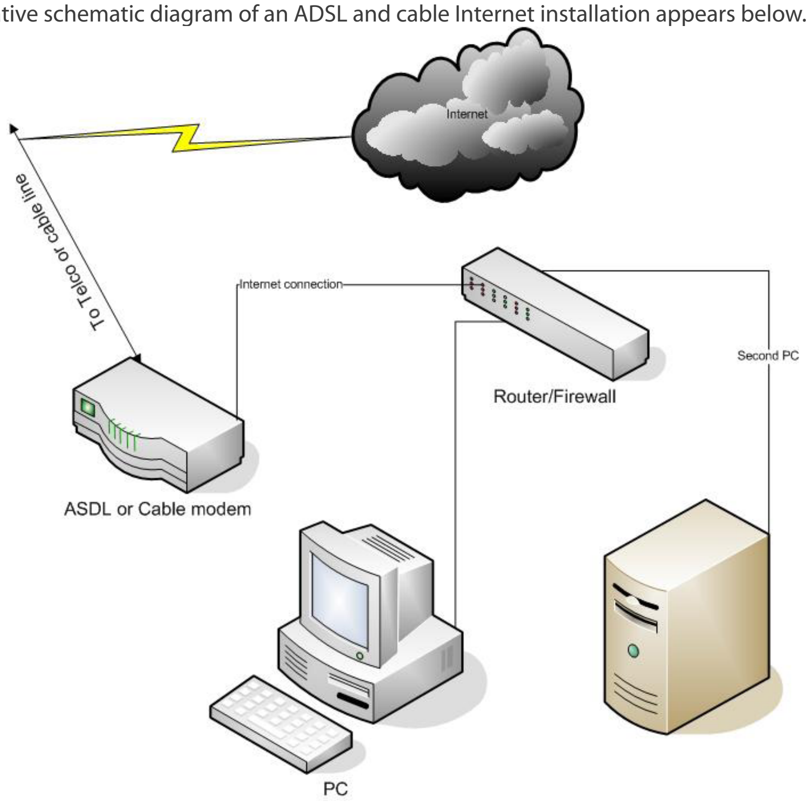


Figure 20 - ASDL and Cable Internet

Satellite

Satellite broadband technology offers Internet access by using a satellite modem that sends signals to a home-based satellite disk that, in turn, sends and receives signals to a terrestrial satellite orbiting above the earth. Homes and small business with twenty or less users can use satellite broadband with download speeds up to 1.5 Mbps and upload speeds of only 128 Kbps. Due to slower Internet access speeds, satellite broadband is used primarily in rural areas that don't have access to cable or DSL technology. As with other types of satellite technology, a clear line-of-sight, southern orientation of the satellite disk is necessary. Satellite broadband Internet access technology hasn't really caught on due to its slower upload and download speeds.

OC-x/SONET

The base rate for OCx using fiber optic media is called OC-1 and operates at 51.84 Mbps. The Synchronous Optical Network (SONET) also uses various OCx speeds on optical fiber. The following table summarizes the current OCx transmission standards and speeds.

Optical Carrier Level	Data Rate
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	10 Gbps
OC-256	13.271 Gbps
OC-768	40 Gbps

Table 4 - Optical Carrier Levels

Wireless

There are a couple of different wireless technologies which are currently used for Wide Area Networks. These include older style microwave point-to-point connections which are used to connect two locations together which have no direct obstruction. Satellite services are also available; of course as long as the location has a relatively unobstructed line to the satellite it is very useful. The problem with using Satellite for WAN connectivity is that it introduces a good amount of delay to the connection and is very expensive over the other land based wireless or wired technologies. The newest of the wireless WAN technologies is WiMAX which is standardized as 802.16. This technology uses some of the same concepts as the 802.11 technologies but offers these types of broadband speeds over a much larger area.

ATM

Asynchronous Transfer Mode (ATM) provides a high speed quality minded solution for large scale WAN deployments. It became popular over the 1990's and early 2000's. ATM splits all traffic into 53 byte cells which are transferred across the ATM network extremely quickly. ATM also offers a large number of QoS options for traffic which allow traffic priority to be very refined. The problem with ATM is also its advantage that is the 53 byte cell. While this cell is very easy to switch at high speed through a network it is very limited by its fixed size. Because of this other technologies are considered more preferred over new ATM deployment, namely MPLS.

MPLS

Multi Protocol Label Switching (MPLS) is a packet switching technique which enables packets to be tagged or labeled to differentiate different types of traffic. These types can be anything from different streams requiring high QoS requirements like VoIP or they can be used to form a VPN to safely transport traffic between multiple companies' branches. MPLS is considered a Layer 2.5 protocol because it has the ability to interoperate directly with both layer 2 protocols like ATM and with layer 3 protocols like IP.

ISDN

ISDN is a digital telecommunications network that can carry voice, data, and video over existing telephone networks. It is designed to provide a single interface for connecting to a phone, fax machine, or PC containing a modem.

The benefits of ISDN include the following:

- ISDN is faster than dial-up modems. Connections are established in less than a second on the D channel.
- Data transfers are faster than on standard analog lines using the 64 Kbps per B channel.
- Combining ISDN channels and PPP multilink provides you more bandwidth on WANs, compared to a single leased line's best performance of 56 Kbps.

ISDN has two communications channels:

- **B-channel** - The Bearer (B) channel. This is a 64 Kbps channel used for voice, video, data, or multimedia calls. There are two B channels that can be combined for a total speed of 128 Kbps.
- **D-channel** - The Delta (D) channel. This operates at 16 Kbps. It's used primarily for communication, or signaling, between switching equipment in the ISDN network and the onsite ISDN equipment.

The ISDN customer purchases ISDN channels in one of two pre-defined configurations:

- **Basic Rate Interface (BRI)** - BRI is what you'll see most often in the field. ISDN users who connect to the Internet generally do so through a BRI configuration. ISDN BRI supports two 64 Kbps B-channels and one 16 Kbps D-channel over a standard phone line. For the test, remember that these channels combined provide you with a data rate of 144 Kbps. This two B, one D setup is how BRI gets its nickname, "2B+D." BRI is very flexible. A single BRI line can support up to three calls at once. This means you can talk, send a fax, and send data simultaneously.
- **Primary Rate Interface (PRI)** - PRI is used primarily by large organizations with demanding communications requirements. PRI supports 23 64 Kbps B-channels and one 64 Kbps D-channel over a high speed DS1 (or T1) line in North America.

Setting up ISDN includes non-ISDN equipment such as an old-style telephone cable. ISDN devices include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment.

ISDN Device Type	Description
TE1 (Terminal Equipment type 1)	Understands ISDN standards and can connect directly into an ISDN network.
TE2 (Terminal Equipment type 2)	Predates ISDN standards; requires a terminal adapter (TA) to connect to an ISDN network.
NT1 (Network Termination 1)	Connects user devices to the ISDN network.
TA (Terminal Adapter)	Converts TE2 wiring to TE1. Connects into an NT1 device for conversion into a two-wire ISDN network.

Table 5 - ISDN Device Types

POTS/PSTN

PSTN is our national public switch or phone network service that carries analog voice data at speeds up to 56 Kbps. Mentioned earlier, Plain Telephone Service (POTS) is the ordinary phone service we use in our homes. Companies, of course, use POTS for their business phones and fax machines and often also use computer modems for internal fax sending and receiving.

Properties

Circuit and Packet Switching

The difference between packet switching and circuit switching is the use of resources. Using circuit-switched networks, messages are broken into packets. Circuit switching uses a dedicated connection between the sender and receiver that is maintained throughout the exchange. Network resources using circuit-switched networks are static before the start and until the end of the data transfer, creating a logical circuit.

Using packet-switched networks, on the other hand, messages are broken into packets, each of which can take a different route through the network to the destination where the packets are reassembled. So, in packet-switched networks, resources are not reserved and can travel several routes through various routers.

The following figure visually compares the two types of switching.

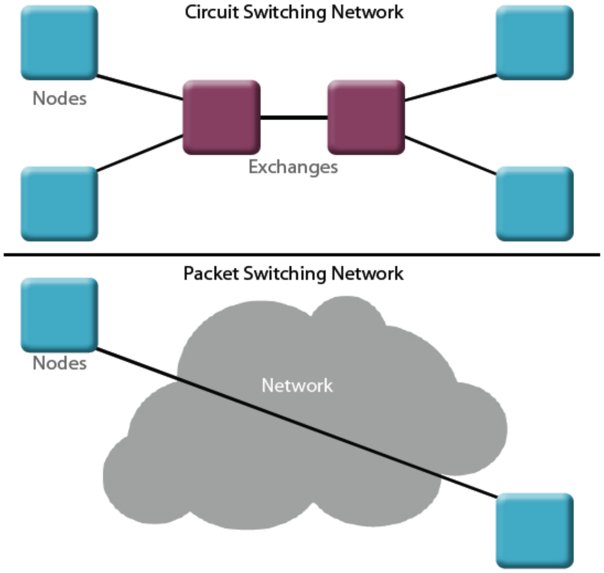


Figure 21 - Packet and Circuit Switched Network examples

Of course, it's not *really* that simple. Not all networks can be classified as pure circuit-switched networks or pure packet-switched networks.

This table compares the two switching types:

Resource	Circuit Switching	Packet Switching
Dedicated path?	Yes	No
Available bandwidth?	Fixed	Dynamic
Could bandwidth be wasted?	Yes	No
Store-and-forward transmission?	No	Yes
Each packet follows the same route?	Yes	No
Call setup?	Required	Not required
When can congestion occur?	At setup time	On every packet
Charge?	Per minute	Per packet

Table 6 - Circuit and Packet switching comparison

Circuit-switched networks have the following advantages and disadvantages:

- Allow for high volumes of data to be transferred with guaranteed transmission capacity. This provides support for real-time traffic. Circuit switching is ideal for data that must be transmitted quickly, and arrive in sequencing order and at a constant arrival rate. It is ideal for transmitting real time data, such as audio and video.
- They are short-lived. When sending short messages, the setup delay easily makes up a large proportion of the total connection time, which means a reduction in network capacity.
- They are static. Other users cannot use the circuit, even if it's inactive.

By contrast, packet-switched networks have the following advantages and disadvantages:

- Support many connections at once. Most WANs protocols, such as TCP/IP, X.25 and Frame Relay, are based on packet-switching technologies.
- Short messages are not delayed by long messages. This generally means packet-switched networks are more efficient than circuit-switched networks. Packet switching is more efficient for bursts data, and can withstand delays in transmission, such as e-mail messages and Web pages.
- In packet-switched networks, performance tends to drop when there are a large number of users.
- They lack error checking and guaranteed delivery of packets.

Speed

The speed of WAN connections varies considerably depending on the requirements of the specific situation. Circuits are still available mainly using frame relay which can go as low as 64 Kbps. On the other side different SONET connections support speeds up to 40 Gbps with speeds on the drawing board of well above 160 Gbps.

Transmission Media

The transmission media which is used for WAN's varies considerably depending on the type of connection and the requirements. Low speed frame relay links can be used to reach branch offices with very low bandwidth requirements; this type of connection can be done through a fractional-T1 circuit which can use as little as one timeslot of 64 Kbps. Several different technologies can be transmitted on a variety of media, including coaxial, UTP, STP, and fiber. Higher speed connections tend to use fiber connections because of its natural security characteristics and that its signal does not degrade easily.

Distance

As stated above depending on the type of connection required the media will determine the length a signal can be transmitted without having the signal boosted. Copper based cables are limited more than fiber cables because the signal is more susceptible to outside interference. Fiber based cables can be used to travel hundreds of miles depending on the type of power which is used to transmit the light over the cable.

2.6 Categorize LAN Technology Types and Properties

Types

- 10BASE-T
- 100BASE-TX and 100BASE-FX
- 1000BASE-T, 1000BASE-SX, and 1000BASE-LX
- 10 GBASE-SR, 10 GBASE-LR, and 10 GBASE-ER

The tables below summarize details such as media type, maximum cable length, etc. about Ethernet and Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet.

Designation	Media Type	Maximum Cable Length	Maximum Transfer Speed	Connector	Topology
10BASE-T	Cat 3 or better UTP	100 meters	10 Mbps	RJ-45	Star
100BASE-TX	Cat 5 UTP	100 meters	100 Mbps	RJ-45	Star
100BASE-FX	Micro multimode optical fiber	412 meters (half duplex) 2km without a repeater (full duplex)	100 Mbps (half duplex) or 200 Mbps (full duplex)	SC fiber-optic connector	Star usually set up only as point-to-point

Table 7 - Ethernet and Fast Ethernet

Designation	Media Type	Max Cable Length	Max Transfer Speed	Connector	Topology
1000BASE-T	Cat 5, 4pr	100 meters	1 Gbps	RJ-45	Star
1000BASE-SX	Micro multimode optical fiber	550m (50u) 275m (62.5u)	1 Gbps	SC fiber-optic connector	Point-to-point
1000BASE-LX	Multimode or single mode Fiber optic	550 meters (multimode) or 5000 meters (single mode)	1 Gbps	SC fiber-Optic connector	Point-to-point
1000BASE-CX	STP	25 meters	1 Gbps	DB-9 or HSSDC	Point-to-point

Table 8 - Gigabit Ethernet

Designation	Media Type	Max Cable Length	Max Transfer Speed	Connector	Topology
10 GBASE-SR	Multimode optical fiber	300 meters	10 Gbps	LC Fiber Connector	Point-to-point
10 GBASE-LR	Single mode optical fiber	10 kilometers	10 Gbps	LC Fiber Connector	Point-to-point
10 GBASE-ER	Single mode optical fiber	40 kilometers	10 Gbps	LC Fiber Connector	Point-to-point
10 GBASE-SW	Multimode optical fiber	300 meters	10 Gbps	LC Fiber Connector	Point-to-point (SONET)
10 GBASE-LW	Single mode optical fiber	10 kilometers	10 Gbps	LC Fiber Connector	Point-to-point (SONET)
10 GBASE-EW	Single mode optical fiber	40 kilometers	10 Gbps	LC Fiber Connector	Point-to-point (SONET)
10 GBASE-T	UTP	100 meters	10 Gbps	RJ-45	Star

Table 9 - 10 Gigabit Ethernet

Properties

CSMA/CD

CSMA/CD is a contention protocol that defines a set of rules for how network devices compete for sending data along network media. Using CSMA/CD, a computer containing a NIC listens to the network for network communications before sending data. If it doesn't hear another computer sending data, it begins the process of sending its own data. This part is the "Carrier Sense" part. Computers on the same network compete with one another for communication access using similar network media. This is the "Media Access" part. Using CSMA/CD, computers are aware that network collisions can occur, so they are careful to listen for network communication packet collisions. This is the "Collision Detection" part. If a collision occurs, both computers back off the cable media and wait a random period of time before retransmitting their network packets.

Broadcast

A physical LAN broadcast is sent out to all parties on the same physical media. When used with a switch or hub broadcasts are limited to layer 2. When using a router broadcasts are limited to the specific port they are transmitted on. Physical broadcasts are used for a variety of things, mainly to locate devices on the LAN which are unknown to other hosts and to broadcast the presence of services on the LAN.

Collision

A collision on a LAN happens when more than one device transmits at the same time on the same physical wire. This happens often in half-duplex mode as CMSA/CD does not always keep several devices off the wire simultaneously. The difference between a hub and a switch is that the collision domains are restricted to each port individually instead of the whole device. With a hub all devices on every port must wait on every device connected to the hub. On a switch this is limited to the devices which are connected to one port. This is why hubs for the most part are extinct. This added ability greatly increases the efficiency of the switch over the hub.

Bonding

Bonding is a term which defines the combining of several ports into one virtual physical port. The technology which does this is called EtherChannel. This is typically used between large servers and a switch or between switches to increase the amount of bandwidth that is available between the devices. For example, if you have a server which has a high utilization it might be good to get hardware which supports bonding two or more Ethernet connections together to raise the bandwidth available to the clients. The advantage of this over separate independent ports is that only one IP address is required for multiple Ethernet connections. If a failure occurs on one of the links it is simply taken out of service and the link remains up.

Speed

As with WAN's the speed of LANS is greatly dependant on the requirements and the money available to invest in equipment. Typical LAN speeds vary from 10 Mbps through 10 Gbps and 100 Gbps is being researched.

Distance

The distance of a LAN is also dependant on the requirements of a specific network. As fiber technologies are also available for LAN's it is possible to extend a LAN for hundreds of miles but that would really constitute a WAN. Ethernet technologies which used to only be used for LAN's is now common in WAN's. Distance as a property is only restricted by the definition of Local.

2.7 Explain Common Logical Network Topologies and Their Characteristics

Peer to Peer

A peer-to-peer network topology simply means that each of the network devices is a client and there is no central system which is used to authenticate between the devices. This type of topology is typically only used in home networks or in very small business environments. In order to share resources between peer-to-peer computers it must be configured to either allow anonymous access or each user must be independently configured on each client (peer).

Client/server

When using a Client/Server arrangement there is a number of client machines which use a central server or servers to provider their services. These services can include authentication, file serving, addressing services and mail services among others. This type of topology is much easier to maintain as users can be defined in one central location and be used on all clients. This information can also be used for file sharing allowing specific users the rights to add, change or delete files on the server.

VPN

A VPN is a private, secure connection to the public Internet. It allows a "point-to-point" connection between a remote user and their business LAN and it also is used to improve security between wireless nodes. The connection used mostly by companies, uses encryption and authentication.

VLAN

VLANs (Virtual Local Area Networks) are groups of network nodes that form a single broadcast domain based upon logical associations rather than physical connections or location. VLANs usually use a switch operating at Layer 2 of the OSI Model, but you'll usually (but not always) need a Layer 3 device, such as a router, to allow VLANs to communicate with each other.

2.8 Install Components of Wiring Distribution

Vertical and Horizontal Cross Connects

A general cross-connection is a location where different sections of the cable infrastructure come together. This is the point where the cables are routed to the specific equipment which will be handling them. A horizontal cross-connect is typically the location where all of the connections from a specific floor originate from, these typically are end-user cable connections. A vertical cross-connect is typically where all the cables from various floors come together. Sometimes these are in the same physical location.

Patch Panels

A patch panel consists of a number of different terminated circuits which are able to be patched together. Typically the back of these panels consists of the raw cabling coming into the panel and punched down with a 66 or 110 tool. The front of these panels is typically a connection which is easy to connect and reconnect. For Ethernet these connections are a modular RJ-45 connection. The different circuits can then be connected to different locations easily through the use of short patch cables at the front of the panel. The figure below shows what a simple RJ-45 patch panel looks like:

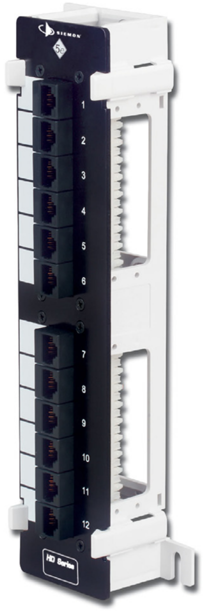


Figure 22 - Ethernet (RJ-45) Patch Panel

66 Block

The 66 block is a common type of telecommunications panel which is used to connect together connections between different devices. 66 blocks connect together individual copper conductors using a punch down tool which is specific to the 66 block. The following figure shows a picture of a current style 66 block:

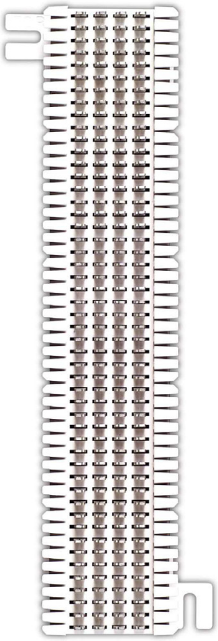


Figure 23 - 66 Block

MDFs

The Main Distribution Frame (MDF) is a telecommunications term which is used to describe the main point of connection for all Central Office (CO) circuits. The types of blocks which are used to connect the circuit will vary depending on the specific location but can include 66 and 110 blocks.

IDFs

The Intermediate Distribution Frame (IDF) is a location which is where equipment can be connected from. The IDF is different from the MDF in that it is not the main termination point for all the circuits but simply a point between the MDF and the circuit's final location. A good example of this would be a floor wiring closet. An IDF can also be used interchangeably with a vertical or horizontal cross-connect depending on the location.

25 Pair

A 25-pair cable is a common type of copper cable which is used to route multiple circuits between various points within an office or building. The following figure shows an example of a 25-pair cable with Amphenol 50-pair connections:

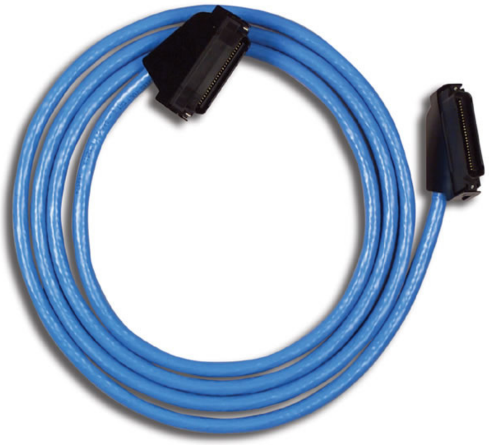


Figure 24 - 25-pair cable

100 Pair

A 100-pair cable is another type of common telecommunications cable inside of CO's which is used to transport several circuits inside only physical cable. The following figure shows an example of a 100-pair cable:

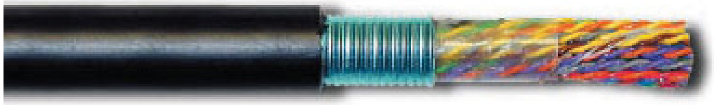


Figure 25 - 100-pair cable

110 Block

A 100 block is another type of telecommunications panel which is used to connect together connections between different devices. 110 panels tend to be used in new installations and are used almost exclusively when routing LAN cables. A 110 style of connection is also used on most modular patch panels.
The following figure shows a picture of the 110 style of connection:

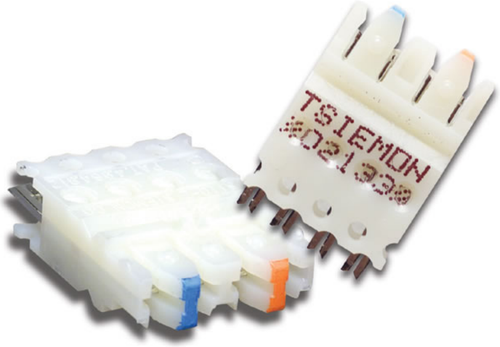


Figure 26 - 110 style connection

Demarc

The Demarcation point is simply the point in a connection or circuit where the responsibility changes. When getting a circuit from a telephone company they will provide the cable up to a certain spot within the location which is typically a modular jack box. At this location the customer is responsible for the rest of the wire inside the building or office. It is the telephone company's responsibility to maintain the circuit up to this point under normal circumstances.

Demarc Extension

A Demarcation extension is a term which is used to describe an intermediate testing point between the demarc and the end of the circuit. Sometimes there is no real point to be referred to as a demark extension. If a cable goes to a small typically tan box and then connects via a modular jack of some sort to the final device then this little tan box is the demark extension. FYI, this is also referred to as an 'Extended Demarc'.

Smart Jack

A smart jack is a term which is used to describe a device which is owned by a telecommunications company that has the ability to test the incoming or outgoing circuit. This device is also referred to as the Network Interface box (NI). It should be noted that this point can sometimes also be referred to as the demarc depending on specific installation.

3.0 Network Devices

3.1 Install, Configure and Differentiate Between Common Network Devices

Hubs operate in Layer 1, the Physical layer, of the OSI Reference Model. A hub is a device that connects all the nodes of a single network. Each device is connected to a single cable that connects directly into the hub. All transmissions that come into a physical port are rebroadcast to all other connections.
That means if one device sends network packets, all the other devices will receive them. All devices connected by a hub are in the same collision domain. A hub generally uses Category 5 media cabling.
Types of hubs include standard (10Mbps), Fast Ethernet (100Mbps), and 10/100 combo versions.
Small peer-to-peer networks (less than 10 devices) are a good candidate for a hub. Larger networks call for switches.

Several types of hubs are available. **Passive hubs** function as an unobstructed pathway for data, enabling it to go from one device or segment to another; it does not regenerate or process signals. By contrast, **active hubs** do regenerate and process signals. The term concentrator is associated with a passive hub and multiport repeater referees to an active hub. Another type of hub is the **intelligent hub**. These hubs offer extra features that allow an administrator to monitor network traffic passing through the hub and to administer ports on the hub. Intelligent hubs are also stackable, so that you can stack them physically on top of each other, conserving space. Another term for an intelligent hub is manageable hub. Yet another type of hub is the **switching hub**, which actually reads the destination address of each packet and then forwards the packet to the correct port. This device approaches the characteristics of a true switch.

You should also be aware that hubs used in Token Ring networks are called **MAUS (multistation access units)**, also known as MSAUs. This device physically connects network computers in a physical star topology containing a logical ring structure. MAUs can be chained together by connecting the Ring Out port of one MAU to the Ring In port of another, then connecting the last MAU's Ring Out port to the Ring In of the first MAU in the chain. This forms a complete loop, or ring. MAUs fix one of the drawbacks of Token Ring networks. In Token Ring networks, a single non-operating node can break the ring. The token simply gets stuck. A MAU solves this problem by shorting out nonfunctioning nodes, thus maintaining the ring structure.

Repeater

A repeater is a simple device which takes a signal, boosts the power level and resends it. These are typically used in the middle of a circuit where the endpoint is physically far away.

Modem

A modem is a device that changes digital data into analog signals transmitted over analog medium, such as telephone lines. Modem stands for **mo**dulator/**dem**odulator.

There are three types of modems you need to know about for the exam:

- **Traditional (POTS/PSTN) -** POTS/PSTN (plain old telephone service/public switch transmission network) is used by telephones and computer modems. Modems are inexpensive and often built into the motherboard. They convert the phone line's analog signal into digital signals that the computer understands. The theoretical highest speed achievable by a modem is 56Kbps. In reality, however, data transfer rates of 48 to 53.3Kbps are achieved to noise and other types of phone line interference.
- **DSL (Digital Subscriber Line)** - **DSL** is a popular high-speed technology popular with both consumers and businesses and is primarily used for connecting to the Internet. Unlike the traditional modem, a DSL line remains connected to the Internet continuously. This means connections are constantly available or always on. Typical data download rates with ADSL are up to 1.544 Mbps with upload rates as high as 1,024 Mbps.

  The two main types of DSL are Asymmetric DSL (**ASDL**) and Symmetric DSL (**SDSL**). ADSL allows more data to be sent over existing copper telephone lines, requires a special ADSL modem, and is increasing in popularity. SDSL also allows more data to be sent over existing copper telephone lines. SDSL both sends and receives data at the same speeds (symmetric) and is used mostly in Europe. SDSL also requires a special SDSL modem.
- DSL uses multiple channels in higher frequency ranges (greater than 3200Hz) than regular voice phone calls, which means it offers greater bandwidth than traditional modems. You don't have to install a separate phone line for DSL: A DSL line can carry both voice and data. As long as DSL service is available in your area, you can purchase and install it using existing phone lines. If you have DSL service on the same service line used to make ordinary voice calls, make sure to also install DSL filters on all the telephone devices. Otherwise, callers will hear a very annoying hissing noise during voice calls. DSL requires a special DSL modem and optional router. Prices for equipment, installation and monthly service vary, though prices have dropped recently.
- **Cable modems** - Provide high-speed Internet access via coaxial cable television lines. At speeds of up to 36Mbps, cable modems using coaxial cable provide much greater bandwidth than telephone lines with speeds up to 3MBps for accessing the World Wide Web. Cable modems require a special DSL modem and optional router. Prices for equipment, installation and monthly service vary, though prices have dropped recently and are competitive with DSL monthly fees.

A disadvantage to using a cable modem for Internet access is that many customers in a local area share access and thus bandwidth—this results in lower transmission rates if everyone in the local area is surfing the Web.

NIC

A Network Interface Card (NIC) is everything its name suggests. It is a card installed in a networked device, such as a computer, that creates an interface or connection to your network. Most NICs are either built into the motherboard or installed as a separate expansion card. PCs, such as laptops, that lack expansion slots often use special PC card NIC adapters or have built-in wireless connectivity instead. A NIC can be wired (Ethernet) or wireless (WLAN).

Media Converters

A transceiver is a network device that transmits and/or receives analog or digital signals. Most computers on LANs use a NIC that contains a built-in transceiver to transmit and receive network signals. In Ethernet networks, a transceiver is sometimes referred to as a medium access unit (MAU). Other network devices, such as cable and ADSL modems, routers, and switches, also contain a transmitter. In an ADSL modem, for example, the connection on the back of the modem, often labeled WAN, is the transmitter converting analog DSL signals into digital signals and connects to a firewall router on a LAN or directly to your home PC NIC. The following figure shows an example of a copper to multimode fiber converter:

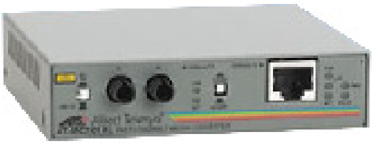


Figure 27 - Media Converter

Basic Switch

Switches have a thing or two in common with hubs. Both devices can connect multiple segments of a single network and both allow those network devices to communicate. Like hubs, switches are used in Ethernet environments and support speeds of 10Mbps, 100Mbps, and 1000Mbps. There is, however, one key difference: A switch filters and forwards packets between LAN segments, making a direct connection between the transmitting device and the destination device separating devices attached to each port into different collision domains.. Compare that to a hub, which rebroadcasts signals out from all ports. On a switched network, only the sending device and the receiving device transmit and receive the signal. The main benefit of a switch over a hub is that no bandwidth is wasted by sending signals to devices that don't need the signal.

Switches operate in Layer 2, the Data Link layer, and sometimes in Layer 3, the Network layer of the OSI Model. Layer 2 switches read the MAC address to determine where a packet is going. Operating at Layer 2 or Layer 3, switches support the use of packet protocols.

Figure 28 - Basic switch

Layer 3 switches can perform some routing functions like Layer 3 forwarding from the hardware but they do not take the place of routers in a network. Layer 3 switches function like Layer 2 switches but use IP or network addresses to communicate. A Layer 3 switch allows you to use switching hardware for routing, which is faster because it eliminates a lot of the latency you'll normally see in regular routers. Switches are a little more expensive than hubs, but because of their speed advantages, are more commonly used today in all types of Ethernet networks.

Bridge

Bridges provide an inexpensive and easy way to connect network segments, much as hubs and switches do. Like switches, they connect two segments of the same LAN or they connect two LANs using Ethernet or Token Ring. Similar to a switch, a bridge operates at Layer 2 on the OSI Reference Model. Bridges and switches both isolate and contain collision domains within a segment. They both transmit broadcasts from one segment to another (which can lead to broadcast storms). Similar to switches, bridges also learn and maintain a table where nodes are located based on MAC addresses.

What sets a bridge apart from a switch is that switches allow simultaneous communications between any two nodes. Bridges are used primarily to segment networks. A switch is designed to communicate with individual nodes whereas a bridge communicates with and between network segments.

When designing a network with more than one segment, the debate often comes down to whether to use a bridge, a switch, or a router. A bridge's best use is to join LANs containing different media types, such as UTP and coaxial. Bridges are also helpful in creating larger networks, and in keeping network segments free from data that doesn't belong on a particular segment. Bridges, however, are seldom used to bridge two LANs because they broadcast all messages to everyone.

Wireless Access Point

As the name suggests, wireless access points transmit wireless network signals to wireless client devices. The range of these signals varies, depending on variables as floors, metal and concrete walls. In general, the range is about 300 feet in a building, up to 1000 feet in open air. In many ways, WAPs are like cellular phone towers. Wireless client PCs can "roam" through and between access points, which extends the coverage area.

Most WAPs, however, cannot communicate with each other wirelessly. In general, WAPs communicate only with wireless clients. This is especially true for inexpensive, consumer-grade WAP products. This means that you can't use two WAPS to wirelessly connect two non-wireless LANs together. To do this, you need to purchase and use a wireless bridge.

WAPs are usually configured using the provided software. It's important for clients to not only change the default workgroup name, but also to enable and configure wireless security discussed later in this study guide. Wireless clients need to also configure the SSID and channel number assigned to a WAP to create a connection.

Basic Router

A router, which operates at Layer 3 of the OSI Model, creates and connects several LANs. However—and here's the key difference between a router and a bridge or switch—a router also permits two *different* network topologies, such as Ethernet and Token Ring on the same LAN. A router provides multiple communication paths (compared to only one on a bridge) between segments, and map nodes on a segment and the connecting paths using a routing protocol and internal routing tables. Network broadcasts cannot transverse a router, but they can transverse switches and bridges.

Figure 29 – Router

Routing over a segmented network is no different than routing over an Internet network. The router uses the packet's destination IP address (this is what makes it a Layer 3 device). Remember, bridges and switches use the Layer 2 MAC address to determine where a frame should go. If the destination IP address is on a segment directly connected to the router, then the router forwards the frame out the appropriate port to that segment. If not, the router will search its routing table and then send it packets to a matching IP address in the routing table.

When you're thinking about hubs, bridges, switches, and routers, remember that routers are the only devices of the four that allow you to share a single IP address among multiple network clients.

Basic Firewall

A firewall is a hardware device or software that is most often used to protect networks and home PCs from malicious attacks from the Internet. Firewalls protect against spyware, hijackers, hackers, viruses, Trojan horses, worms, phishing, and spam are most often used with other protective software, such as anti-virus, anti-spam, and software. Although more expensive than software firewalls, hardware firewalls offer better protection than software alone.

LANs and ISPs commonly use hardware routers that contain built-in firewall protection. Router firewalls using packet filtering and port blocking examine network packets entering or leaving the company's Intranet and block packets that do not meet specified security criteria. Firewalls can also be configured to use sets of pre-defined "rules" and ACLs (access control lists). For example a rule can be created to block certain known IP addresses of phishers. On the software side, proxy servers can be deployed to intercept all packets entering and leaving the network. The proxy server effectively masks or hides the true network addresses on the company's private Intranet. Also, Windows XP Professional, Service Pack 2, when installed, enables a software firewall built into the NOS to primarily protect PCs against worms. Zone Alarm for Windows and SmoothWall for Linux are other good software firewall products that can be downloaded from the Internet.

In summary, the best firewall protection is a combination of both hardware and software: Use an ISP that offers firewall protection, install a firewall router between your cable or DSL modem and your LAN, install Windows XP SP2, and install anti-virus and anti-spam software (be sure to maintain the software with frequent updates).

Basic DHCP Server

A basic DHCP server has the responsibility to issue the IP address to the different devices on a network. This server also has the capability to assign gateway information along with DNS, WINS and various other servers' information at the same time.

On smaller installations, a DHCP server will be located on each LAN segment. For example, almost all home routers (Linksys, Netgear) are also simple DHCP servers and provide addressing, gateway and DNS server information which is used to establish network connectivity.

On larger installations where it is impractical to have a DHCP per segment a central server will be responsible for issuing IP addresses and other information. This makes it much easier to manage both the server and the IP addresses being issued.

3.2 Identify the Functions of Specialized Network Devices

Multilayer Switch

A multilayer switch is different from a typical switch in that it not only handles layer two traffic but also layer three traffic. All normal operations done by a router are integrated into the switch. The switch also has some advantages over using a standalone router; this includes an ability to perform many of the logic functions which are done by the microprocessor on a router on an Application-Specific Integrated Circuit (ASIC) which is more efficient.

Content Switch

A Content switch is another type of multilayer switch. The Content switch performs functions above layer three. This can include load balancing HTTP, HTTPS, and VPN traffic among other purposes.

IDS/IPS

Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) both are used for similar functions. Both are meant to detect a network attack. A network detection system is passive, meaning that they are forwarded a copy of all traffic and watch for attacks to happen. An intrusion protection system is active, meaning that it sits directly in-line with network traffic and watches traffic as it physically come in. An IPS is more secure because it has the ability to block an attack before the end system is affected at all. However, the disadvantage of an IPS is that it does require that all traffic go through it which potentially creates a bottleneck for network traffic. An IDS is intended to respond to an attack that it detects but the end system may have already been affected in some way. At least one of these systems is essential in today's corporate networks as attacks happen all the time. The choice of which one to employ greatly depends on the specific implementation of the company network and the budget.

Load Balancer

A load balancer is a device which is used to balance between multiple servers. In most implementations this is done to give the impression of several servers being located at one physical IP address. The load balancer takes in the traffic and passes it based on the specific balancing algorithm chosen.

Multifunction Network Devices

A multifunction device is a device which provides a combination of services including printing, copying, faxing and scanning.

DNS Server

The DNS server on a network is responsible for mapping domain names to specific IP addresses. Without the DNS server working in a network all devices would require knowledge of the specific IP address of every needed device. While in a very small network this is not a problem in any bigger network it would be almost impossible to remember every IP address. It is however much easier to remember a specific name of a site. The DNS server essentially does the memory work for you and maps these names.

DNS servers are able to keep multiple types of records including Host (A), mail exchanger (MX), aliases (CNAME) and reverse lookup (PTR). An A record is simply a one to one match with a name and a specific IP address. A MX record is used to specify what the name is of the email server for a specific domain name. The CNAME record is used to point one name to another, for example, yahoo.com -> www.yahoo.com. This type of record prevents the need for an excessive amount of A records all referencing an IP address. If this IP address were to change and several A records were configured, each record would need to be changed as well. If these records are replaced by CNAME records then only the original A record would need to change. A PTR record is used to reverse map a domain name, what this means is that it provides the ability to take a specific IP address and map it to a name instead of the reverse.

Bandwidth Shaper

A Bandwidth shaper is used to take traffic which enters the shaper without any order and uses the priority information marked inside the traffic and outputs the traffic in an order based upon these markings. A bandwidth shaper can also be configured to mark traffic as higher or low priority based on specific details of the traffic itself. The shaper will then use these markings when it outputs the traffic.

Proxy Server

Data packets from the Internet can be intercepted by a firewall set up on a proxy server. Proxy servers configured with firewall protection examine all packets before they are sent to destination nodes. Packets not permitted are discarded. *Note*: A Proxy server's primary function is to examine requests for Internet access coming from an internal node. If the request is to a site not permitted, it is discarded and the requesting node is sent a message. For a fuller explanation of proxy servers, review the next section.

CSU/DSU

The **CSU/DSU** is two devices often bundled as one unit found in equipment rooms where the network connects via T-series data connectors, like a leased T1 or T3 line. The CSU/DSU connects a digital carrier, such as the T1 to the network equipment, usually a router. The CSU terminates the line at the customer site, whereas the DSU performs the actual transmission through the CSU. The CSU also provides diagnostics and remote testing while the DSU provides buffering and data flow control. Typically, the two devices are packaged together as a single unit. Think of it as a very high-powered, very expensive modem. Such a device is required for both ends of a leased T1 or T3 connection and both ends must be use the same communications standard.

3.3 Explain the Advanced Features of a Switch

PoE

Power over Ethernet (PoE) is used to provide a power source for small Ethernet devices which are not located close to a good power source. Typically they have been used to power VoIP devices including phones and conference equipment. The defined standard for PoE is 802.3af which describes the amount of power which is available and how it will be negotiated with the devices.

PoE can be provided in one of two ways, either through a PoE capable switch or through a power injector. A PoE switch must have a sufficient power supply which has the ability to power all of the devices connected to it. A power injector is typically used when a PoE capable switch is not available. It plugs into a standard outlet and provides power over the Ethernet connection.

Spanning Tree

The Spanning Tree Protocol (STP) was created to prevent bridging loops. Bridging loops occur when there is more than one path from one part of the network to another. It does this by only allowing traffic to pass along one of the ports at a time. All of the alternative ports are blocked unless the forwarding port fails.

The STP path selection process is based on the cost of the path to the root switch. The root switch is intended to be the center of the switching network. Forwarding port selection is done using a basic cost metric where by each port is given a specific STP cost and the path is selected based on the lowest overall cost. This can also be affected by biasing this calculation with port priorities. STP communications happen through the exchange of Bridge Protocol Data Units (BPDU).

When a port comes into service it passes through a number of STP states until it is allowed to forward. These states in order include: Listening, Learning, and Forwarding/Blocking. During these states the port is communicating with the STP network and figuring whether it is allowed to forward or not. If it is considered an alternate path then it will be put into a blocking state until the forward port fails.

VLAN

A Virtual LAN (VLAN) is a technology which is used on switches to isolate traffic on a physical LAN. It does this by assigning the traffic from specific ports to a VLAN. Any traffic which comes into this port is only forwarded to other ports which are also in that specific VLAN. By default, all traffic on unassigned ports on a switch is put into VLAN 1. If nothing else is configured on the switch the traffic on all ports forwards as normal. If traffic isolation is wanted then each specific port which is to be isolated can be configured in a different VLAN. For example, if you wanted ports which were secured and ports which were not secured assigned to individual VLAN's on a switch. All traffic which would be transmitted on the secured network would only go to other ports marked in the same VLAN and vice versa. There are two ways a port can be assigned into a VLAN, statically and dynamically. Static VLAN membership is manually done for each port on the switch. Dynamic VLAN assignment is done through the use of a server; this server determines the VLAN assignment based on information in the traffic entering the port. For example, the server could look for a specific MAC address. It should be known that when only a switch is available no traffic from one VLAN to another is possible. For traffic to pass from one VLAN to another a layer three device is needed.

Trunking

Trunking is a method of transmitting the traffic from multiple VLANS over a single link. Trunking is typically done on a port which connects to either other switches or a layer three device. When connected to another switch it is possible for ports on a specific VLAN to be transmitted to ports in the same VLAN on another switch. When connected to a layer three device, trunking is typically used to allow the connection between separate VLAN's which is performed by this device.

There are two main types of VLAN trunking, 802.1Q and Inter-Switch Link (ISL). 802.1Q is the standard which is used to define VLAN trunking. All switches which support trunking support 802.1Q. 802.1Q differentiates the VLAN traffic by tagging each piece of network traffic with a VLAN id. This tag is then used to determine which VLAN the traffic is intended for. ISL is a Cisco technology which can only be run on Cisco equipment. This technology is not typically used anymore with Cisco equipment or. ISL works by tagging the traffic similarly to 802.1Q, however the method is different. ISL does this by encapsulating the whole frame of traffic with an ISL header and footer. 802.1Q simply adds a small tag inside the frame.

Port Mirroring

Port mirroring is used to replicate all the traffic to and from a specific port to a separate port. This is typically done either for troubleshooting purposes or when using a traffic analysis device, like an IDS.

Port Authentication

Port authentication is used to make sure that the device which is using a specific port is allowed to send traffic to other devices on the network. This is done through the use of 802.1x authentication. This type of authentication works by obtaining information from the transmitting client and verifying its right to use the port. This information can be something as simple as verifying the MAC address of the transmitting client or can involve authentication through a RADIUS or TACACS+ server. The latter requires specific software on the client system.

3.4 Implement a Basic Wireless Network

Install Client

When setting up a client a couple pieces of information are required before connection is possible. Find out whether the device is being connected through an access point (Infrastructure) or directly to another device (Ad-hoc). Find out what the Security Set Identifier (SSID) of the remote device is. Find out if security is enabled and if so when the parameters which are used are set to. Once these parameters are known the client is able to be setup.

Access Point Placement

The placement of an access point is greatly dependant on where the users of the wireless users will be located when using the network. When placing an access point to cover a wide area make sure to pick an area which is central to the location, this way as much of the structure as possible will be able to use the wireless network. Just like wired networks, wireless networks are influenced by outside interference. Depending on the specific type of equipment used (2.4 or 5.8 GHz.) several other devices may be competing on the same frequency. As well other common pieces of equipment are notorious for sending interference into the same frequency range, these include devices like microwaves.

Install Access Point

When configuring an access point a couple of decisions need to be made; this will directly affect how the clients are setup and how well your network operates. These include what type of encryption is required when transmitting traffic over the wireless network, what frequency range, channels and what Extended SSID to use.

Configure Appropriate Encryption

When selecting a type of encryption the real question becomes what type of encryption can the equipment support. A lot of older equipment is limited to specific types of encryption and because of this forces all other newer devices in the network to use this lower standard. For most current applications either TKIP or AES encryption should be used on the wireless network, as long as all clients support them.

Configure Channels and Frequencies

The selection of which frequency range to use should be done before the purchase of the wireless equipment. Most wireless equipment is limited to use only one of the available wireless frequencies. Typically equipment which uses the 2.4 GHz frequency is cheaper and more widely available, but there are many different pieces of equipment which also use this range. These include everything from cordless phones to baby monitors. The 5.8 GHz band does not have as much interference as the 2.4 GHz band, however as the frequency of a signal goes up it has a harder time penetrating through different materials which are normally found in walls and ceilings.

The selection of the frequency also limits the number of non-overlapping channels which are available. When using the 2.4 GHz band only 3 channels are non-overlapping, these include 1, 6 and 11. When using the 5.8 GHz band there are 12 non-overlapping channels and more possibly depending on on-going standards and 5.8 GHz band changes. Most current equipment can be set to automatically select the channel based on the amount of interference on the channel. The equipment will match and select the channel which is the most optimal.

Set ESSID and Beacon

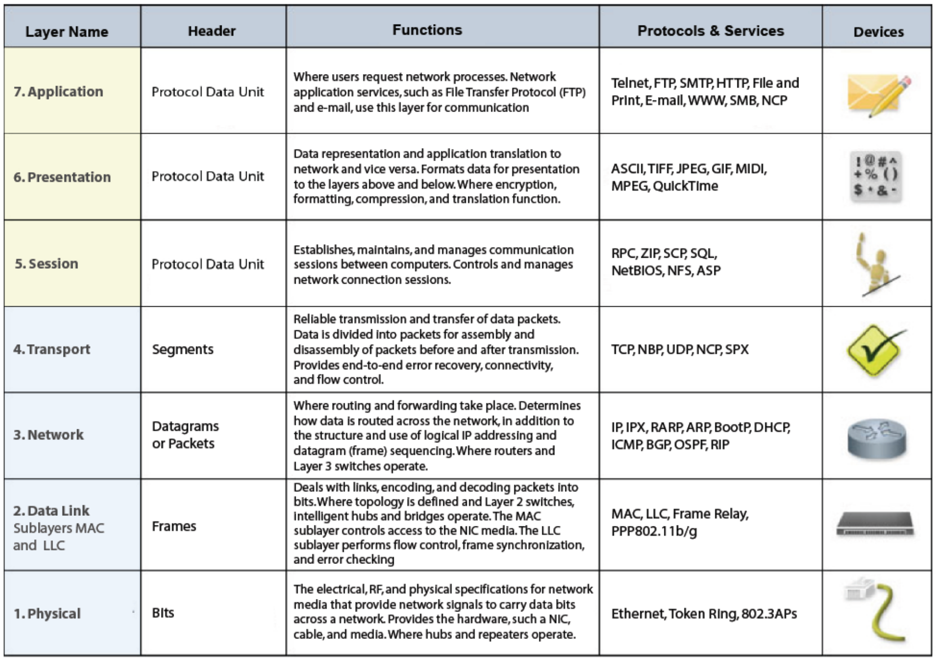
The ESSID (SSID) which is selected is typically something that identifies the wireless network to the people intended to be using it. By default, on most equipment this ESSID will be broadcast out in a wireless beacon (think of it as a 'I am here' message). The beacon typically includes the ESSID, speeds available, parameter sets and capability information. Typically a beacon is configured to be sent every 100 ms, unless there is a reason to change this it is recommended that this not be changed.

Verify Installation

The simple way to verify a wireless installation is to make sure that the client has correctly established connectivity with the access point and that network access it possible through the client. If this is not possible it should be verified that the ESSID and encryption information match.

4.0 Network Management

4.1 Explain the function of each layer of the OSI model



Layer Name	Header	Functions	Protocols & Services	Devices
7. Application	Protocol Data Unit	Where users request network processes. Network application services, such as File Transfer Protocol (FTP) and e-mail, use this layer for communication	Telnet, FTP, SMTP, HTTP, File and Print, E-mail, WWW, SMB, NCP	
6. Presentation	Protocol Data Unit	Data representation and application translation to network and vice versa. Formats data for presentation to the layers above and below. Where encryption, formatting, compression, and translation function.	ASCII, TIFF, JPEG, GIF, MIDI, MPEG, QuickTime	
5. Session	Protocol Data Unit	Establishes, maintains, and manages communication sessions between computers. Controls and manages network connection sessions.	RPC, ZIP, SCP, SQL, NetBIOS, NFS, ASP	
4. Transport	Segments	Reliable transmission and transfer of data packets. Data is divided into packets for assembly and disassembly of packets before and after transmission. Provides end-to-end error recovery, connectivity, and flow control.	TCP, NBP, UDP, NCP, SPX	
3. Network	Datagrams or Packets	Where routing and forwarding take place. Determines how data is routed across the network, in addition to the structure and use of logical IP addressing and datagram (frame) sequencing. Where routers and Layer 3 switches operate.	IP, IPX, RARP, ARP, BootP, DHCP, ICMP, BGP, OSPF, RIP	
2. Data Link Sublayers MAC and LLC	Frames	Deals with links, encoding, and decoding packets into bits. Where topology is defined and Layer 2 switches, intelligent hubs and bridges operate. The MAC sublayer controls access to the NIC media. The LLC sublayer performs flow control, frame synchronization, and error checking	MAC, LLC, Frame Relay, PPP802.11b/g	
1. Physical	Bits	The electrical, RF, and physical specifications for network media that provide network signals to carry data bits across a network. Provides the hardware, such a NIC, cable, and media. Where hubs and repeaters operate.	Ethernet, Token Ring, 802.3APs	

Yellow	=	Upper layers
Blue	=	Lower layers

Here's a few ways to remember the seven layers of the OSI model:

- From the top down: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
- From the bottom up: **P**lease **D**o **N**ot **T**ake **S**ally's **P**izza **A**way.

4.2 Identify Types of Configuration Management Documentation

Wiring Schematics

A correct wiring schematic of a network is vital in order to make troubleshooting considerably easier. The wiring schematic includes everything in detail from the pinouts of the individual jack going to each device to the specific location that each wire inside a physically is located. For example, if crossover cables are needed to connect together two network devices this would be detailed in the wiring schematic.

Physical and Logical Network Diagrams

A physical network diagram is responsible for keeping track of how each individual device is connected to the other devices. For example, each user device is typically connected to the network through a switch. This physical diagram will show which physical ports each device is attached to. This physical diagram will also detail how all the higher level equipment is physically connected; this will include items like router to router and router to switch connections.

The logical network diagram is a higher level representation of how the network connects together. For example, when viewing an IP logical diagram it may not include the specific switches which are inline because they are not a specific IP hop. If the network includes VLAN's this diagram would also show specific VLAN assignments across the network.

Baselines

One of the things that is good to do once a network is up and running is to perform a performance baseline. This baseline is normally done to measure the 'normal' level of specific criteria under normal conditions. The specific criteria which is usually used for a baseline includes processor, memory, hard disc and network adapter utilization levels.

Policies, Procedures and Configurations

The policy and procedures for an organization include a number of different subjects which are wide ranging. These include specific criteria for user access privileges, correct computer usage (acceptable-use), security requirements (e.g. passwords, time of use, auditing), application requirements (Are individual programs allowed to be installed?), and several other.

Regulations

Regulations are essentially something which is typically wrapped into the policies and procedures for a company because if the company is in a specific industry then they must comply. Some of the best known regulations come from the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA). These Acts specify how information must be handled in specific instances in order to keep the information as secure as possible.

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

When analyzing a problem having up-to-date documentation makes like much easier. This is because often when troubleshooting a network physical access is either not possible or not likely to happen in an efficient timeframe. Using this documentation gives the troubleshooter a picture of how the network is connected and thus makes problem isolation easier.

When making changes to the wiring layout of a network an existing wiring schematic is vital. This way it is known how each specific cable is connected at all termination points and being terminated by what type of equipment. Under normal circumstances wiring does not magically stop working unless there is some sort of work happening which could affect it in some way.

Both physical and logical network diagrams are probably the most important piece of information which can be available to a troubleshooter should a problem occur. This is because equipment does fail and knowing what ports a specific piece of equipment connects through makes troubleshooting easy.
A logical network diagram comes in handy when a problem exists which is not physical in nature, this would include issues like routing problems.

Having a baseline to compare current performance against makes the life much easier when trying to make sure the network in question is performing as good as possible. This baseline can be used to find out which devices in the network are potentially overloaded and in what way. This information can then be used when making equipment upgrade decisions.

Update Wiring Schematics, Physical and Logical Network Diagrams, Configurations and Job Logs as Needed

One of the things that is most common on many networks is a very accurate set of schematics and diagrams when the network is first built then letting all of these go out of date as the network is upgraded. The problem of course is that when a problem does come up and proper documentation is not available this makes the troubleshooting of the network much timelier. This is because someone typically must go physically to a piece of equipment and verify the connectivity as well as someone must go into each piece of equipment in question and verify the current configurations.

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)

Packet sniffing utilities are a mainstay of network troubleshooting; they allow the administrator the ability to watch the specific traffic as it traverses the network. This when used with knowledge of network protocols enables the administrator the ability to figure out complex problems. Their main methods of network connection include going through a network SPAN port or through software directly installed on the end-system.

Connectivity software is typically used to monitor the current status of devices based on a simple ping or SNMP message which is used periodically to make sure that devices are still reachable.

Load testing is done to check the true capabilities of the network against the expectations. This is typically done when new equipment is installed to make sure that everything performs as expected. Throughput testing can also be done at the same time as it is performed to check the actual throughput of the network against the design expectations.

System logs, History logs, Event logs

The numbers of logs which are available to a network administrator are many. On windows servers, the typical three logs which are kept include an application, security and system log. The application log only keeps messages which are specific to applications including programs like Exchange and SQL server. The security log keeps track of login and logoff events as well as any potential security problems. The system log keeps track of events which are specific to the Windows system including drivers and services. On networking equipment a log is kept typically which includes the status of interfaces and protocols run on the device.

4.5 Explain Different Methods and Rationales for Network Performance Optimization

Methods

QoS

Quality of Service (QoS) is used to represent different levels of traffic which can exist on a network. For example, on a network which transports voice it must be given a higher priority as it is more affected by a lower level of service. Several different levels of service are available depending on the QoS standard being followed. The two ways of marking IP traffic include using a Type of Service (ToS) or through Diffserv which defines Differentiated Services Code Points (DSCP) both which use the Differentiated Services field inside the IP header. When using ToS there are eight main levels of priority from 0 through 7 with 0 being the default with no expectation of preference and 7 being the highest level of priority. When using Diffserv there are a number of different DSCP's which are defined which include varying priorities and put more or less influence on different characteristics of the traffic including bandwidth and delay.

Traffic Shaping

Traffic shaping is a method which is used to take network traffic and rearrange it so that higher priority traffic is able to be passed in front of lower priority traffic. This can be done in a couple of different ways. The traffic shaper itself is able in some circumstances to make traffic priority decisions directly on the shaper. In most situations however the traffic shaper is given traffic which has already been marked with priority information, this way the shaper simply makes its decisions based on this marking.

Load Balancing

Another way to improve the performance on a network is to setup load balancing. This technique allows more than one device to be used to perform the same function. All devices do the same task and are able to be used based on the amount of load, this way a high amount of load will be spread upon all of the devices.

High Availability

High availability is a design standard where the availability of the devices within the system are of highest priority. Often the availability of a system is measured by the total amount of uptime which is usually notated by percentage of uptime.

Caching Engines

A caching engine is a device which is placed inline with network traffic and stores information which is commonly requested. This device is then able to load the original data only once and updated occasionally. This way information is able to be more quickly accessed and the loading time of the information is reduced.

Fault Tolerance

Fault tolerance is the ability of a system to deal with a failure without much or any service loss. This is typically through the use of multiple devices, one which is used to perform primary duties and a second which is used when there is a failure in the primary. This is what is called 1 + 1 redundancy. Other types of redundancy exist including N + 1 redundancy which allow one secondary device to backup several primaries.

Reasons

Latency Sensitivity

In modern networks which run voice and video applications it is very important to optimize the delay over the network. This is because too much delay on a voice or video transmission makes it very hard to follow the conversation. With added delay there is also a concern over traffic which is received out of order, when this happens this traffic must either be put back into correct order or dropped. The amount of time that a device has to reorganize this traffic is finite.

High Bandwidth Applications

While some applications require a greater focus on delay, others are more interested in the amount of bandwidth available. These applications are less interested in some amount of delay than overall high bandwidth availability. These applications may include file transfer.

Uptime

When considering the availability of a specific device it is important to focus on what the amount of expected uptime is. Uptime is simply the amount of time that a device is accessible for its given duty. Higher availability applications require a higher amount of uptime. For example, if a hospital uses a VoIP system for communications it is very important that these communications stay available. That said it is very important for the uptime of these VoIP devices to be as much as possible.

4.6 Given a Scenario, Implement the Following Network Troubleshooting Methodology

With Network+ there is a proposed nine step model for troubleshooting, these are described below.

Information Gathering – Identify Symptoms and Problems

One of the most important steps when trying to troubleshoot a problem is correctly finding the problem and identifying the symptoms of the problem. Once this is found it is important to gather as much information as possible about the devices which are affected.

Identify the Affected Areas of the Network

Once the problem and symptoms have been identified it is important to find out what parts of the network have been affected by the problem. This can be done in a variety of ways depending on which type of devices have the problem. If a router or switch has been affected it is possible to find out the status of the affected device by viewing the status of the links which directly connect to other routers and switches. If a specific computer has been affected the status of the network can be obtained initially through the switch which is connected to it. Along with this information common tools can be used to verify connectivity, these tools include ping and traceroute (tracert on windows) among others.

Determine if Anything has Changed

During this step it needs to be determined if the problem or symptom is something new or something that has always existed. For example, is this something that just now has been noticed but was never really working?

Establish the Most Probable Cause

Once the problem has been isolated and defined it is necessary to figure out the most logical reasons for the specific problem. In networks there are a number of root cause possibilities and will greatly depend on the experience of the person troubleshooting. A couple of examples include port mismatches (speed or duplex), VLAN mismatch, incorrect IP assignment, and other misconfigured IP parameters to include a few.

Determine if Escalation is Necessary

The next thing to consider in troubleshooting is whether the problem is within the capabilities of the people currently troubleshooting it and whether they can fix the problem. If it is believed that this will potentially be a problem is always best to as for additional help through the escalation of a ticket.

Create an Action Plan and Solution Identifying Potential Effects

The next step involves creating an action plan which would correct the problem. Another thing that needs to be analyzed is whether the proposed solution will affect other systems. If so, it must be analyzed whether this affect on other systems will be detrimental to their services. If fixing one problem is going to greatly affect another working service it may be best to perform the fix at a time when these services are less used.

Implement and Test the Solution

This step involves the implementation of the proposed action plan. Once all of the actions have been taken which were laid out it is important to test all systems affected to make sure that the fix worked and that all systems are operational.

Identify the Results and Effects of the Solution

This step involves a more detailed look at whether the solution which was performed caused any ongoing problems with either the target system or with other related systems. Sometimes fixing one thing can have a negative effect on another system so it is best to keep an eye on these solutions to make sure the affects are positive. If a problem is found then it is necessary to go back and find a solution which will fix this problem and not affect any other system negatively.

Document the Solution and the Entire Process

Once the solution has been performed and adequate testing has been performed to make sure all systems are operating it is good to fully document the solution and how it was performed. This information can be very useful both as a teaching tool and as a basis for fixing other future similar problems.

4.6 Given a Scenario, Troubleshoot Common Connectivity Issues and Select an Appropriate Solution

Physical Issues

Cross Talk

Crosstalk is what happens on a twisted pair cable when the signal from one cable affects the signal from another. The only way to completely get rid of crosstalk is to isolate and shield every cable, as this is not very cost effective it is more typical to vary the twist rate of the individual pairs within a cable. It is still possible for crosstalk to happen with cables with the same twist rate so having a cable with varying twist rates is optimal.

Near End Crosstalk

Near End Crosstalk (NEXT) is the measurement of crosstalk when measured at the transmitting end.

Attenuation

Attenuation is simply the natural signal degradation which happens over a distance. This is why UTP cables being run for Ethernet are limited to 100 meters, this is because at 100 meters the signal is so degraded that it becomes unrecognizable from the noise in the line. A fiber optic signal degrades less over the distance of the cable and because of this is more useful for long distance cable runs.

Collisions

A collision happens when more than one transmitter tries to transmit on a wire at the same time. Most technologies have methods for reducing or eliminating collisions through flow control or carrier detection.

Shorts

A cable short happens in electrical based cables only when the current going down a wire contacts another media which allows it to be propagated down a path which is not intended.

Open Impedance Mismatch (echo)

Cables which are used in telecommunications have balanced impedance, if there is an impedance mismatch then the signal arrives at different times at the far end of the cable. This causes on a voice line what is known as echo. When there is an 'open' cable state which is indicated by cable testing equipment then this can be indicated also as an impedance mismatch as part of the connection does not connect to the far end and part of it does.

Interference

When talking about networks there are two different types of well known interference: Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI). One affects wired networks and the other affects wireless networks. There are many different sources of EMI including power cables, other telecommunications cables, televisions, monitors, and many types of machinery among many other sources. RFI interference comes from other objects which emit noise into a specific radio frequency spectrum. For example, microwave ovens are notorious at injecting noise into the 2.4 GHz band.

Logical Issues

Port Speed

Port speeds on modern switches is available at 10, 100 and 1000 Mbps. If a specific port is statically set to one of these and the device attached is set to another or does not support the configured speed then the port will not be operational. Most switch ports automatically default to automatic configuration; this negotiation allows both the switch and the device to arrange a port speed which is supported by both.

Port Duplex Mismatch

The port speed as well as the port duplex must match in order for a port to become operational. As with port speed if a specific port duplex is configured and the device connected does not support it, the port will remain non-operational. The provided options include half and full duplex. Like port speed, by default a port will automatically negotiate the port duplex setting.

Incorrect VLAN

An incorrect VLAN assignment is harder to diagnose because the end device does not know which VLAN it is assigned to. Because of this all troubleshooting must be done from the switch. If a device is assigned into an incorrect VLAN it will be unable to communicate with any of the devices it is suppose to. This is because of the nature of VLAN's, inter VLAN communication is not possible without the use of a layer three device.

Incorrect IP Address

Most often when an incorrect IP has been assigned it has been statically assigned. This is because a dynamic IP assignment should be given correctly. If an incorrect IP has been assigned the device will be unable to communicate on the network at all and to any device, if this does happen simple ping troubleshooting should prove this suspicion.

Wrong Gateway

If an incorrect gateway has been configured then the device will be able to communicate with all local (in the same subnet) devices but not devices which are not local. The first step in troubleshooting an incorrect gateway is to make sure the configured gateway is in the device's subnet and whether the device is able to be pinged.

Wrong DNS

If an incorrect DNS server has been configured all devices will be able to be contacted directly via their IP address but no devices will work using their hostname. When troubleshooting first make sure that the DNS servers are reachable using a ping test, most DNS servers still allow you to ping them.

If should be noted that some names may work if they are statically configured in a local host's file, however this file is typically not used on most computers. Only a few corporate administrators may take advantage of this option as a backup to important local hosts.

Wrong Subnet Mask

An incorrect subnet mask can present as an interesting problem depending on what mask is assigned. If the mask which is assigned allows the end device to still be in the subnet of the gateway then normal communications will work correctly. However, if services are used which use local broadcasts then the address which is used for broadcast will be incorrect and weird symptoms will result.

Issues That Should be Identified but Escalated

There are a number of different problems where it is recommended be escalated to the next level of support. This is because these problems can be extremely complex and require a higher level of technical knowledge.

These conditions include:

- **Switching loops**
- **Routing loops**
- **Route problems**
- **Proxy arp conditions**
- **Broadcast storms**

Wireless Issues

There are also a number of issues which are specific to wireless networks. These conditions include:

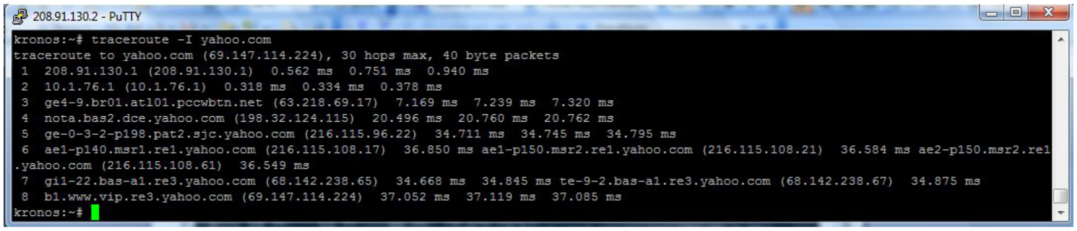
- **Interference (bleed, environmental factors) –** Interference can come from a number of sources and can include anything that potentially sends noise into the used wireless frequency.
- **Incorrect encryption –** Incorrectly configured encryption will present as the network not being able to establish connection with the access point.
- **Incorrect channel –** An incorrectly configured channel will present itself allot like an incorrect security configuration. This is because if there is a channel mismatch the device will be unable to connect to the access point.
- **Incorrect frequency –** When using an incorrect frequency the device will be unable to see the access point at all. This is because the end device is looking in a completely wrong location.
- **ESSID mismatch –** If there is an incorrect ESSID configured then the end device will be unable to associate with an access point.
- **Standard mismatch (802.11 a/b/g/n) –** Having a standard mismatch is a bit more complicated. This is because most of the newer standards are backward compatible. 802.11g is backward compatible with 802.11b; 802.11n is backward compatible with 802.11a, b, and g.
- **Distance –** Just like wired signals, wireless signals have a specific range. Once a device is located at the end of this range the device will be unable to connect with the access point.
- **Bounce –** Bounce is the wireless version of repeating a signal, at times the bounce that is given to a wireless network may spread the wireless signal over a larger area than expected. Take care to make sure the signal only is propagated within the confines of the intended area.
- **Incorrect antenna placement –** The position of an antenna or antennas greatly affects how a network signal is spread out. If these antenna(s) are placed in a location which is not proper for the intended target area the wireless network will be ineffective.

5.0 Network Tools

5.1 Given a Scenario, Select the Appropriate Command Line Interface Tool and Interpret the Output to Verify Functionality

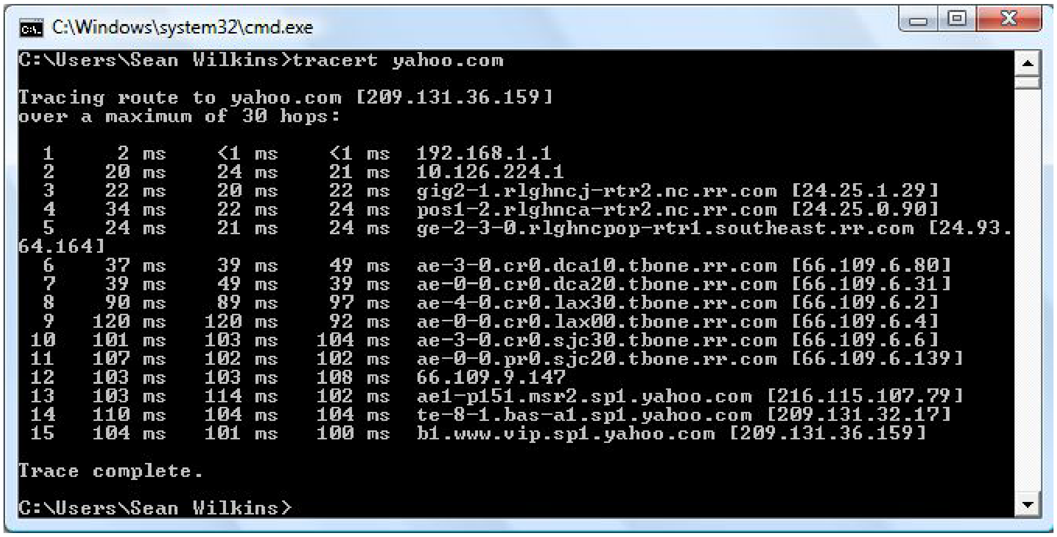
Traceroute

The traceroute utility enabled an administrator to obtain the specific path which is being followed to a specific location. The traceroute utility is called 'traceroute' on Linux based machines and 'tracert' on windows machines. There are two different methods which are used by the traceroute utilities, the Linux variant by default uses UDP packets and the windows variant uses ICMP echo request packets. Both find the path to the destination through the manipulation for the Time To Live (TTL) value in the IP header. The TTL specifies the maximum number of hops a packet can be sent before the packet is dropped and an error message is sent back to the originating host. The traceroute utility works by starting with a TTL of 1 and going up until the end system is reached in order to obtain the path. The following figures show the windows and Linux variants of this command:



```
kronos:~# traceroute -I yahoo.com
traceroute to yahoo.com (69.147.114.224), 30 hops max, 40 byte packets
 1  208.91.130.1 (208.91.130.1)  0.562 ms  0.751 ms  0.940 ms
 2  10.1.76.1 (10.1.76.1)  0.318 ms  0.334 ms  0.378 ms
 3  ge4-9.br01.atl01.pccwbtn.net (63.218.69.17)  7.169 ms  7.239 ms  7.320 ms
 4  nota.bas2.dce.yahoo.com (198.32.124.115)  20.496 ms  20.760 ms  20.762 ms
 5  ge-0-3-2-p198.pat2.sjc.yahoo.com (216.115.96.22)  34.711 ms  34.745 ms  34.795 ms
 6  ae1-p140.msr1.re1.yahoo.com (216.115.108.17)  36.850 ms ae1-p150.msr2.re1.yahoo.com (216.115.108.21)  36.584 ms ae2-p150.msr2.re1
.yahoo.com (216.115.108.61)  36.549 ms
 7  gi1-22.bas-a1.re3.yahoo.com (68.142.238.65)  34.668 ms  34.845 ms te-9-2.bas-a1.re3.yahoo.com (68.142.238.67)  34.875 ms
 8  b1.www.vip.re3.yahoo.com (69.147.114.224)  37.052 ms  37.119 ms  37.085 ms
kronos:~#
```

Figure 30 - Linux traceroute command

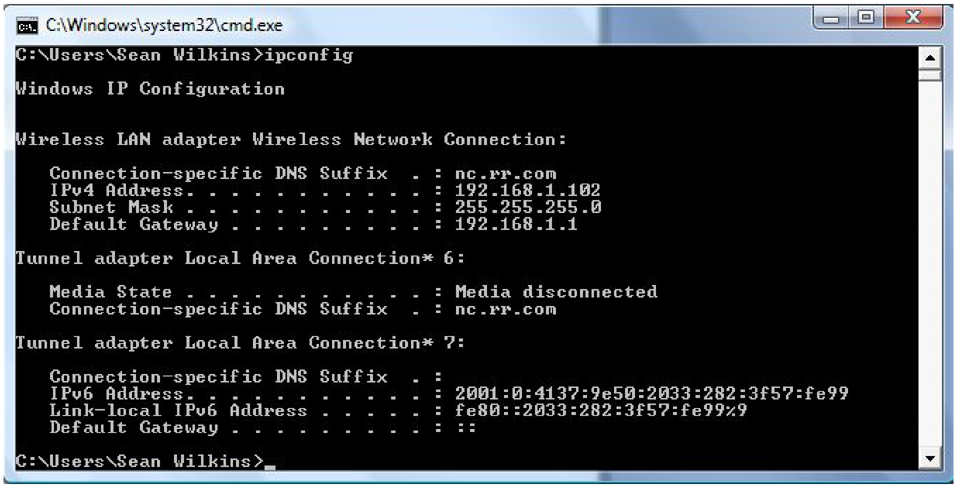


```
C:\Users\Sean Wilkins>tracert yahoo.com

Tracing route to yahoo.com [209.131.36.159]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  192.168.1.1
  2    20 ms    24 ms    21 ms  10.126.224.1
  3    22 ms    20 ms    22 ms  gig2-1.rlghncj-rtr2.nc.rr.com [24.25.1.29]
  4    34 ms    22 ms    24 ms  pos1-2.rlghnca-rtr2.nc.rr.com [24.25.0.90]
  5    24 ms    21 ms    24 ms  ge-2-3-0.rlghncpop-rtr1.southeast.rr.com [24.93.
64.164]
  6    37 ms    39 ms    49 ms  ae-3-0.cr0.dca10.tbone.rr.com [66.109.6.80]
  7    39 ms    49 ms    39 ms  ae-0-0.cr0.dca20.tbone.rr.com [66.109.6.31]
  8    90 ms    89 ms    97 ms  ae-4-0.cr0.lax30.tbone.rr.com [66.109.6.2]
  9   120 ms   120 ms    92 ms  ae-0-0.cr0.lax00.tbone.rr.com [66.109.6.4]
 10   101 ms   103 ms   104 ms  ae-3-0.cr0.sjc30.tbone.rr.com [66.109.6.6]
 11   107 ms   102 ms   102 ms  ae-0-0.pr0.sjc20.tbone.rr.com [66.109.6.139]
 12   103 ms   103 ms   108 ms  66.109.9.147
 13   103 ms   114 ms   102 ms  ae1-p151.msr2.sp1.yahoo.com [216.115.107.79]
 14   110 ms   104 ms   104 ms  te-8-1.bas-a1.sp1.yahoo.com [209.131.32.17]
 15   104 ms   101 ms   100 ms  b1.www.vip.sp1.yahoo.com [209.131.36.159]

Trace complete.

C:\Users\Sean Wilkins>
```

Figure 31 - Windows tracert command

IPconfig

The ipconfig command is used on a windows device to obtain the current IP configuration which is configured. The ipconfig command can also be used to perform limited functions including clearing the Windows DNS cache. The following figure shows an example of the ipconfig command:

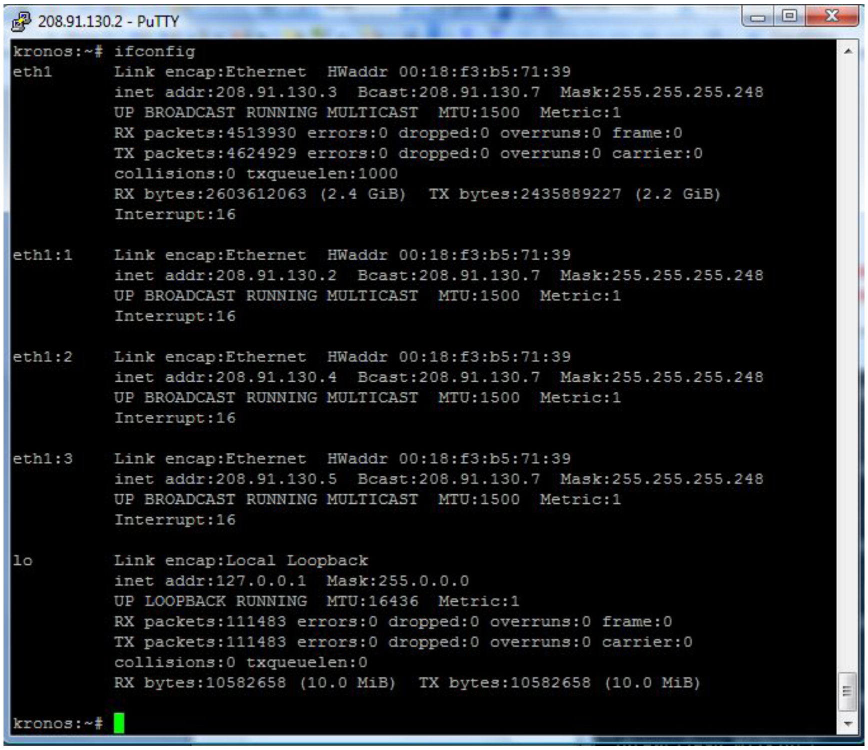


```
C:\Users\Sean Wilkins>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : nc.rr.com
   IPv4 Address. . . . . . . . . . . : 192.168.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : nc.rr.com

Tunnel adapter Local Area Connection* 7:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e50:2033:282:3f57:fe99
   Link-local IPv6 Address . . . . . : fe80::2033:282:3f57:fe99%9
   Default Gateway . . . . . . . . . : ::

C:\Users\Sean Wilkins>_
```

Figure 32 - Windows ipconfig command

IFconfig

The ifconfig command is similar to the ipconfig command except it is used on Linux based machines. Similarly to the ipconfig command the ifconfig command is able to show the currently used IP configuration. The following figure shows an example of the ifconfig command:

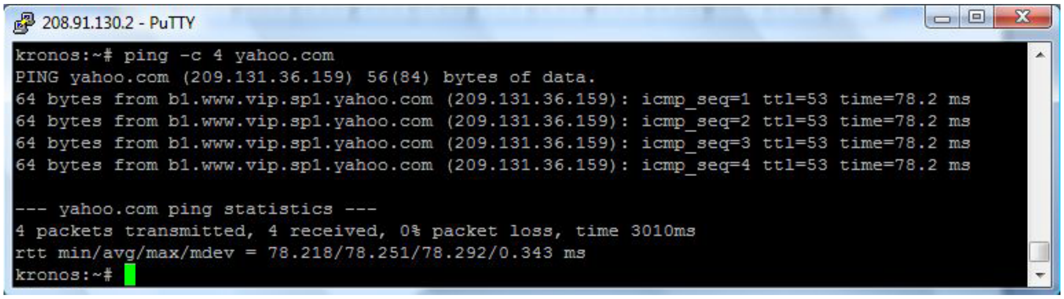


```
kronos:~# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:18:f3:b5:71:39
          inet addr:208.91.130.3  Bcast:208.91.130.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4513930 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4624929 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2603612063 (2.4 GiB)  TX bytes:2435889227 (2.2 GiB)
          Interrupt:16

eth1:1    Link encap:Ethernet  HWaddr 00:18:f3:b5:71:39
          inet addr:208.91.130.2  Bcast:208.91.130.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:16

eth1:2    Link encap:Ethernet  HWaddr 00:18:f3:b5:71:39
          inet addr:208.91.130.4  Bcast:208.91.130.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:16

eth1:3    Link encap:Ethernet  HWaddr 00:18:f3:b5:71:39
          inet addr:208.91.130.5  Bcast:208.91.130.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:16

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:111483 errors:0 dropped:0 overruns:0 frame:0
          TX packets:111483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10582658 (10.0 MiB)  TX bytes:10582658 (10.0 MiB)

kronos:~# █
```

Figure 33 - Linux ifconfig command

Ping

The ping command is one of the most common and most useful of all network utilities. It is used to find out the current status of an end device. The ping utility works by sending an ICMP echo request packet to the end system, under normal circumstances if the device is reachable it will respond with an echo reply. It should be noted however that many personal firewall software packages which are run on modern machines block ICMP echo messages by default for security. If testing computers which are running these types of programs make sure that ICMP echo messages are allowed while troubleshooting. The following figure shows an example of the ping command in use:

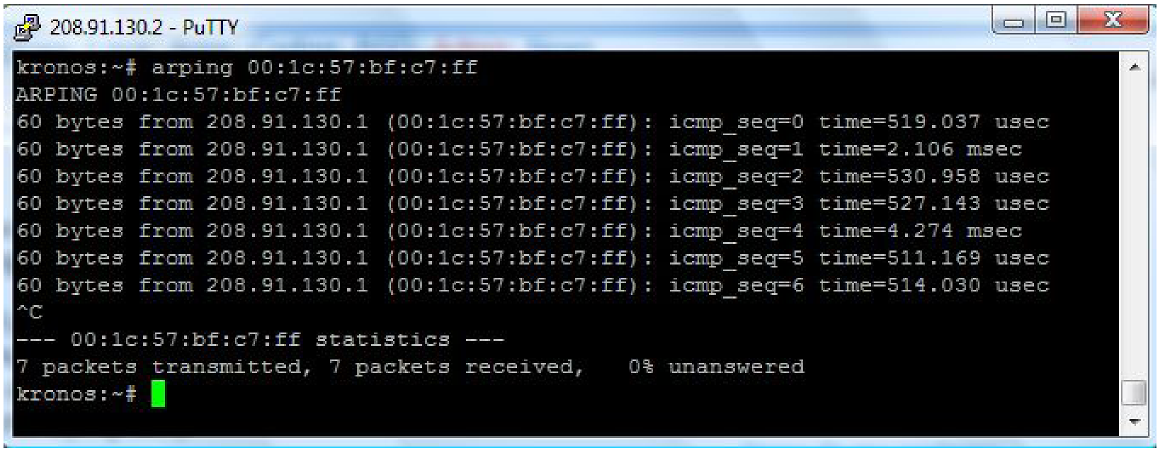


```
kronos:~# ping -c 4 yahoo.com
PING yahoo.com (209.131.36.159) 56(84) bytes of data.
64 bytes from b1.www.vip.sp1.yahoo.com (209.131.36.159): icmp_seq=1 ttl=53 time=78.2 ms
64 bytes from b1.www.vip.sp1.yahoo.com (209.131.36.159): icmp_seq=2 ttl=53 time=78.2 ms
64 bytes from b1.www.vip.sp1.yahoo.com (209.131.36.159): icmp_seq=3 ttl=53 time=78.2 ms
64 bytes from b1.www.vip.sp1.yahoo.com (209.131.36.159): icmp_seq=4 ttl=53 time=78.2 ms

--- yahoo.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 78.218/78.251/78.292/0.343 ms
kronos:~#
```

Figure 34 - ping command

Arp Ping

An ARP ping has the same function as an IP ping but is used at layer two. The arping utility works by sending out an ARP message to the destination MAC address specified. If a device with the MAC address is on the local network then it will respond. The following figure shows an example of the arping utility:

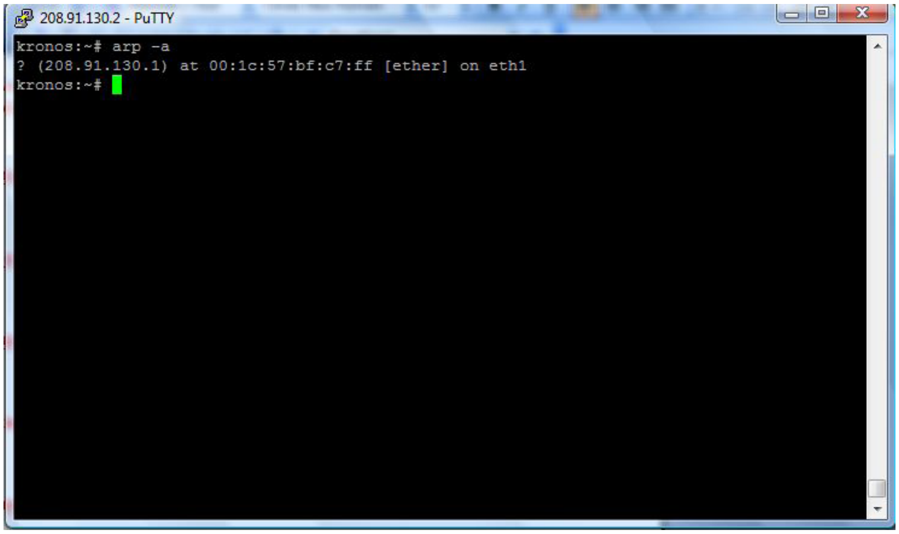


```
kronos:~# arping 00:1c:57:bf:c7:ff
ARPING 00:1c:57:bf:c7:ff
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=0 time=519.037 usec
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=1 time=2.106 msec
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=2 time=530.958 usec
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=3 time=527.143 usec
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=4 time=4.274 msec
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=5 time=511.169 usec
60 bytes from 208.91.130.1 (00:1c:57:bf:c7:ff): icmp_seq=6 time=514.030 usec
^C
--- 00:1c:57:bf:c7:ff statistics ---
7 packets transmitted, 7 packets received,   0% unanswered
kronos:~#
```

Figure 35 - arping utility

Arp

The Address Resolution Protocol (ARP) is used to resolve the MAC to IP relationship. The ARP command is used to display the current ARP entries as well as gives the ability to both statically add and delete ARP relationships. The following shows an example of the ARP command displaying current entries in the ARP table:

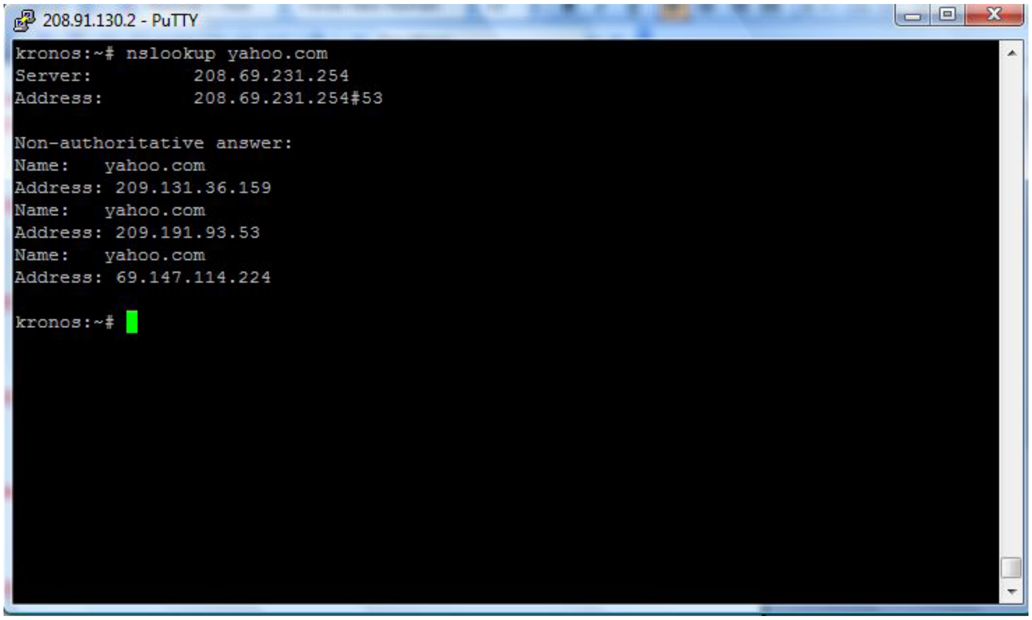


```
kronos:~# arp -a
? (208.91.130.1) at 00:1c:57:bf:c7:ff [ether] on eth1
kronos:~#
```

Figure 36 - arp command

NSlookup

The nslookup utility is used to lookup information on the DNS servers. By default, the nslookup utility will lookup this information on the machines configured DNS servers. It is possible however to query specific DNS servers with this utility as well. The following figure shows an example of the nslookup utility in use to find the DNS server information about the yahoo.com domain:

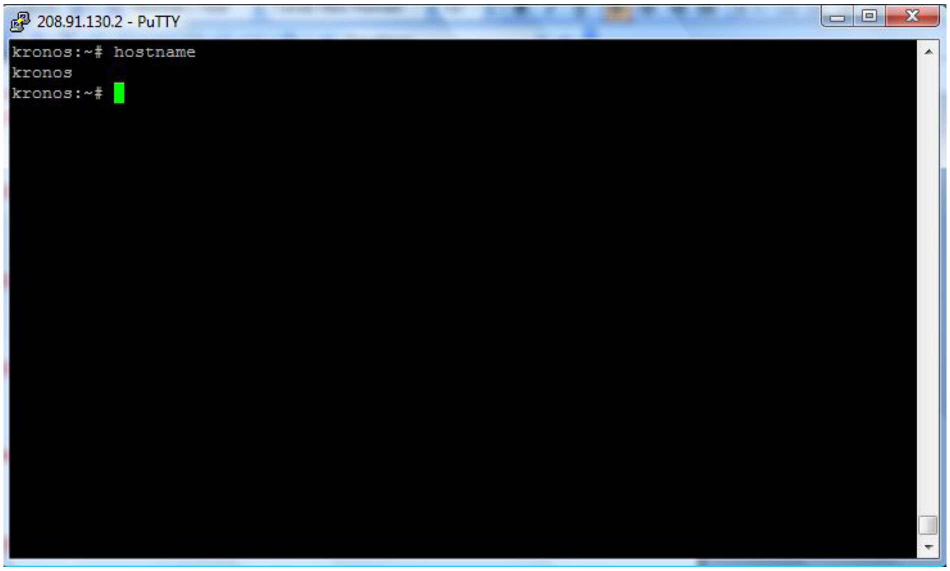


```
kronos:~# nslookup yahoo.com
Server:         208.69.231.254
Address:        208.69.231.254#53

Non-authoritative answer:
Name:   yahoo.com
Address: 209.131.36.159
Name:   yahoo.com
Address: 209.191.93.53
Name:   yahoo.com
Address: 69.147.114.224

kronos:~#
```

Figure 37 - nslookup utility

Hostname

The hostname utility is used to display the currently configured hostname of the current system. The following shows an example of the hostname utility:

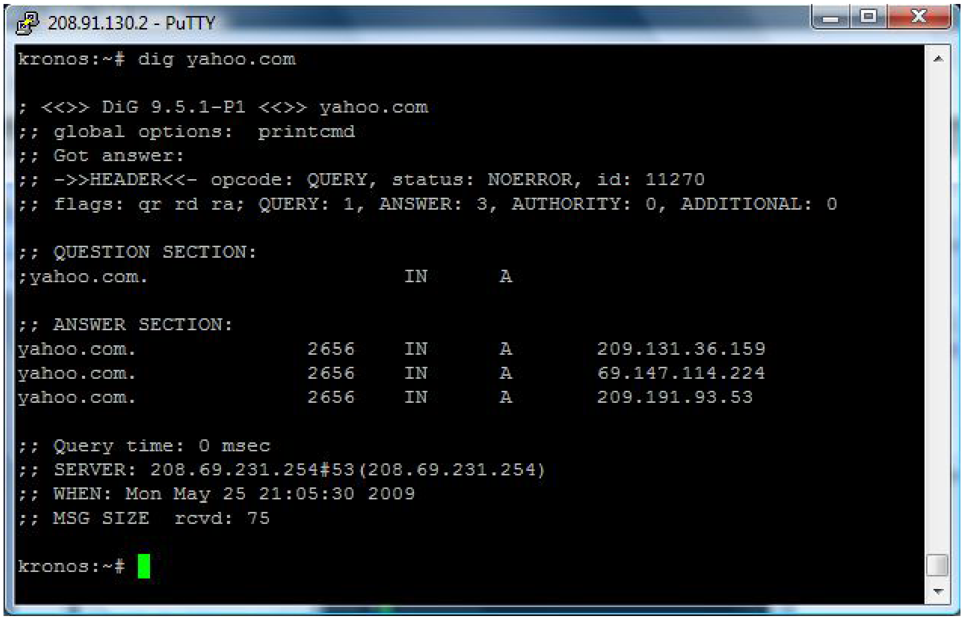


```
kronos:~# hostname
kronos
kronos:~#
```

Figure 38 - hostname utility

Dig

The Domain Information Groper (dig) utility is used to lookup DNS information. The dig utility allows a wider variety of options that the nslookup utility. The following shows an example of the dig utility:

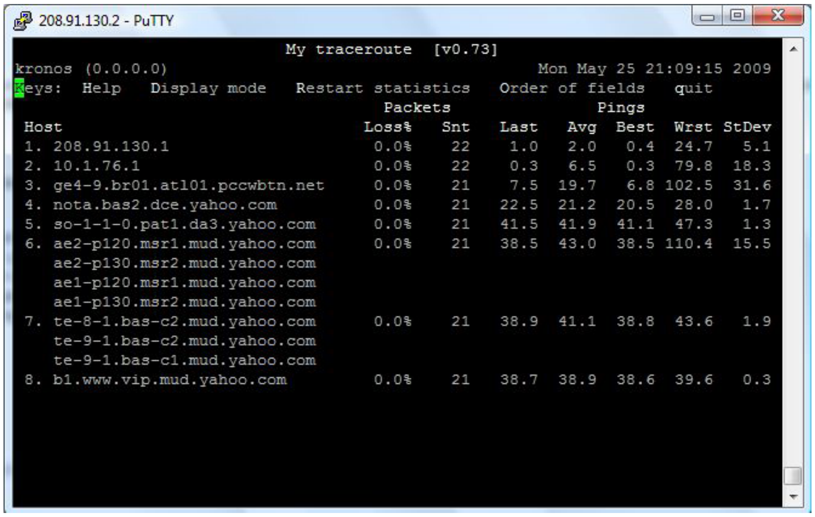


```
kronos:~# dig yahoo.com

; <<>> DiG 9.5.1-P1 <<>> yahoo.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11270
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              2656    IN      A       209.131.36.159
yahoo.com.              2656    IN      A       69.147.114.224
yahoo.com.              2656    IN      A       209.191.93.53

;; Query time: 0 msec
;; SERVER: 208.69.231.254#53(208.69.231.254)
;; WHEN: Mon May 25 21:05:30 2009
;; MSG SIZE  rcvd: 75

kronos:~#
```

Figure 39 - dig utility

Mtr

The mtr utility is a mix of the traceroute utility and the ping utility. This can be used to analyze the path to a destination continuously to find intermittent problems. The following figure shows and example of the mtg utility in use:

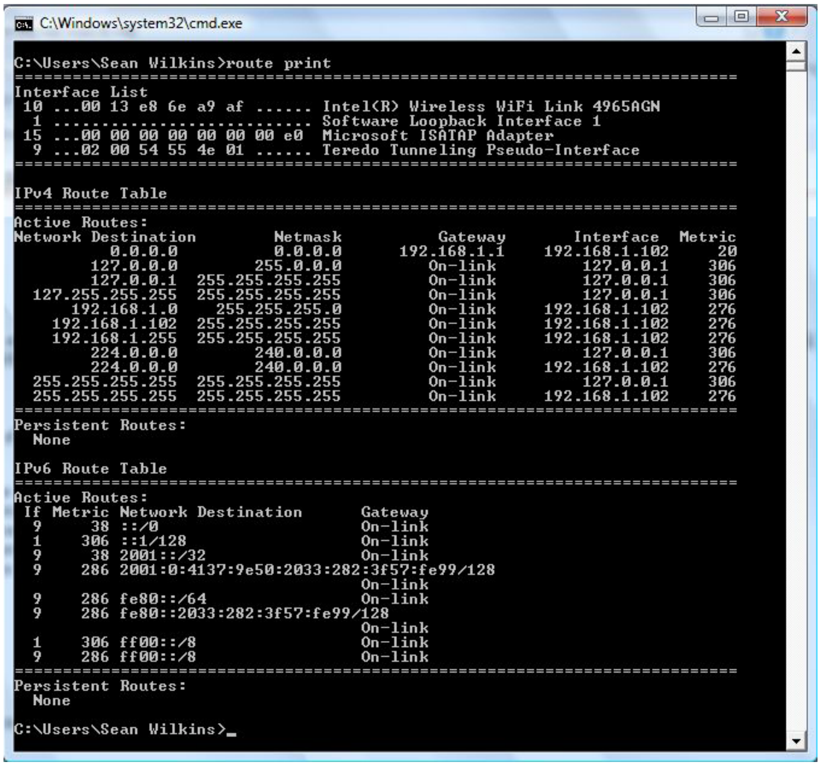


```
                             My traceroute  [v0.73]
kronos (0.0.0.0)                                   Mon May 25 21:09:15 2009
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets               Pings
 Host                                   Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 208.91.130.1                         0.0%    22    1.0   2.0   0.4  24.7   5.1
 2. 10.1.76.1                            0.0%    22    0.3   6.5   0.3  79.8  18.3
 3. ge4-9.br01.atl01.pccwbtn.net         0.0%    21    7.5  19.7   6.8 102.5  31.6
 4. nota.bas2.dce.yahoo.com              0.0%    21   22.5  21.2  20.5  28.0   1.7
 5. so-1-1-0.pat1.da3.yahoo.com          0.0%    21   41.5  41.9  41.1  47.3   1.3
 6. ae2-p120.msr1.mud.yahoo.com          0.0%    21   38.5  43.0  38.5 110.4  15.5
    ae2-p130.msr2.mud.yahoo.com
    ae1-p120.msr1.mud.yahoo.com
    ae1-p130.msr2.mud.yahoo.com
 7. te-8-1.bas-c2.mud.yahoo.com          0.0%    21   38.9  41.1  38.8  43.6   1.9
    te-9-1.bas-c2.mud.yahoo.com
    te-9-1.bas-c1.mud.yahoo.com
 8. b1.www.vip.mud.yahoo.com             0.0%    21   38.7  38.9  38.6  39.6   0.3
```

Figure 40 - mtg utility

Route

The route utility is used to add, delete and display the contents of the routing table on a device. The following figure shows an example of the display of a routing table on a device:

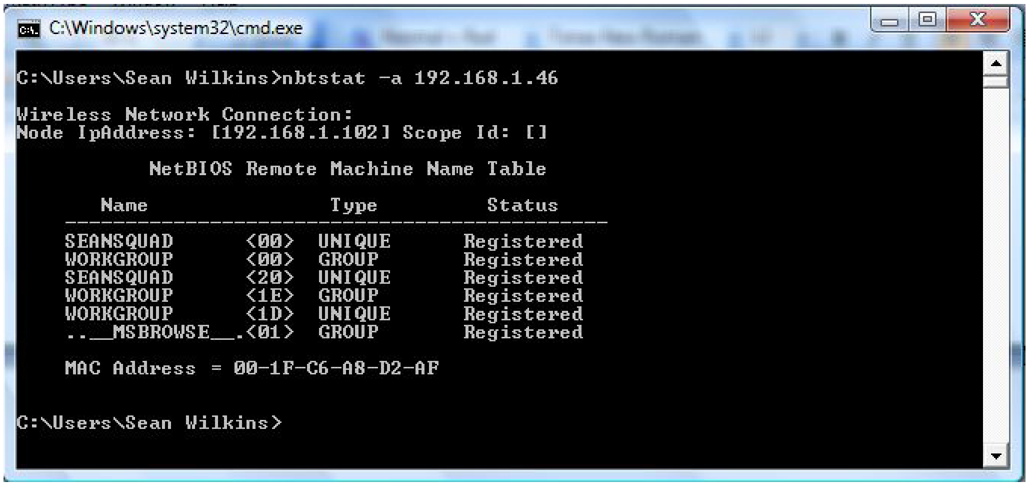


```
C:\Users\Sean Wilkins>route print
===========================================================================
Interface List
 10 ...00 13 e8 6e a9 af ...... Intel(R) Wireless WiFi Link 4965AGN
  1 ........................... Software Loopback Interface 1
 15 ...00 00 00 00 00 00 00 e0  Microsoft ISATAP Adapter
  9 ...02 00 54 55 4e 01 ...... Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.102     20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link     192.168.1.102    276
    192.168.1.102  255.255.255.255         On-link     192.168.1.102    276
    192.168.1.255  255.255.255.255         On-link     192.168.1.102    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.1.102    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.1.102    276
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9     38 ::/0                     On-link
  1    306 ::1/128                  On-link
  9     38 2001::/32                On-link
  9    286 2001:0:4137:9e50:2033:282:3f57:fe99/128
                                    On-link
  9    286 fe80::/64                On-link
  9    286 fe80::2033:282:3f57:fe99/128
                                    On-link
  1    306 ff00::/8                 On-link
  9    286 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\Sean Wilkins>_
```

Figure 41 - route utility

NBTstat

The nbtstat utility is used to display information which is used with Netbios over TCP/IP. The following figure shows the nbtstat being used to query the information from another computer:

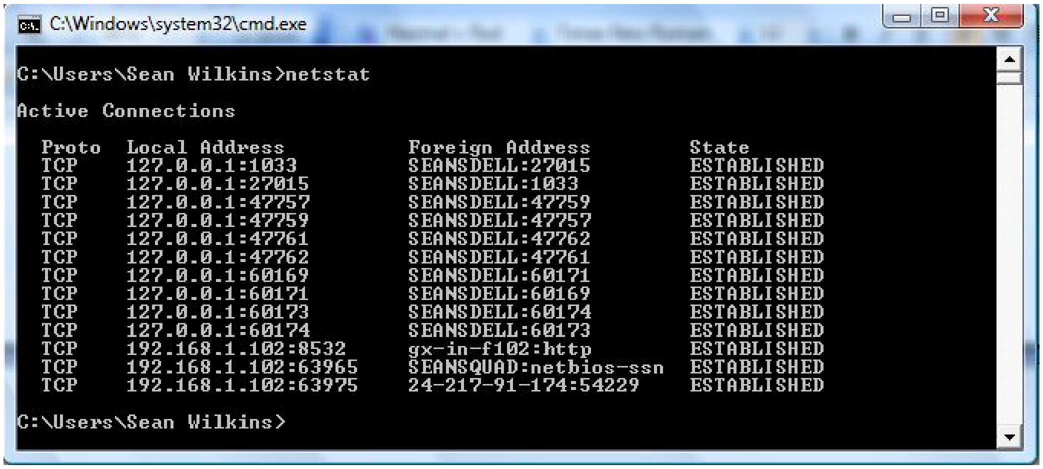


```
C:\Users\Sean Wilkins>nbtstat -a 192.168.1.46

Wireless Network Connection:
Node IpAddress: [192.168.1.102] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SEANSQUAD      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    SEANSQUAD      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 00-1F-C6-A8-D2-AF


C:\Users\Sean Wilkins>
```

Figure 42 - nbtstat utility

Netstat

The netstat utility is used to display the current IP ports which are being listened for and which ones are currently in use. The following figure shows the netstat utility used to display the currently listening ports on the device:



```
C:\Users\Sean Wilkins>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1033         SEANSDELL:27015        ESTABLISHED
  TCP    127.0.0.1:27015        SEANSDELL:1033         ESTABLISHED
  TCP    127.0.0.1:47757        SEANSDELL:47759        ESTABLISHED
  TCP    127.0.0.1:47759        SEANSDELL:47757        ESTABLISHED
  TCP    127.0.0.1:47761        SEANSDELL:47762        ESTABLISHED
  TCP    127.0.0.1:47762        SEANSDELL:47761        ESTABLISHED
  TCP    127.0.0.1:60169        SEANSDELL:60171        ESTABLISHED
  TCP    127.0.0.1:60171        SEANSDELL:60169        ESTABLISHED
  TCP    127.0.0.1:60173        SEANSDELL:60174        ESTABLISHED
  TCP    127.0.0.1:60174        SEANSDELL:60173        ESTABLISHED
  TCP    192.168.1.102:8532     gx-in-f102:http        ESTABLISHED
  TCP    192.168.1.102:63965    SEANSQUAD:netbios-ssn  ESTABLISHED
  TCP    192.168.1.102:63975    24-217-91-174:54229    ESTABLISHED

C:\Users\Sean Wilkins>
```

Figure 43 - netstat utility

5.2 Explain the Purpose of Network Scanners

Packet Sniffers

Packet sniffers or packet monitoring tools are used to watch the traffic which both enters and exits the computer which is running the software. These utilities are important when you are trying to troubleshoot complex problems which are hard to diagnose with conventional tools.

Intrusion Detection Software

Intrusion detection software is used on devices to keep track of potential intrusion into the system. Intrusion detection software works by analyzing a copy of the traffic coming into a device. If any potential intrusions are detected an action is taken depending on configuration.

Intrusion Prevention Software

Intrusion prevention software is a little different then detection software as it actively analyzes traffic coming into the device before the device receives it. If any potential attack is detected then the suspect traffic is dropped. What other actions that can be taken at this point vary, from nothing to reporting the offending address to an administrator.

Port Scanners

Port scanner software is used to detect potential holes in the security of devices. This is done through a number of different techniques which probe both TCP and UDP ports on a device. Depending on which ports are open they could potentially pose a security threat to the device.

5.3 Given a Scenario, Utilize the Appropriate Hardware Tools

Cable Testers

A cable tester is used to test the continuity on UTP and STP cable media and can also test fiber cables. The tester has the ability to check the four pairs of twisted pair wire conductors for continuity and correct polarity. Media testers only test the media cable. They cannot be used on active networks connected to a switch. Optical testers have the ability to measure the optical wavelengths allowed through a cable and check for optical loss over the length of the cable.

Modern cable testers come in many varieties from the most simple continuity tester to a complex tester which measures correct voltage, impedance and current on copper media and measures loss, dispersion and other optical characteristics on optical media.

Protocol Analyzer

A Protocol analyzer looks a lot like a packet sniffer in that it records the traffic which comes into a specific port. The difference is in the analysis; a protocol analyzer is designed to take a granular look at specific protocols. This can include sequencing analysis, delay, delay variation, conversation analysis, VoIP stream analysis and many other analysis capabilities depending on the specific equipment used.

Certifiers

A certification tester is used to measure the characteristics in a network to ensure proper adhesion to published standards. This includes everything from cable certification (CAT 5e, CAT 6) to delay certification for VoIP implementations. These testers are not meant for the small environments because they are quite costly.

TDR

A Time-Domain Reflectometer (TDR) is a tool which is used to find problems with cabling. When using a TDR on copper media a signal is sent across the wire, once this is done the device listens to see if any part of the signal is reflected back. Under normal circumstances this type of testing can be done either with an open cable (no connection at the end) or with a terminated cable (which absorbs the signal). If a reflection of the signal is received on the transmitting end then a cable problem exists. These devices can be used to measure how far into a cable run a specific problem is found in order to make troubleshooting easier. These devices have the capability to find everything from cable shorts to cable taps.

OTDR

A TDR can also be used on optical media, when used in this way an optical signal is generated and measures either at the far end or through a simple far end loop back. This way the receiving device can measure the characteristics of the incoming signal to determine potential cable issues.

Multimeter

One of the most known of networking tools is a multimeter. A multimeter is used to measure a number of different things including voltage, current, and impedance among others. These can be used for a number of different purposes from voltage checking on device power supplies to simple cable fault detection.

Toner Probe

A toner probe is used to troubleshoot network installations. It is usually used along with a probe that traces the signal emitted from a tone generator. The tone generator and probe are used to verify cable continuity, identify wiring faults, and determine line polarity and voltage in networks. The probe is equipped with a tone amplifier and an LED indicator that detects audible frequency tones for accurate tracing and identification of wires. It can be used on ACTIVE Ethernet cables with the Link Indicator. This probe is a good tool to use on active networks for finding cable at a punch down block for a particular wall jack. The following figure shows an example of a toner probe:

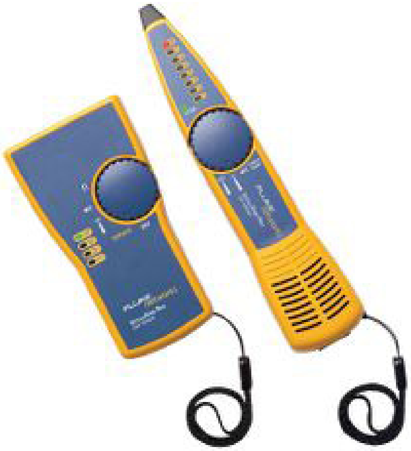


Figure 44 - Toner probe

Butt Set

A butt set is a tool which is typically used by telephone employees to tap into phone lines from a central connection point, usually using a 66 or 110 block as a clip on point. They can be used as a normal phone with many capabilities including speaker phone, tone and pulse dialing, and several other measuring abilities depending on the style of test set. The follow figure shows an example of a butt set:

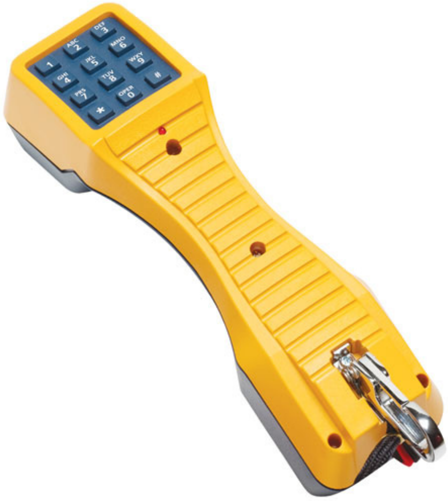


Figure 45 - butt set

Punch Down Tool

A punch down tool is used to connect cables to a connection point. The typical connection is a 66 or 110 type of connection. The following figure shows an example of a punch down tool.

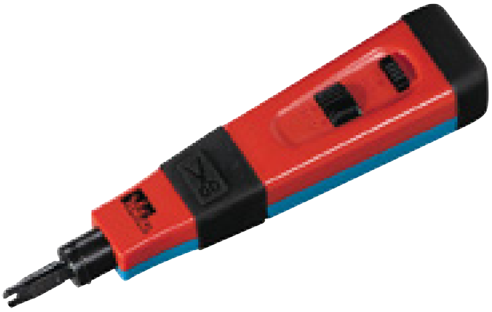


Figure 46 – punch down tool

Cable Stripper

A cable stripper is a simple tool which is used to remove the outer jacket of a cable. Typically this jacket is made of some type of plastic. The following figure shows an example of a wire stripper:

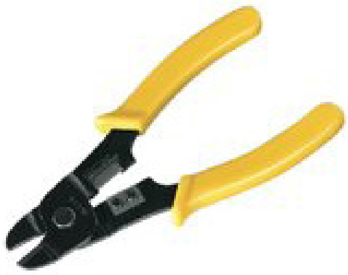


Figure 47 - Wire stripper

Snips

Snips can be used to define a number of different tools; all of these typically are used for cutting wire. In the telecommunications world the most common type of snip used is electrician's scissors. The following figure shows an example of what snips look like:

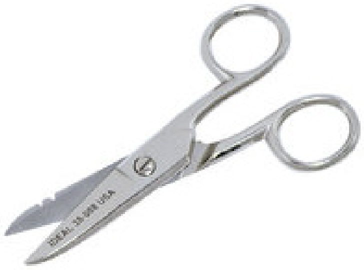


Figure 48 - Snips

Voltage Event Recorder

A voltage event recorder is used to track the continuous status of a provided voltage. The recorder will track different events which happen to the voltage level; these events include over or under voltage and voltage loss among other events. Many of today's consumer power system provide some level of voltage alerts, however higher end systems which can be obtained provide a much higher level of monitoring granularity.

Temperature Monitor

A temperature monitor is a device which keeps track of the temperature of a number of devices and the overall ambient temperature of the overall environment. This is then used to affect how the environment is heated or cooled to make sure each device is run at its most optimal temperature. If this is not done or it is not possible devices will have a more limited life as the changes in temperature greatly affect the electronics.

6.0 Network Security

6.1 Explain the function of hardware and software security devices

Network Based Firewall

A network based firewall is intended to protect a group of machines within a network. The purpose of the firewall is to block traffic from reaching devices inside the network. The firewall is configured to only allow traffic to enter devices inside the network on specific ports or for specific services. A network based firewall is run on separate hardware inline with the connection going outside the network.

Host Based Firewall

A host based firewall provides the same functionality but only for a specific host. Host based firewalls are not quite as secure as network based solutions because the end device does have to process the traffic which leaves an opening for potential threats.

IDS

Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) both are used for similar functions. Both are meant to detect a network attack. A network detection system is passive, meaning that they are forwarded a copy of all traffic and watch for attacks to happen. An IDS is intended to respond to an attack that it detects but the end system may have already been affected in some way.

IPS

An intrusion protection system is active, meaning that it sits directly in-line with network traffic and watches traffic as it physically come in. An IPS is more secure because it has the ability to block an attack before the end system is affected at all. However, the disadvantage of an IPS is that it does require that all traffic go through it which potentially creates a bottleneck for network traffic.

VPN Concentrator

A Virtual Private Network (VPN) concentrator is a device which is used as a hub to several spoke remote VPN's. Typically the VPN concentrator is housed at a central location and terminates a number of different types of endpoint. Traditionally the VPN concentrator has been used to centrally provide access to remote users into the corporate network. As broadband becomes cheaper VPN's concentrators are also used to terminate VPN's from remote offices as a cheap alternative to private lines.

6.2 Explain Common Features of a Firewall

Application Layer vs. Network Layer

A network-layer firewall only uses the information which can be obtained through data at the transport layer (Yes, this is confusing) and below. This includes the source and destination IP address, protocol and source and destination port numbers. This type of firewall is good but can be vulnerable to a number of different attacks because it is not aware of the specific of the specific traffic session and what exactly is happening with the traffic.

An application-layer firewall adds the ability to monitor not only the above information but also several other pieces of information which are available over the transport layer. This includes everything from cookies, Meta information, specific protocol information, session data, among other things. This more in depth knowledge of these higher levels of data give an application-layer firewall the advantage. The problem that can happen when processing this amount of data is time and resources. Because an application-layer firewall processes several different pieces of information as it comes into the device it requires a great amount of processing and memory resources which can slow down the speed of traffic interpretation.

Stateful vs. Stateless

A stateless firewall blocks and permits traffic strictly based on the associated rules without consideration for existing traffic sessions. For example, when connecting to an outside device a connection is initiated to that device and a return traffic flow returns. If that returning traffic does not come back into a port which is permitted it will be dropped regardless of the status of the session.

A stateful firewall works by keeping track of traffic sessions. If a connection is initiated to an outside device the stateful firewall will track and allow traffic which returns in response to that traffic, pending that it returns on the destination port which was requested by the originating device. This type of firewall is much more functional because many different protocols do not use static port assignments for return traffic. The port assignments are made on-the-fly by the originating device. A good example of this is passive FTP sessions, with passive FTP sessions the server port used for the origination of data transfer traffic is dynamically chosen by the server for each session. When this happens it is not possible for a stateless firewall to know this port is safe and it will block traffic coming from it. In active FTP mode, all data transfer traffic is originated on port 20.

Scanning Services

Scanning services may be provided on some higher end firewalls. What this provides is a method of scanning the traffic for problems before it reaches the end device. This scanning can include virus, spyware and malware tests on HTTP, SMTP, and POP traffic as well as several other types of in depth scanning techniques depending on the equipment.

Content Filtering

Content filtering works hand-in-hand with scanning services to look over the content of the incoming traffic and to filter it based on a number of different techniques. These techniques include Bayesian filtering, keyword lookup, header lookup, and specific URL's to name a few.

Signature Identification

Signature identification also works hand-in-hand with these other techniques by looking for the specific signatures of viruses, worms and spyware. Many of these different threats can be caught simply by looking for a specific signature inside the scanned traffic.

Zones

A *zone* when used in a network security context refers to an area of the network with a specific trust level. Typical zones include inside, outside and DMZ. In this case the inside of the network would typically be highly trusted while the outside and DMZ zones are with not trusted or moderately trusted. The firewall can be configured to treat the traffic from different zones in different ways depending on their configured trust level.

6.3 Explain the Methods of Network Access Security

Filtering

ACL

An Access Control List (ACL) is a list of statements which either permit or deny traffic based on a number of different parameters. ACL's are typically grouped into standard or extended. With a standard ACL only the source of the traffic is used for match. An extended ACL allows many options to be used to match; these include protocol, source and destination address information and TCP or UDP port numbers when using IP. Each statement must be configured to either permit or deny the traffic and be configured in a specific direction on an interface.

Tunneling and Encryption

SSL VPN

An SSL VPN is used to establish a secure connection between an end device and a central system. An SSL VPN does this by using a SSL compliant web browser. The user can then login to a specific SSL VPN web site and authenticate. At this point the two main options are to have a VPN portal which is web based and allows access to the internal network devices; the other option is an SSL VPN tunnel which allows access to some non-web based content through an SSL tunnel via the web browser.

PPTP

PPTP is a form of encryption that provides the "tunnel" for secure connections over the Internet and is used to create a Virtual Private Network. VPN provides users with a dial-up, private, secure direct connection to a server or corporate network via the public Internet.

L2TP

L2TP was designed by the Internet Engineering Task Force (IETF) to support non-TCP/IP protocols using VPNs over the Internet. L2TP combines the best features of two tunneling protocols: PPTP (Point-to-Point Tunneling Protocol) and L2F (Layer 2 Forwarding). As the name implies, it operates at Layer 2 of the OSI Reference Model. L2TP uses packet-switched network connections; making it possible for endpoints to be located on different nodes. It supports a number of protocols, including IP and AppleTalk. L2TP is a good protocol to use when you have two non-TCP/IP networks that must have Internet access.

IPSEC

IPSec is a security protocol that provides authentication and encryption over the Internet. It operates at the Network layer and secures all packets operating in the upper OSI layers. It works with IPv4 and IPv6 and has broad Industry support. IPSec uses either Authentication Header (AH) or Encapsulating Security Payload (ESP) to ensure sender authentication and data encryption. It is most often used to secure VPN on the Internet using digital certificates sent from the server to authenticate the sender.

Remote Access

RAS

The RAS is installed on the server with one or more modems installed. Used for client remote access to a network.

RDP

A Windows XP/Vista/Windows 7 network client uses the RDP client SW utility to remotely connect to a network via a MS Terminal server. Using authentication to establish the connection, clients can then use the network resources such as mapped drives to run applications and printers remotely. There is also an open source RDP client called rdesktop that runs on UNIX/Linux systems allowing connections between *nix and Windows systems using RDP.

PPPoE

PPPoE uses PPP over Ethernet and it connects Ethernet LAN users to the Internet using an ASDL or cable modem. Users share the broadband connection. Phone ISPs use PPPoE with ADSL modems for consumer DSL Internet access.

PPP

Protocol used to establish an Internet connection between serial point-to-point links. PPP uses the Data Link layer of the OSI model to send TCP/IP packets to a server that connects the client on the Internet.

VNC

Virtual Network Computing (VNC) provides a method of remotely administering systems from a remote location. VNC does this by providing a remote representation of the remote systems screen and translates the mouse and keyboard actions to the remote system for processing. There are a number of different utilities which perform this function including Windows remote desktop, X Windows, TightVNC, RealVNC and UltraVNC to name a few.

ICA

Independent Computing Architecture (ICA) is an application server protocol which provides access to a common desktop environment which is run on a central system. ICA was designed so that the remote client devices would not need to be very complex as most of the hard drive and processing capabilities are run on a central server.

6.4 Explain Methods of User Authentication

PKI

Public Key Infrastructure (PKI) is a system which connects together a group of secure devices through a central public key/private key system. When using PKI each communicating user or device will obtain a public and private key; the private key is used to decrypt messages which are sent for the user or device, the public key is used to encrypt messages intended for a specific user or device. The public keys are sent to everyone a user or device wants to securely communicate with. Each key pair is certified by a Certificate Authority (CA) which verifies the identity of the user or device utilizing the key pair.

Kerberos

Kerberos is more than a strong, secure network authentication protocol. It's a full-fledged security system designed to provide strong authentication for client/server applications by using secret-key cryptography. Created at MIT, Kerberos establishes a user's identity as soon as he or she logs onto a network where Kerberos is supported. A unique key (ticket) is issued to each user after the user logs onto the network. All network messages that the user sends over the network contain this unique key used to identify the user-sender. The user identification and security credentials contained in the embedded ticket are used throughout the entire network session. The encryption used by Kerberos is freely available. The source code can also be downloaded via the Internet. The Windows 2000 family, Windows XP, Windows Server 2003, UNIX, Novell, and Linux all support Kerberos.

AAA

Authentication, Authorization and Accounting (AAA) is a security model which is utilized by administrators and network designers so that their devices are kept the most secure. The authentication portion of the model covers user and device authentication to use certain devices and/or resources. The authorization portion of the model covers specific permissions to perform individual tasks on a device and the accounting portion of the model covers how these different tasks are logged for future review.

RADIUS

RADIUS is an industry standard authentication protocol that provides authentication, authorization, and accounting services. A RADIUS client such as a dial-up server, RADIUS Proxy server, or VPN server sends user name, password, and connection information in a RADIUS message to a RADIUS server. The RADIUS server sends a RADIUS message response that authorizes and authenticates the RADIUS client.

TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) is an AAA protocol similar to RADIUS. TACACS+ is mainly used on Cisco devices and provides similar functionality to RADIUS. The two differ in a couple of areas; mainly that TACACS+ separates authentication, authorization, and accounting while RADIUS combines authentication and authorization and that TACACS+ uses TCP and RADIUS uses UDP.

Network Access Control

802.1x

The IEEE 802.1x standard includes a method for passing the Extensible Authentication Protocol (EAP) over both wired and wireless networks. EAP provides authentication services for wireless networks not using PPP.

CHAP

CHAP is an authentication protocol that uses a hashed algorithm called Message Digest 5 (MD5) S that provides client response encryption. Remote Access Service servers, some Network Access servers, and some Proxy servers support using CHAP. CHAP is supported on PPP connections and requires authentication not only when initially making the connection, but also during the session. Failure to authenticate will result in the session being ended. CHAP is a weak, one-way authentication protocol.

MS-CHAP

MS-CHAP v1 offers more security than CHAP and is an authentication protocol that uses a challenge handshake process. A Remote Access Server sends a challenge to the remote client. The remote access client sends back a response containing the user name and a non-reversible, encrypted password challenge string. The RAS checks the response determining its validity and, if valid, authenticates the user. Microsoft CHAP v1 is supported on Windows NT4 Server, Windows 2000 Server, and Windows Servers 2003.

MS-CHAP v2 is an authentication protocol that offers stronger security than MS-CHAP v1 by providing mutual authentication. Using two-way or mutual authentication, the client's user name and password are validated by the RAS. The Windows 2000 family, Windows XP, and Windows Server 2003 all support using MS-CHAP v2. Note that MS-CHAP, Version 2 authentication is not compatible with MS-CHAP, version 1.

EAP (Extensible Authentication Protocol)

EAP is a general protocol that provides support for several different authentication protocols such as EAP-TLS (EAP-Transport Level Security), MS-CHAP, Kerberos, certificates, public key authentication, and smart cards. It is often used by wireless devices to connect to a RADIUS authenticator server. A wireless client requests a WAN connection from an AP, which requests the identity of the user and transmits the user's identity to an authentication server such as RADIUS. The RADIUS server asks the AP for proof of identity, gets it, and sends it back to the server.

EAP-TLS uses certificates for user authentication such as smart cards. Smart cards are often used with laptop and notebook PCs to provide remote access authentication. EAP-TLS provides mutual authentication, negotiation of encryption type, and is the strongest authentication protocol method.

6.5 Explain Issues that Affect Device Security

Physical Security

One of the things which should always be kept in mind is that any device loses all of its fancy logical security if it is physically vulnerable. One thing that must be paid close attention to is the physical security of the equipment, as many different devices are configured with methods of access without proper passwords when physical access it possible. When this access is given other problems also can exist if someone was to install tapping equipment inline with the equipment or to reroute existing cables.

Restricting Local and Remote Access

When it comes to network and device access control it is very important to keep a tight reign on these possible access points; when configuring local access it is vital to make sure that only users with administrative privileges can access servers from the local consoles. When configuring remote access it is best to make sure that access is only provided to those users who require it and to disable remote access to everyone else. There are a couple of main principles which should be followed when it comes to access-control. These include:

- Utilizing implicit denies in all rule creation: this way if access is not specifically given it is implicitly denied.
- Follow a least privileged model: All access which is given should be given based on the lowest privileges which are given. For example, if a group membership gives you full access but user access gives you limited access then your effective permissions would be limited.
- Separate Administrative duties: This way administrative privilege is only given to aspects of the network which are used by that specific administrator.
- Cross-Train Administrators: This way if one administrator is unavailable for whatever reason there is another administrator who can deal with any issues.

Secure Methods vs. Unsecure Methods

SSH, HTTPS, SNMPv3, SFTP, SCP

One of the things that should be well known to any administrator is which protocols are safe and secure and which ones are not. Based on this knowledge the selection, different protocols can be chosen for specific application depending on what the specific circumstances are. All of the protocols listed in the heading provide a secure method of exchanging communications between both ends of the connection. All of them could potentially be used over an unsecure network if necessary.

TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2

On the flip side are the protocols listed in the heading of this section, these different protocols do not provide a secure method of communications between both ends of the connection. Use great caution when using these protocols as the information being transmitted between devices is in the clear and can be easily intercepted with little or no technical knowledge.

6.6 Identify Common Security Threats and Mitigation Techniques

Security Threats

DoS

Of all the different security threats one of the hardest ones to mitigate is a Denial of Service (DoS) attack. This is because it typically does not attack a specific service but just tried to make the device as busy as possible in order to limit the amount of resources which are available for normal use.

Viruses

Viruses are some of the most well known of security threats, this is because the influence of their damage is wider spread and more visible to the common user. There are a number of different things which a virus can do to a system; generally there are no real bounds. Since a virus requires some action on the part of a user they can be prevented easier but provide a higher level of access then some other forms of attack.

Worms

A worm differs from a virus in that it does not need to be initiated by a user. When infected with a worm the consequences tend to be higher than viruses because they are built to propagate themselves in such a way that many different insecure systems can be affected in a short amount of time over a variety of different networking technologies.

Attackers

The number of different types of attackers is as diverse as the number of fish in the sea. Everybody from a seasoned security engineer to a 10 year old playing on their home computer have the ability to attack. A trusting administrator does not stay an administrator for that long.

Man in the Middle

A man in the middle attack works by trying to trick both sides of a given connection to relay their traffic through an infected device. There are a number of different methods for doing this including ARP poisoning and host file infection.

Smurf

A smurf attack does not involve a number of different blue characters dancing across the screen! In all seriousness a smurf attack is a type of DoS attack which tricks a remote device into flooding another remote device. This is done by an attacker hijacking an IP address of the first remote device; once this is done the attacker will send a ping packet out to the broadcast address of a subnet. In turn the router on the subnet will send the ping out to all devices on the subnet which results in all the hosts sending a ping reply back towards the router.

Rogue Access Points

A rouge access point is an access point which is put in range of a valid network in order to get valid clients to connect and share their information. This is one of the major risks of running a wireless network, by getting clients to connect to the rouge access point it completely gets past one level of security which exists with physical networks.

Social Engineering (phishing)

What this involves is the collection of information through the imitation of a person or device which is legitimate. When dealing with people directly this involves a potential attacker calling a person and pretending to be an employee of a company which does business with the person; this relationship tends to equate a level of trust with the person and can be used to gain access to information which would not be possible if contacted as a stranger. When dealing with a device performing a similar function it is called phishing, what this entails is the use of a media which is used to imitate the look and feel of a legitimate business (email or web site). Typically, these types of attacks use common bank or large scale businesses to imitate and attempt to get the target to enter personal information in order for the attacker to use for their own purposes.

Mitigation Techniques

Policies and Procedures

A clear and concise policies and procedures document should be made available to all users so that they have a proper method of dealing with specific situations. This includes everything from how to form passwords to correct remote access procedures.

On the administrative side this includes a standard for providing privileges to users and devices, how to add, change or delete users and computers on the network, auditing procedures, and many other directives to be followed which will make the life of an administrator easier.

User Training

There is nothing more affective in keeping a system safe then having well trained users. If the users are aware of why the different policies and procedures have been put into place and how and why they work they are more likely to follow them and more likely to be aware of potential problems as they occur. This also provides them with the reasoning of why they are typically not permitted to install applications or other different programs on their work machines. This training also makes them aware of the different techniques which are used by potential attackers in obtaining inside information.

Patches and Updates

There is nothing more useless than a machine which is attacked when a perfectly good patch is available; As well it is also useless for a device to run an antivirus solution and not to maintain the virus database.

Always make sure to either use automatic update on products or use manual updating and monitor the available updates often. Typically when installing system patches on servers and workstations it is good to test a patch before installing it as there may be unintended consequences in a specific environment. When updating virus or spyware definitions it is best to automatically update as the chances of a virus database update affecting a system is very low. Hot fixes which are typically released to fix only specific problems in specific circumstances should only be applied once ample testing has been performed. These types of patches are typically not meant to be installed on every system but simply meant to provide a short term solution to a specific problem. Unless the specific problem exists on your systems wait until an official service release is available.

Practice Questions

Chapter 1 Network Technologies

1. You are designing an internetwork. Due to the variety of technologies and connectivity methods in use, you need to select routing protocols that support unequal cost path load balancing. Which protocols will you select?
Select the two best answers.

❍ A. RIP v.1
❍ B. RIP v.2
❍ C. IGRP
❍ D. EIGRP
❍ E. OSPF

2. A customer is having issues with their mail server, and they utilize POP. What protocol and port number would you need to examine in the traffic stream?
Select the best answer.

❍ A. TCP, 119
❍ B. TCP, 23
❍ C. UDP, 110
❍ D. UDP, 69
❍ E. TCP, 110

3. What are the advantages of a link-state protocol over a distance-vector protocol?
Choose TWO.

❍ A. Slower convergence
❍ B. Low resource utilization
❍ C. Faster convergence
❍ D. Scalability
❍ E. Full routing table updates

Chapter 2 Network Media and Topologies

1. You have a fully meshed T1 WAN network connecting 10 LAN's from 10 locations. The link providing the best route from A to B goes down. Which of the following are true concerning this scenario?
Select the best answer.

❍ A. Traffic will reroute assuming you have a secondary route
❍ B. The WAN will go down
❍ C. Only traffic from A to B will be down
❍ D. A backup dial-on-demand link will be brought up

2. You are asked to help out a small business who is having some network issues. They have a manufacturing shop where they press metal with large, electrically powered, machines. They have computers in the shop that control the machines. Periodically, these computers seem to lose connectivity with the server, where their designs are stored. Which of the following do you recommend?
Select the best answers.

○ A. Replace their UTP with STP
○ B. Replace the UTP with fiber
○ C. Replace the switch with a router
○ D. Put a UPS on the switch

3. You are called to a customer's office where they are having trouble with their 802.11b wireless network. Sometimes it works fine and other times it does not. When you arrive, you find that they are running their network on channel 1. The neighboring office has a network on channel 2. They are using the network to surf the Internet and connect to a file/print server. What do you recommend?
Select the best answer.

○ A. Upgrade 802.11b to 802.11g to get more bandwidth
○ B. Implement Bluetooth
○ C. Change channels
○ D. Change the WAP to run in 802.11a mode to get more throughput

4. You are a consultant for a large brokerage firm that is designing a new network. They have 2 main trading sites and 10 branch offices. Redundancy is required between the main sites and for one of the branches, which serves as a secondary backup site. They are very cost-conscious. Which network topology would you recommend?

○ A. Star
○ B. Full mesh
○ C. Partial mesh
○ D. Bus

Chapter 3 Network Devices

1. What is the purpose of a redundant controller on a disk array?
Select the best answer.

○ A. So that if the network goes down, the other controller takes over.
○ B. So that power is lost on the server, the other RAID controller takes over.
○ C. So that if a disk driver goes out, the other RAID controller recovers.
○ D. So that if one RAID controller fails the redundant becomes primary.

2. What is the purpose of RAM memory in Cisco routers?
Select the three best answers.

❍ A. It is used to store run-time configuration information.
❍ B. It is used as a persistent configuration storage.
❍ C. It is used for packet buffers.
❍ D. It is used by running processes.
❍ E. RAM is used as a persistent IOS storage.

3. What information is included in BPDUs sent by bridges and switches as part of their STP operations?
Select the four best answers.

❍ A. Values for the hello, forward delay, and max-age protocol timers
❍ B. The bridge ID of the sending switch
❍ C. The spanning-tree path cost to the root
❍ D. Its DNS name
❍ E. The ID of the root bridge

Chapter 4 Network Management

1. Which of the following is the correct IP address range for the first octet of the class B IP address range, assuming you are using classful networking?
Select the best answer.

❍ A. 1-127.x.x.x
❍ B. 128-191.x.x.x
❍ C. 192-223.x.x.x
❍ D. 191-223.x.x.x
❍ E. 192-224.x.x.x

2. You connect a new PC to a switch. Other devices are working through the switch, but the new PC does not connect to the network. You have an APIPA address on your NIC. You do have a link light on the switch. You do a release/renew on another PC and they get an APIPA address too. Yet, other PC's, who have addresses, are continually able to access the network. What is the first thing you should check?
Select the best answer.

❍ A. If the switch is powered on
❍ B. If you have a link light on the switch
❍ C. If your Internet connection is up
❍ D. If you have a bad or incorrect cable type
❍ E. If the DHCP server is down

3. Given the following scenario, what is the next recommended course of action? A user contacts you with a network issue. By talking with them, you learn about the problem and possible causes. You find out where the problem is occurring and see if anything may have recently changed. You think that you know what the most likely cause of the problem is.
Select the best answer.

❍ A. Identify symptoms and potential causes
❍ B. Establish what has changed
❍ C. Select the most probable cause
❍ D. Implement the action plan and solution
❍ E. Identify the results and effects of the solution
❍ F. Document the solution

4. Given the following scenario, what is the next recommended course of action?
A customer calls you, needing help with their network. You find out their problem, come up with a fix and it works. What do you need to do now?
Select the best answer.

❍ A. Identify symptoms and potential causes
❍ B. Establish what has changed
❍ C. Select the most probable cause
❍ D. Implement the action plan and solution
❍ E. Identify the results and effects of the solution
❍ F. Document the solution

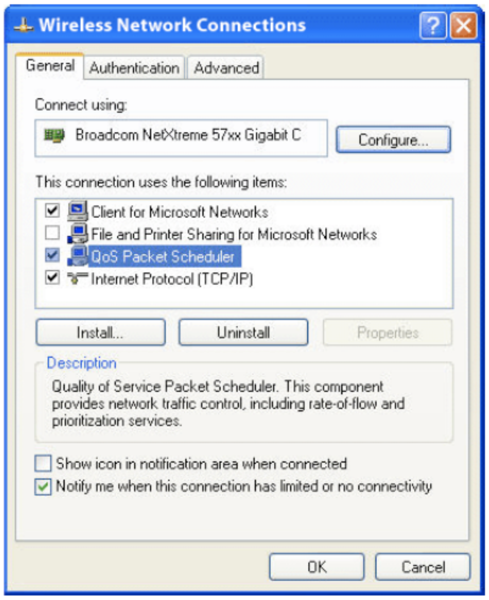
5. Which of the following addresses is a APIPA address?
Select the best answer.

❍ A. 169.254.10.192
❍ B. 169.168.10.10
❍ C. 172.16.10.10
❍ D. 192.168.1.1
❍ E. 168.169.254.1

6. Take a look at the attached exhibits. The exhibit shows part of the network configuration for this laptop. Other computers on the wireless LAN cannot access a share on this laptop. What is the problem? Select the best answer.

- ○ A. File and print sharing is disabled
- ○ B. File and print sharing is enabled
- ○ C. The computer is set to receive a dynamic DHCP IP address and it must have a static IP address to share files
- ○ D. The QoS packet scheduler is enabled
- ○ E. File sharing does not work over a wireless NIC

Exhibit(s):



Wireless Network Connections

Connect using:

Broadcom NetXtreme 57xx Gigabit C

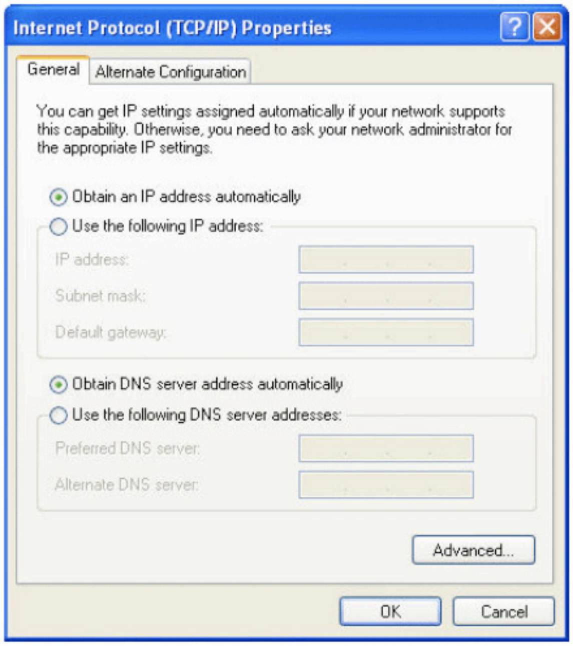
This connection uses the following items:

- ☑ Client for Microsoft Networks
- □ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Quality of Service Packet Scheduler. This component provides network traffic control, including rate-of-flow and prioritization services.

- □ Show icon in notification area when connected
- ☑ Notify me when this connection has limited or no connectivity



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

7. After receiving a tech-support call and testing your solution, what else do you still need to do? Select the best answers.

○ A. Check to see if it worked
○ B. Document
○ C. Find the most probable cause
○ D. See if anything has changed
○ E. See what, if anything, it has affected

Chapter 5 Network Tools

1. What command and associated switches created the following output?

```
Active Connections
Proto Local Address Foreign Address State PID
TCP mynb100:4097 64.233.161.147:http ESTABLISHED 3236
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\WININET.dll
[iexplore.exe]
```

Select the best answer.

○ A. Netstat -vb
○ B. Nbtstat -v
○ C. Nslookup -s
○ D. Netstat -a

2. You are running Windows XP on your home PC. You enable Terminal Services and want to access your PC remotely, using this feature. You try it from your laptop while traveling, but you can't get to your PC's IP address: 10.0.0.2. What is the problem? Select the best answers.

○ A. You need NAT forwarding
○ B. Terminal Services doesn't work over the Internet
○ C. You need to buy a license to use this feature
○ D. You need to use your router's WAN IP
○ E. You need to use your router's LAN IP instead

3. Which statements about half- and full-duplex are true? Choose THREE.

○ A. Half-duplex transmissions are prone to collisions.
○ B. All network devices support both transmission modes.
○ C. Hub-based networks must use half-duplex mode in order to detect collisions.
○ D. Full-duplex links have their collision detect circuits disabled.
○ E. Half-duplex mode allows 100% efficiency over Ethernet.

Chapter 6 Network Security

1. You have encryption enabled on one side of your link, but not on the other. What will be the result? Select the best answer.

❍ A. Communications will work fine.
❍ B. You will have one way communications.
❍ C. You will have no communications.
❍ D. This is not possible. When you configure encryption, it automatically configures it on both sides of the connection.

2. You have salesmen who visit your users' offices. These salesmen typically want Internet access. They have the user disconnect their PC's ethernet cable so that they can use the jack to connect to the Internet. You feel that this is a security risk because the salesman's laptop could have a virus. What feature would you enable to prevent this? Select the best answer.

❍ A. Port security
❍ B. Port blocking or filtering
❍ C. Authentication
❍ D. Encryption

3. You fear that one of the computers on your network has a worm that sends thousands of packets to all computers on the network every minute. What feature might enable on your switch to prevent or slow this down?
Select the best answer.

❍ A. Port security
❍ B. Broadcast storm control
❍ C. Authentication
❍ D. Encryption

4. Which of these are associated with a denial of service (DoS) attack?
Select the best answers.

❍ A. Attacker cuts cable to all phone & data lines going to building
❍ B. Attacker uses so much bandwidth of a company's Internet circuit that normal services are interrupted
❍ C. Using all CPU on the company's email server
❍ D. Changing the default route to go to null on core router
❍ E. Harvesting all usernames and passwords

5. What is the difference between WPA 1 and 2?
Select the best answer.

❍ A. WPA 1 can only use TKIP encryption.
❍ B. WPA 2 supports the AES cipher, and WPA 1 does not.
❍ C. WPA 2 has improvements in the information elements within frames.
❍ D. WPA 1 is only appropriate for the small office environment.

Answers & Explanations

Chapter 1

1. Answers: C, D

Explanation A. RIP v. 1 only supports equal cost path load balancing on 4 ports by default. However, RIP v.1 can be configured to support up to 6 equal paths for load balancing.

Explanation B. RIP v. 2 only supports equal cost path load balancing on 4 ports by default. However, RIP v.2 can be configured to support up to 6 equal paths for load balancing.

Explanation C. Both IGRP and EIGRP support unequal cost path load balancing. In other words, a router configured for some of these routing protocols is able to install more than a single "best" path to the destination.

Explanation D. Both IGRP and EIGRP support unequal cost path load balancing. In other words, a router configured for some of these routing protocols is able to install more than a single "best" path to the destination.

Explanation E. OPSF only supports equal cost path load balancing, over 4 paths by default, with the possibility to configure 6 equal cost paths.

2. Answer: E

Explanation A. TCP port 119 is the Network News Transfer Protocol.

Explanation B. TCP port 23 is the Telnet port.

Explanation C. 110 is the POP port number, but it operates on TCP.

Explanation D. UDP port 69 is utilized by TFTP.

Explanation E. TCP port 110 is utilized by POP.

3. Answers: C, D

Explanation A. Link-state protocols are known for their fast convergence time.

Explanation B. Link-state algorithms place a high load on the device CPU, and can have very poor performance in unstable networks.

Explanation C. Link-state protocols have much faster convergence times than distance-vector protocols.

Explanation D. Link-state protocols are built to scale, and can handle very large networks, if implemented properly. Once the topology is built, only periodic updates are sent to keep the routing table current.

Explanation E. Link-state protocols are very efficient, and only pass required link information to other devices.

Chapter 2

1. Answer: A

Explanation A. Because this is a fully meshed network, all locations have a link to all other locations. By having that link, they should also have routes. Routing protocols compare the routes and choose the best route. When the best route went away, the secondary route will come up.

Explanation B. The WAN won't go down because this is a fully meshed network where all hosts have a direct connection to all other hosts.

Explanation C. Traffic from A to B will go down, but the network should have a secondary route to be able to reroute the traffic. This answer is true, but the outage should be momentarily.

Explanation D. The scenario did not mention any sort of dial-on-demand (dial up) link.

2.Answers: A, B, D

Explanation A. Their unshielded twisted pair (UTP) cable is probably getting interference from the electrical motors in the shop. By replacing it with shielded twisted pair (STP), they may be able to prevent this interference.

Explanation B. Their unshielded twisted pair (UTP) cable is probably getting interference from the electrical motors in the shop. By replacing it with fiber optic cabling, they will be able to prevent this interference.

Explanation C. You cannot simply replace a switch with a router. These devices have different purposes and there is nothing wrong with using a switch in the scenario described.

Explanation D. It is possible that the switch is losing power. By connecting a UPS to power the switch, you may prevent the switch from losing power as well as the PC's from losing network connectivity.

3. Answer: C

Explanation A. There is nothing in the question that indicates that they need more bandwidth.

Explanation B. Bluetooth is a wireless specification for short-range, low-power devices and has little to do with the kind of networking 802.11b wireless networks engage in. Implementing Bluetooth would neither hurt nor help the customer, in this case.

Explanation C. With 802.11b and 802.11g wireless networks, it is commonly recommended to only use channels 1, 6, and 11 so that different wireless networks don't overlap and interfere with each other.

Explanation D. You cannot just change the wireless access point (WAP) without changing wireless network cards as well. Also, there is no issue stated with the throughput of the wireless network.

4. Answer: C

Explanation A. The star topology is also called "hub and spoke." All traffic must pass through the central hub. Star topologies do not provide any redundancy.

Explanation B. A mesh topology provides redundant links, and provides multiple paths to reach a destination. Even if a link fails, there is an alternate path. However, this topology is very expensive.

Explanation C. A partial mesh provides for limited redundancy at certain locations. This ensures that high priority sites have the required redundancy, and it does not have the high cost of the full mesh.

Explanation D. Incorrect. The bus topology is an older technology where network nodes are attached to coaxial cable along the wire strand.

Chapter 3

1. Answer: D

Explanation A. RAID controllers on a disk array are not related to the network.

Explanation B. A redundant RAID controller doesn't have to do with power. This is notthe best answer.

Explanation C. A redundant RAID controller would not help if a disk driver went out.

Explanation D. The purpose of having a redundant RAID controller is so that if one RAID controller fails the redundant becomes primary (the redundant controller takes over).

2. Answers: A, C, D

Explanation A. The running-config configuration file is stored in RAM. As RAM is a volatile storage area, running-config needs to be saved to NVRAM if you want to make it persistent.

Explanation B. The running-config configuration file is stored in RAM. As RAM is a volatile storage, running-config needs to be saved to NVRAM if you want to make it persistent.

Explanation C. A portion of RAM is reserved for packet buffers. Packets that need to be processed and switched are stored temporarily in RAM.

Explanation D. RAM is used by the running IOS image (on most platforms) and for processes that run on the router, as well as for their data structures.

Explanation E. RAM is volatile, and is not used as a persistent IOS storage. Flash is typically used as a persistent storage for IOS images.

3. Answers: A, B, C, E

Explanation A. This important information allows switches to discover each other on the network, as well as to detect when a switch/bridge failure occurs.

Explanation B. This information is important because each switch/bridge needs to have a unique way to identify neighbor devices and their knowledge of the STP topology.

Explanation C. Each switch/bridge informs its neighbor about its proximity to the root bridge/switch. Based on this information, other switches (from lower levels) will calculate per port distance to the root bridge to determine which ports must be disabled.

Explanation D. Switches don't care about DNS names, and don't send this kind of information in BPDUs. DNS operates on layers 5-7 (from session to application layer).

Explanation E. Each switch needs to inform its neighbors about the switch that it considers a root bridge in the STP topology.

Chapter 4

1. Answer: B

Explanation A. This is the correct range for the first octet of the class A IP address range.

Explanation B. This is the correct range for the first octet of the class B IP address range.

Explanation C. This is the correct range for the first octet of the class C IP address range.

Explanation D. This is not one of the IP address ranges. The correct range for the class B network is 192-223.x.x.x.

Explanation E. This is not one of the IP address ranges. The correct range for the class B network is 192-223.x.x.x.

2. Answer: E

Explanation A. The question stated that other devices are working through the switch, thus, the switch must be powered on.

Explanation B. The question stated that you do have a link light on the switch.

Explanation C. The question didn't say anything about the Internet. If you don't have an IP address, you will never be able to use the network, much less the Internet.

Explanation D. As you have a link light on the switch, your cable should be good. Also, other PC's that were working cannot get a DHCP address either. Therefore, it is unlikely that multiple cables suddenly went bad on the switch.

Explanation E. Because you cannot get a DHCP address, but do have a link light, check to verify that the DHCP server is up and running. You received an automatic private IP address (APIPA), meaning that your PC could not obtain a DHCP address, but was set to DHCP.

3. Answer: D

Explanation A. You have already done this while talking to the user.

Explanation B. You have already done this while talking to the user.

Explanation C. You have already done this while talking to the user.

Explanation D. Now that you think you know what the most likely cause of the problem is, you need to implement the action plan. The Network+ Recommended logical troubleshooting strategy is:

1. Identify the symptoms and potential causes
2. Identify the affected area
3. Establish what has changed
4. Select the most probable cause
5. Implement an action plan and solution including potential effects
6. Test the results
7. Identify the results and effects of the solution
8. Document the solution and process

Explanation E. Prior to identifying the results and effects of the solution, you need to implement your proposed solution and test it.

Explanation F. Prior to documenting the solution, you need to propose, test, and identify the results of your proposed solution.

4. Answer: F

Explanation A. You have already done this.

Explanation B. You have already done this.

Explanation C. You have already done this.

Explanation D. You have already done this.

Explanation E. You have already done this.

Explanation F. The final step is that you need to document the successful solution you Network Management 32 have implemented and tested. The Network+ Recommended logical troubleshooting strategy is:

1. Identify the symptoms and potential causes
2. Identify the affected area
3. Establish what has changed
4. Select the most probable cause
5. Implement an action plan and solution including potential effects
6. Test the results
7. Identify the results and effects of the solution
8. Document the solution and process

5. Answer: A

Explanation A. Any address beginning with 169.254.x.x is an automatic private IP address.

Explanation B. To be an APIPA, an address must start with 169.254.

Explanation C. To be an APIPA, an address must start with 169.254.

Explanation D. To be an APIPA, an address must start with 169.254.

Explanation E. To be an APIPA, an address must start with 169.254.

6. Answer: A

Explanation A. This problem is that file and print sharing is disabled. This must be enabled to have another computer access a share on your computer. However, it is not required for you to access a share on another computer.

Explanation B. File and print sharing is not enabled. That is the problem. It must be enabled to share files.

Explanation C. A static IP address is not required to share files.

Explanation D. This has nothing to do with it.

Explanation E. File sharing, or any other network communications should, in general, work the same way on a wireless network as it does on a wired network.

7. Answers: A, B

Explanation A. An important part of a troubleshooting strategy, after you find a solution and test it, is to see what the full results were of your solution and the test. The Network+ Recommended logical troubleshooting strategy is:

1. Identify the symptoms and potential causes
2. Identify the affected area
3. Establish what has changed
4. Select the most probable cause
5. Implement an action plan and solution including potential effects
6. Test the results
7. Identify the results and effects of the solution
8. Document the solution and process

Explanation B. An important step in the process is documenting the solution. This is so that it can be easily solved the next time the problem occurs.

Explanation C. You must have already done this, as you already found a solution and are testing it.

Explanation D. You must have already done this, as you already found a solution and are testing it.

Explanation E. You must have already done this, as you already found a solution and are testing it.

Chapter 5

1. Answer: A

Explanation A. Netstat -vb is what created the sample output. Netstat -vb shows the operating system components & programs that created the open port.

Explanation B. Nbtstat shows NETBIOS over TCP/IP protocol statistics. It is helpful to troubleshoot NETBIOS to IP address mapping issues or find out a computer's NETBIOS name with only its IP address. It did not create the sample output shown.

Explanation C. Nslookup is used to perform DNS lookups and troubleshooting. It did not create the output shown.

Explanation D. Netstat -a shows all active connections but it doesn't show the programs & components used to create the connection.

2. Answers: A, D

Explanation A. Yes, you need NAT port forwarding. You need to configure your router to forward all terminal services ports to the IP address of your PC. This is because you will be using the public IP address of the router.

Explanation B. Terminal services (the RDP protocol) works fine over any IP network (like the Internet).

Explanation C. There is no license needed for one PC to access another PC via terminal server for remote administration.

Explanation D. Yes, you would point the remote terminal services client to your router's public Internet WAN IP address.

Explanation E. In most cases, you enable NAT port forwarding on your router to the PC's private LAN IP address. You point your remote terminal services client to the router's public Internet WAN IP and the router forwards the proper terminal services port to the PC. Therefore, you cannot use your routers LAN IP address because that would be a private IP address, on the same network as your PC.

3. Answers: A, C, D

Explanation A. Correct. Half-duplex transmissions rely on nodes to detect collisions and perform retransmission, and therefore are susceptible to collisions.

Explanation B. Incorrect. Hubs require end devices to run at half-duplex.

Explanation C. Correct. Hubs rely on network nodes to detect collisions and retransmit.

Explanation D. Correct. On switched networks, full-duplex transmission allows transmissions in both directions, and provides point-to-point transmission. Because there is a "dedicated" connection between end nodes, collision detection is not required.

Explanation E. Incorrect. Half-duplex can attain around 50-60% of the bandwidth of a link due to collisions and retransmissions.

Chapter 6

1. Answer: C

Explanation A. Communications cannot occur successfully as one side is encrypting traffic and the other is not.

Explanation B. The question stated that encryption was enabled. You must assume that this means that it is required for inbound and outbound communications. Therefore, communications could not occur.

Explanation C. Because one side is requiring all traffic to be encrypted, it will drop any traffic that comes in and is not encrypted. Thus, there will be no successful communications.

Explanation D. This is not true. There is no automatic configuration of encryption on both sides of a link.

2. Answer: A

Explanation A. Port security is a switch feature in which it keeps track of the first device's MAC address that connects to it. Thereafter, it will only allow that device to connect to the Ethernet port. If another device tries to connect, it disables the port and sends a SNMP trap to notify an administrator. This configuration can vary, but this is generally how it works.

Explanation B. Port blocking or filtering is where certain TCP ports are stopped from going over the network. For example, to stop FTP traffic, you would configure your firewall to block port 20 & 21.

Explanation C. Some form of authentication on your Internet connection could prevent the salesman from accessing the Internet, but he could still get on the local LAN. You want to prevent that security risk completely. Authentication is close, but it is not the best answer.

Explanation D. There might be some way you could use encryption to help in this problem, but it is not the best choice.

3. Answer: B

Explanation A. Port security will prevent the MAC address on a switch port from changing, once established. It won't do anything to control the flow of traffic on a switch that already has allowed a device to use a port.

Explanation B. To prevent broadcasts (packets to all computer on the network), a feature called broadcast storm control can be enabled on most business-class switches.

Explanation C. Authentication would not help in this case because the PC is already connected to the network and any computer can send a network broadcast.

Explanation D. Encryption would not help in this case because the PC is already connected to the network and any computer can send a network broadcast.

4. Answers: A, B, C, D

Explanation A. Physical attacks on network infrastructure are a form of denial of service (DoS) attack. By the attacker cutting all phone lines to a building, this would affect all computer leased lines as well. For example, this would cause all Internet circuits to be down at that building (assuming they did not use wireless or cable for Internet access).

Explanation B. This is a classic example of a denial of service (DoS) attack. By the attacker using so much bandwidth that no other normal traffic (like email) can flow, the attacker has denied those services. A known way to do this is with a smurf attack using ICMP.

Explanation C. This is a common DoS attack. By using all the CPU or disk on a critical server, the attacker is creating a denial of service for whatever critical service that system provided.

Explanation D. By changing the default route on the core router to instead go to null, the attacker is sending all traffic to nowhere (all outbound traffic disappears). Thus, the attacker has denied whatever critical services are in use from responding to any request.

Explanation E. This would be called a phishing attack, whereby the attacker tricks or lures users into giving up sensitive information and allowing access to a protected network. The keyword in this answer is "harvest".

5. Answer: C

Explanation A. Incorrect. Both WPA 1 and 2 can utilize either TKIP or CCMP encryption.

Explanation B. Incorrect. WPA 1 and 2 both support AES and TKIP ciphers.

Explanation C. Correct. WPA 2 has been improved through the use of information elements within the beacons, association frames, and four-way handshakes. The handshake process has been improved to pass more information, without extra transmissions.

Explanation D. Incorrect. WPA 1 and 2 have both been built for all different network types.