CompTIA® Network+ Exam Notes : Osi Models And Its Functions

examguides.com/Networkplus/network-plus-1.htm

1. Networking Concepts

1.1 OSI model and its function

The OSI model (Open System Interconnection) model defines a computer networking framework to implement protocols in seven layers. A protocol in the networking terms is a kind of negotiation and rule in between two networking entities. The figure below shows the OSI reference model and the seven layers.

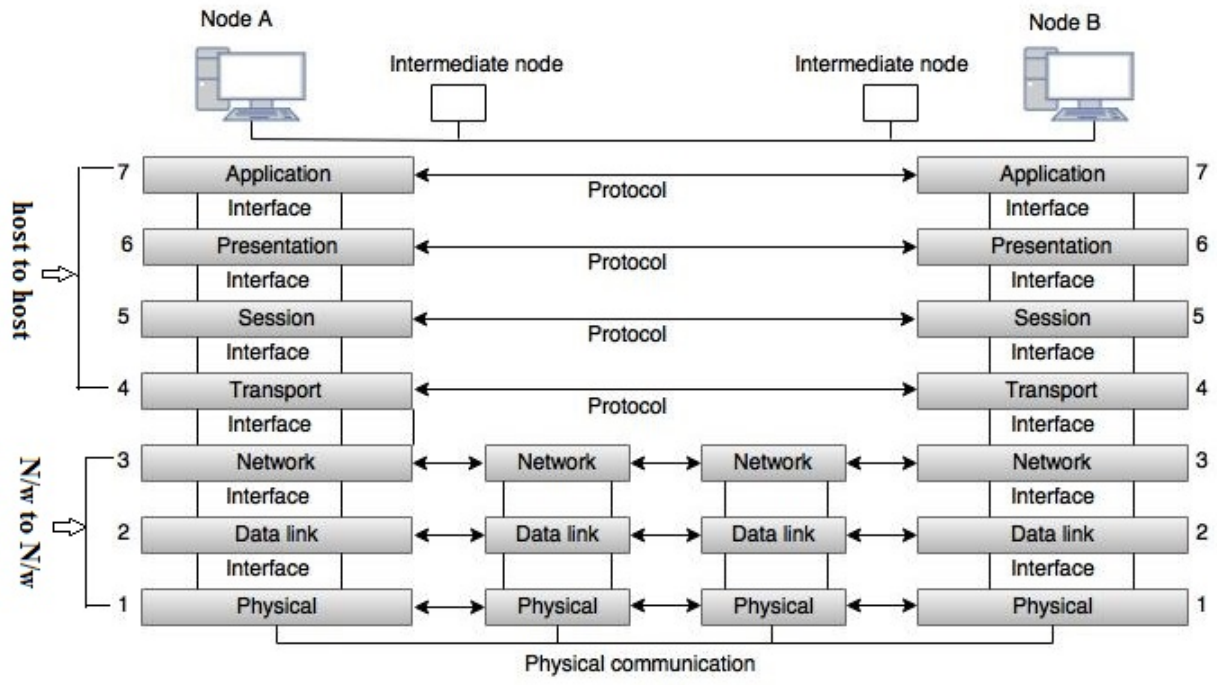


Fig: OSI Model

Interface between layers

Interface is responsible for passing the data and network information down through the layers of the sending device and back up through the layers of the receiving device.

The 7 layers of OSI model are briefly explained below:

1. The Application Layer (Layer-7): Application layer is responsible for identifying and establishing the availability of intended communication partner and verifying sufficient resources exist for communication. Some of the important application layer protocols are: WWW, SMTP, FTP, etc. Application layer (layer 7) is the protocol layer that provides interface to the users or other programs. Most of the applications such as Telnet and FTP operate at layer 7 of the OSI stack.

2. The Presentation Layer (Layer-6): This layer is responsible for presenting the data in standard formats. This layer is responsible for data compression, decompression, encryption, and decryption. Some Presentation Layer standards are: JPEG, MPEG, MIDI, PICT, Quick Time, TIFF. The presentation layer formats the data such that the upper layers are able to understand the data.

3. The Session Layer (Layer-5): Session Layer is responsible for co-ordinating communication between systems/nodes. The following are some of the session layer protocols and interfaces: a) Network File System (NFS), SQL, RPC (Remote Procedure Call), X-Windows, ASP, DNA SCP. The Sessions layer is responsible for maintaining communication sessions.

4. The Transport Layer (Layer-4): The Transport Layer is responsible for multiplexing upper-layer applications, session establishment, and tearing-down of virtual circuits. This layer does "flow control" to maintain data integrity. Flow Control prevents the problem of a sending host on one side of the connection overflowing the buffers in the receiving host. The Transport layer is responsible for maintaining end-to-end communications so that the information is transported reliably over the network.

5. The Network Layer (Layer-3): There can be several paths to send a packet from a given source to a destination. The primary responsibility of Network layer is to send packets from the source network to the destination network using per-determined methods. Routers work at Network layer. The Network layer is responsible for routing packets through the Internet.

In other words, Layer 3 protocols correspond to the network layer and use packets as unit of exchange. IP Security (IPSec) is an example of Layer 3 tunneling protocol. IPSEC encapsulates IP packets in an additional IP header before sending them across an IP network.

- The Packet Filters work at Network Layer of OSI model.
- The Application Layer Proxy works at the Application Layer of OSI model
- Network Address Translation (NAT) is primarily used to hide internal network from external network, such as the Internet. A NAT basically translates the internal IP addresses to external IP addresses and vice-versa. This functionality assures that external users do not see the internal IP addresses, and hence the hosts.

- A Firewall implemented with stateful technology (like Checkpoint Firewall) works at all layers of the OSI model.
- Gateway is used to translate protocols, as it works at the application layer.

6. The Data Link Layer (Layer-2): Data Link Layer is layer 2 of OSI reference model. The Datalink layer is responsible for transmission and reception of frames. It does error detection and correction and uses frame headers for this purpose.This layer is divided into two sub-layers:

- Logical Link Control (LLC) sub-layer.
- Media Access Control (MAC) sub-layer.

The LLC sub-layer handles error control, flow control, framing, and MAC sub-layer addressing.

The MAC sub-layer is the lower of the two sub-layers of the Data Link layer. MAC sub-layer handles access to shared media, such as Token passing or Ethernet.

Examples of data-link layer protocols that use point to point dedicated connection are:

- PPP
- HDLC
- LAPB

Examples of data-link layer protocols that use packet switching are:

- Frame Relay
- ATM
- X.25

7. Physical Layer (Layer-1): The actual flow of bits take place through Physical layer. At Physical layer, the interface between the DTE and DCE is determined. Physical layer is responsible for bit synchronization. Physical layer, as the name implies, transmits the physical signals over the media. The media may be electrical (such as 10BaseT) or optical (such as FDDI).

The following are some of the standard interfaces are defined at Physical layer:

EIA/TIA-232, EIA/TIA-449,V.24,V.35,X.21,G.703,HSSI (High Speed Serial Interface).

Segments are associated with Transport layer,

Packets are associated with Network Layer, and

Frames are associated with Data Link Layer.

Repeaters work at Physical layer (Layer 1),

Bridges and simple switches work at Data Link Layer (Layer 2),

Routers work at Network Layer (Layer 3) of ISO-OSI Reference Model.

A Wireless Access Point (WAP) works at the physical layer of OSI model.

Previous Contents Next

CompTIA® Network+ Exam Notes : Network Topologies

examguides.com/Networkplus/network-plus-2.htm

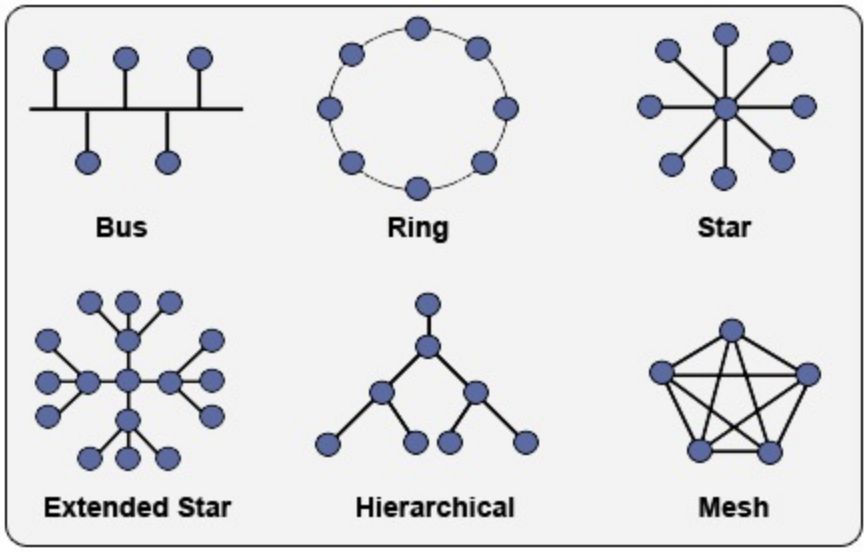
1. Networking Concepts

1.2 Network Topologies

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

Wired Topologies:

Network topological are categorized into Bus, Ring,Star,Tree,Mesh and Hybrid. Below fig shows the different types of topologies.



1. Bus: Bus topology uses one main cable to which all nodes are directly connected. The main cable acts as a backbone for the network. One of the computers in the network typically acts as the computer server. The first advantage of bus topology is that it is easy to connect a computer or peripheral device. The second advantage is that the cable requirements are relatively small, resulting in lower cost.

2. Star: In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server that manages the network, or it can be a much simpler device that only makes the connections between computers over the network possible.

The advantages of a star topology are:

- Addition or deletion of nodes can be done easily
- Any failure at a single node does not effect the whole network
- It is easy to diagnose a star network. Simply diagnosing the HUB will show up which node is bad.
- We can use several cable type in the same network with a hub that can support multiple cable types

The disadvantages of a star topology are:

If the central hub fails, the whole segment will fail

3. Ring: In ring topology, the computers in the network are connected in a circular fashion, and the data travels in one direction. Each computer is directly connected to the next computer, forming a single pathway for signals through the network. This type of network is easy to install and manage.

4. Hierarchical Topology: It is also known as the Tree topology. It can be considered as the combination of linear bus and star topologies as it contains systems with star topology connected to a linear bus main cable. There is dependency on the main linear bus line, and therefore any fault in this line can bring the entire segment down. However, this type of arrangement is supported by many hardware and software tenders. This topology is also known as expanded star topology. The configuration and wiring is difficult in comparison to other topologies. However, its point to point wiring for individual sections is a desirable feature of this topology.

5. Mesh Topology: In this type of arrangement every node participating in the network is connected to every other node. However, this tends to be very expensive and difficult to implement. Multiple paths are can be used for transmitting a message. Due to the presence of dedicated links, it does not provide any traffic problem.

6. Extended Star Topology: It refers to the arrangement which is basically an extension of star topology. An Ethernet network with several LANs extending beyond a single level may be seen as an Extended Star. Another topology that is commonly known is Hybrid topology, which is a combination of any two or more different types of network topologies. This arrangement is known for its flexibility and reliability.

Token Ring is an IEEE 802.5 standard whose topology is physically a star but logically a ring.

10BaseT is IEEE 802.3 standard whose topology is physically a star but logically a bus.

The 5-4-3 rule states that between any two nodes on the network, there can only be a maximum of five segments, connected through four repeaters, and only three of the five segments may contain user connections.

Wireless Topologies

Network topology is a layout of various elements of computer network, such as nodes, links, routers, etc. It is a network topological structure which can be depicted logically or physically.

Physical topology shows the physical location of network's components and cable connections between network nodes. Logical topology describes the data flows, the circulation of signals in physical topology. The physical and logical topologies for two networks can be identical, while their physical interconnections, the distances between nodes, transmission rates, and/or signal types may be differ

Infrastructure mode: The wireless network consist of at least one access point (AP) connected to the wired network and a set of wireless nodes (WN). This configuration is called a Basic Service Set (BSS). Extended Service Set (ESS) is a set of two or more BSSs (multiple cells).

Ad hoc mode: Also called "IEEE ad-hoc mode" or "peer-to-peer mode". This configuration is called Independent Basic Service Set (IBSS) and is useful for establishing a network where wireless infrastructure does not exist or where services are not required. Ad-hoc mode is used when devices or stations communicate directly with each other, without the use of Wireless Access Point (WAP). Ad-hoc mode is useful for establishing a network where wireless infrastructure is un-available or does not exist.

Extended Service Set (ESS) is a set of two or more Basic Service Sets (BSSes) working together to form a single wireless network. Stations are able to move between BSS within a single ESS yet remain "connected" to the fixed network and so continue to receive emails etc. As a Station moves into a new BSS, it will carry out a re-association procedure with the new AP (Access Point). Hotspot is an example of WLAN

Different Types of Networks:

LAN: A Local Area Network is a group of computers and network devices connected together, usually within the same building. By definition, the connections must be high speed and relatively inexpensive (e.g., token ring or Ethernet). A LAN connection is a high-speed

connection to a LAN. For example, most of the buildings within a campus are connected using a LAN.

MAN: A Metropolitan Area Network is a larger network that usually spans several buildings in the same city or town. For example, if your organization has several buildings spread across the city, then they may be connected via MAN.

WAN: A Wide Area Network in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

The number of required WAN connections can be calculated with the formula w = n * (n - 1) / 2, where w = the number of WAN links and n = the number of sites.

For example, a network with 10 sites would require 45 WAN connections to form a fully meshed network: 45 = 10 * (10 - 1) / 2.

ISDN is an example of WAN protocol.

18,000 feet is the maximum distance that a customer can be located from the central office for ISDN connectivity. If necessary, a repeater can be used to increase the distance limitation.

In a full mesh topology, each network node is connected to every other network node. This type of inter connectivity results in highest level of redundancy.

PAN: A Personal Area Network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Infrared(IR) and Near-field communications(NFC) are examples of PAN

WPAN: A Wireless Personal Area Network is a PAN carried over wireless network technologies such as Bluetooth, wireless USB etc.

Both WiMAX and LTE are 4G (4th Generation) cellular technologies. One of the biggest advantages of LTE over WiMAX is its compatibility with all previous mobile technologies GSM, GPRS, UMTS, WCDMA, CDMA, CDMA200, EV-DO.

WiMAX network doesn't support legacy systems like 2G and 3G. WiMAX is a better choice for the low cost installing network. Both WiMAX and LTE can theoretically reach between 10 and 50 Mbps connection speeds, though actual speeds may depend on several factors and

rarely reach the max speeds. WiMAX is an example of WirelessMAN

High Speed Packet Access (HSPA+) is considered a 3.5 generation technology. It has greatly improved data rates over its HSPA forerunner. Because HSPA+ can use an all-IP architecture, it has the potential to evolve into a true 4G technology.

Technologies that facilitate the Internet of Things(IoT):

Bluetooth: It is widely used from smart phones to personal gadgets. It operates in the 2.4 Gigahertz ISM band. Bluetooth signals typically travel over a distance of 10 to 300 feet. Because Bluetooth uses radio frequencies, the devices do not have to be within line of sight of each other.

ANT devices may use any RF frequency from 2400MHz to 2524MHz, with the exception of 2457MHz, which is reserved for ANT+ devices. ANT+ is built on top of the proven ultra-low power ANT protocol, the network is optimized for power consumption, cost, latency, robust communication and ease of implementation. Over all, ANT and ANT+ standards are widely adopted for IoT and uses 2.4GHz ISM band of frequencies.

Zwave (or Z wave or Z-wave), developed by zensys, is a protocol for communication among devices used for home automation. It uses RF for signaling and control. Zwave operates at 908.42 MHz in the US (868.42 MHz in Europe) using a mesh networking topology. Each Z-Wave network is identified by a Network ID and each device is further identified by a Node ID.

IR, short for Infra Red, requires line of sight communication.

NFC is a set of short-range wireless technologies, typically requiring a separation of 10 cm or less. NFC operates at 13.56 MHz.

Previous Contents Next

CompTIA® Network+ Exam Notes : Uses Of Ports And Protocols

examguides.com/Networkplus/network-plus-3.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

1. Networking Concepts

1.3 Uses of ports and protocols

Internet protocols use Well Known port numbers, based on which the packet type is identified.

Commonly used TCP and UDP default ports are as given below:

TCP ports

FTP	20, 21
SSH	22
TELNET	23
SMTP	25
DNS	53
HTTP	80
NTP	123
HTTPS	443

WWW	80
SSL	443 (Secure socket layer)
SNMP	161
SSH	22
POP3	110
IMAP	143

UDP ports

TFTP	69
DNS	53
BOOTPS/DHCP	67
SNMP	161

Note that non-secure email communications use ports 110 and 143.

Port 110 - this is the default POP3 non-encrypted port

Port 995 - this is the port you need to use if you want to connect using POP3 securely

Port 143 - this is the default IMAP non-encrypted port

Port 993 - this is the port you need to use if you want to connect using IMAP securely

Port 465 - this is the port used if you want to send messages using SMTP securely

If you want to access the email server without encryption, then the ports 110/143 need to be accessible.

Various ports that are used for secure email transmission using TLS/SSL are given below:

995 TCP - Post Office Protocol 3 over TLS/SSL (POP3S) (Official)

993 TCP - Internet Message Access Protocol over SSL (IMAPS) (Official)

587 TCP - e-mail message submission (SMTP)

443 TCP - HTTPS (Hypertext Transfer Protocol over SSL/TLS)

Please note that FTP, Telnet, and SMTP use TCP; whereas TFTP and SNMP use UDP.

On a Web server, using SSL, port 443 is the port that the server "listens to" or expects to receive from a Web client, assuming that the default was taken when the server was configured or set up. A port can be specified in the range from 0-65536 on the NCSA server. By default, the port number for a secure Web server is 443 inbound.

When you are accessing a Web page, the browser sends the request over the default port number (For WWW, the default port number is 80). For any reason, If you change the default port number that a Web server listens to, users need to specify the port number in the URL.

SMTP: SMTP is the most widely used e-mail standard on the Internet, and part of TCP/IP stack. SMTP can be used to upload mail over Internet to a Mail server.

POP: POP is used for downloading mail from a mail server to a client machine running POP client.

A SMTP server listens to port 25, and the POP server listens to port 110 by default. Therefore, you need to keep these two ports open for communication with remote client computers. All other ports can be blocked to prevent misuse.

FTP (File Transfer Protocol): It is a client/server protocol used for transferring files between the client computer and server computer, and uses TCP/IP. FTP utilizes two ports, a 'data' port and a 'command' port (also known as the control port). Traditionally, for Active FTP, these are port 21 for the commands and port 20 for the data. If a firewall is to be configured for FTP, allow both the ports for proper FTP connectivity. FTP transfers files in unencrypted form , even the authentication occurs in clear text for FTP and Telnet. A hacker may gain access to an FTP server by exploiting this weakness.

There is another form of FTP, known as Passive FTP. Passive FTP uses port 21 for commands, and any port greater than 1023 for data.

Note that the FTP client computer uses any ports greater than 1023 for communicating with the FTP server. FTP is a connection oriented protocol. It uses TCP/IP for file transfer.

HTTP (Hyper Text Transfer Protocol) and HTML **(Hyper Text Markup Language):** HTTP and HTML used for browsing the Web. HTTP is the protocol used for accessing the World Wide Web services. HTTP operates over TCP/IP. TCP/IP is the protocol, which is used by all internet applications such as WWW, FTP, Telnet etc. IPX/SPX is proprietary protocol stack of Novell NetWare.

TFTP (Trivial File Transfer Protocol): TFTP is a a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features. It has least amount of overhead, and as a result the fastest file transfer protocol.

SFTP: SFTP or secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. It is functionally similar to FTP, but because it uses a different protocol, you can't use a standard FTP client to talk to an SFTP server, nor can you connect to an FTP server with a client that supports only SFTP.

Simple Network Management Protocol (SNMP): SNMP is an application-layer protocol defined by the Internet Architecture Board (IAB) for exchanging management information between network devices. It is a part of Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP is one of the widely accepted protocols to manage and monitor network elements. Security is based on the concept of communities. All machines that are part of same community can talk to one another. Basically, the name of the community is like a password and should be treated that way. Only agents and managers that are part of the same community can talk to one another. The default community name is "public". For security reasons, it is better to change the community name to a difficult to guess name. SNMP uses UDP over IP. It Used to monitor and manage network devices

Numbers 0 - 255 are used for public applications

Numbers 255 - 1023 are assigned to companies so that they can use these port numbers in their applications.

Numbers above 1023 are used by upper layers to set up sessions with other hosts and by TCP to use as source and destination addresses.

SIP operates at the application layer of the OSI model and is used to maintain a multimedia session. SIP uses ports 5060 and 5061.

Protocol Types:

TCP and UDP: The port number used by TCP is 6 and that of UDP is 17. TCP and UDP work at transport layer or the Host-to-Host layer of DOD Model.

TCP is a full-duplex, connection-oriented protocol. It incorporates error checking as well.

UDP (User Datagram Protocol): UDP is a thin protocol. UDP is a connectionless protocol. It doesn't contact the destination before sending the packet and doesn't care whether the packet is reached at the destination.

UDP is a connectionless protocol and TCP is a connection oriented protocol.

Connection oriented Protocols:

1. It guarantees transmitted data will reach its destination

2. It sequences the packets such that the packets are received in a sequenced manner at the destination.

3. TCP/IP is an example of connection oriented protocol.

Connectionless protocols:

1. Connectionless protocols do not guarantee packet delivery.

2. The advantage is less over-head.

3. UDP/IP is an example of connectionless protocol.

ICMP: ICMP (Internet Message Control Protocol) messages are used for basic error reporting between host to host, or host to gateway. It is not used for error reporting between Gateways. ICMP messages are encapsulated using the IP protocol. For example, the command "ping" uses ICMP protocol. In the OSI Reference model, ICMPs are generally considered part of the IP layer. It sends an ICMP message if the destination is unreachable. Routers can make alternate route decisions based on ICMP messages, if appropriate.

Tracert and Ping use ICMP as their base protocol. Telnet and FTP use TCP/IP protocol. Telnet is used for terminal emulation. Telnet requires an username and password to access.

IP: IP is the protocol that works at Internet layer. It forwards the packets based on the network address (IP address) in the packets and the routing tables.

ARP (Address Resolution Protocol): IP works at network layer. IP address is a logical address. If a packet is to be delivered to a destination machine, its physical address (MAC address) needs to be known. ARP is a protocol, which enables a machine to obtain its MAC address from a known IP address. It essentially maps logical and physical addresses.

Reverse ARP (RARP): RARP is used to obtain an IP address using an RARP broadcast. RARP can be used to boot diskless workstations over a network. RARP is used to obtain IP address from a known MAC address.

BootP (Bootstrap Protocol): When a diskless workstation is powered on, it broadcasts a BootP request on the network. A BootP server responds with its IP address, Default gateway, etc.

Both PPP and SLIP can be used for dial up connections. However, SLIP can't be used where the IP address need to be assigned dynamically. The advantage of PPP is multi protocol support, that it can support TCP/IP, IPX, AppleTalk etc. SLIP can support only TCP/IP and IP addresses need to be assigned manually.

The server computer runs the service (also called daemon), where as the remote client computers run the client process. A protocol, such as TCP/IP is required for communication.

Real-Time Transport Protocol (RTP): is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features. Used for delivering media-based data over networks, such as Voice over IP. It is an Internet protocol for transmitting real-time data such as audio and video. RTP runs on top of the UDP protocol.

1. RTCP: RTCP works hand in hand with RTP. RTP does the delivery of the actual data, where as RTCP is used to send control packets to participants in a call. The primary function is to provide feedback on the quality of service being provided by RTP.

2. Real-Time Transport Protocol (RTP): is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.

3. Real Time Streaming Protocol (RTSP): is a protocol used for establishing and maintaining communications with a media server (for example, a video server).

Variables associated with real-time services are presence and multicast/unicast. Presence simply means being connected to the medium in question and being able to respond to the real-time data.

4. H.323 is a signalling protocol used to provide multimedia communications over a network. It's port number is 1720.

5. Media Gateway Control Protocol (MGCP): Used as a call control and communication protocol for Voice over IP networks

Telnet is used to access UNIX and Linux systems. Telnet uses port 23 and is insecure. SSH is considered the secure replacement for Telnet.

Previous Contents Next

CompTIA® Network+ Exam Notes : IP Adressing

examguides.com/Networkplus/network-plus-4.htm

1. Networking Concepts

1.4 IP addressing

Each computer on the Internet having a unique IP address is known as a HOST. IP address is a logical address and used for routing packets over an IP network.

IP addresses are written using decimal numbers separated by decimal points. This is called dotted decimal notation of expressing IP addresses.

The different classes of IP addresses is as below:

Class	Format	Leading Bit Pattern	Network address Range	Maximum networks	Maximum host/nodes
A	N.H.H.H	0	1.0.0.1 to 126.255.255.254	127	16,777,214
B	N.N.H.H	10	128.1.0.1 to 191.255.255.254	16,384	65,534
C	N.N.N.H	110	192.0.1.1 to 223.255.254.254	20,971,52	254
D	N.A.	N.A.	224.0.0.0 to 239.255.255.255	N.A.	N.A.

- Network address of all zeros means "This network or segment.
- Network address of all 1s means "all networks", same as hexadecimal of all Fs. 255.255.255.255 broadcasts to all hosts on the local network.
- Network number 127 is reserved for loopback tests, ie any IP in the range 127.x.x.x is reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address.
- Host(Node) address of all zeros mean "This Host (Node)".
- Host (Node) address of all 1s mean "all Hosts (Nodes) " on the specified network.
- The range of numbers from 224.0.0.0 to 239.255.255.255 is used for multicast packets. This is known as Class D address range.
- it doesn't have network and host bits. If it's a multi-cast address then one IP would go to multiple machines because all have that IP.
- Class E addresses are reserved for future use, or Research and Development Purposes.

Subnetting:

The following are the advantages of subnetting:

- The network congestion improves
- IP addresses can be efficiently used
- Security can be improved (Since it requires a router to switch traffic from one subnet to another, only hosts on a particular subnet can see the packets)

Classful addressing: RIPv1, IGRP are examples of classful routing protocols. It is important to know that classful routing protocols do not exchange subnet information during routing information exchanges. The summarization is always done automatically at major network boundaries.

Examples on subnetting:

Example 1: You are designing an IP addressing scheme for a corporate network. The subnet uses 196.116.18.0/24. What are the valid host addresses available, excluding subnet zero and bradcast address.

Solution: An address where all host part bits are 0 refers to the (this) network, and an address where all bits of the host part are 1 is called a broadcast address. This refers to all hosts on the specified network simultaneously. Thus, 196.116.18.255 is not a valid host address, but refers to all hosts on network 196.116.18.0.

The valid host addresses - 196.116.18.1 through 196.116.18.254

Example 2: What is the directed broadcast address for an IP network 196.233.24.15 with default subnet mask?

Solution: This is a Class C network with default subnet mask, which is 255.255.255.0. The directed broadcast should reach all Hosts on the intended network (or subnet, if subnetted). Therefore, by putting all 1s for the host potion of the IP address, we get 196.233.24.255.

Example 3: You have three physical LAN segments, each with 10 Hosts. All three segments are connected to three different interfaces on your router. What is the minimum number of subnets required?

Solution: Since there are three segments, you need to have three subnets.

Example 4: You are asked to evolve a TCP/IP addressing scheme for your Organization. How many network numbers (subnet number) must you allow when you design the network for your organization? (Choose 2 best answers)

Solution: You need to assign a different network number for each subnet. Also, you need to set aside one network number for each WAN connection.

Example 5: You are given an IP address 154.54.12.36. What is the default subnet mask?

Solution: The IP address 154.54.12.36 belongs to Class B network.

The default subnet mask for different classes of IP networks are as given below:

Class A network: 255.0.0.0

Class B network 255.255.0.0

Class C network 255.255.255.0

Example 6: You have a router with two ports, each having distinct IP address. Both ports are connected to two distinct subnets (segments). The first subnet has 12 clients and a server. The second subnet has 14 clients and a server. What is the total number of IP addresses required?

Solution: The number of distinct IP's required are

1) One each per client computer

2) One each per server computer

3) One each per router interface.

There are 2 servers + 26 clients + 2 router interfaces. Therefore, the total number of IP addresses required are 30. Loopback address is an IP number (127.0.0.1) that is designated for the software loopback interface of a computer. The loopback interface has no hardware associated with it, and is a logical interface only.

Example 7: What is the decimal equivalent of the binary number 1110 0011?

Position of Bit	7th	6th	5th	4th	3rd	2nd	1st	0th
Decimal Value	128	64	32	16	8	4	2	1

Solution: Calculate the decimal equivalent based on the above predefined values.

Given binary number is : 1110 0011

1*(2^7) + 1*(2^6) + 1*(2^5) + 0*(2^4) + 0*(2^3) + 0*(2^2) + 1*(2^1) + 1*(2^0) = 1*128 + 1*64 + 1*32 + 0*16 + 0*8 + 0*4 + 1*2 + 1*1

=128+64+32+0+0+0+2+1 =227

therefore decimal equivalent of 1110 0011 is 227

Note: Binary number is the sum of the digits multiplied with 2n.

Example 8: What is the binary equivalent of decimal number 52?

Solution:

1. Is 52 greater than or equal to 128? => No => Put a 0 in the 128 column.

2. Is 52 greater than or equal to 64? => No => Put a 0 in the 64 column.

Binary conversion: Base table

128	64	32	16	8	4	2	1

3. Is 52 greater than or equal to 32? => Yes => Put a 1 in the 32 column, and subtract 32 from 52. => 52 - 32 = 20.

4. Is 20 greater than or equal to 16? => Yes => Put a 1 in the 16 column, and subtract 16 from 20. => 20 - 16 = 4.

5. Is 4 greater than or equal to 8? => No => Put a 0 in the 8 column.

6. Is 4 greater than or equal to 4? => No => Put a 1 in the 4 column, and subtract 4 from 4. =>4-4=0

7. Is 0 greater than or equal to 2? => No => Put a 0 in the 2 column.

8. Is 0 greater than or equal to 1? => No => Put a 0 in the 1 column.

Example 9: What is the decimal equivalent of hexadecimal F8CE?

128	64	32	16	8	4	2	1
0	0	1	1	0	1	0	0

Solution: Hexadecimal numbers are numbers with the base 16. It uses 16 different digits to represent the numbers. It is denoted as h16, where h is a hexadecimal number. It may be combination and alphabets and numbers. It uses numbers from 0 to 9 and alphabets A to F(11-15). Hexadecimal number is the sum of the digits multiplied with 16n. The table below shows conversion values from binary, octal, decimal, and hexadecimal.

Decimal	Binary	Octal	Hex
00	0000	00	0
01	0001	01	1
02	0010	02	2
03	0011	03	3
04	0100	04	4
05	0101	05	5
06	0110	06	6
07	0111	07	7
08	1000	10	8
09	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

F-15 , C-12, E-14

F8CE= 15x163+8x162+12x161+14x160 = 61440+2048+192+14= 63694

Classless routing protocols: RIPv2, EIGRP, OSPF, BGPv4, and IS-IS are examples of classless routing protocols. In classless routing protocols, subnet information is exchanged during routing updates. This results in more efficient utilization of IP addresses. The summarization in classless networks is manually controlled.

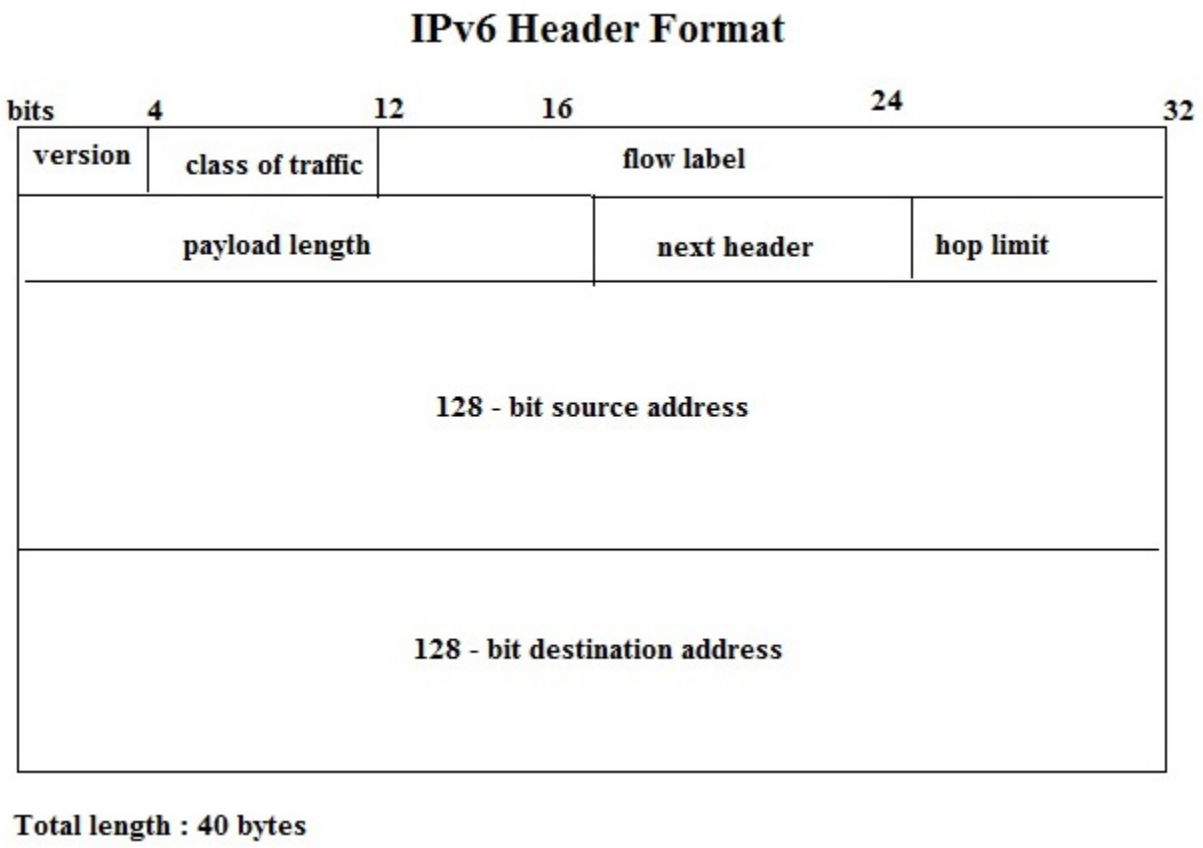
VLSM: RIPv1 and IGRP are true distance-vector routing protocols and can't do much, really-except build and maintain routing tables and use a lot of bandwidth. RIPv2,OSPF, IS-IS, EIGRP, and BGP. These routing protocols support VLSM because the routing protocols send the subnet mask as part of any routing update. EIGRP, and OSPF use Autonomous System (AS) numbers.

IPv6 Addressing: IANA (Internet Assigned Numbers Authority) is the organization under the Internet Architecture Board (IAB) of the Internet Society that oversees the allocation of Internet Protocol addresses to Internet service providers (ISPs). ICANN (a non governmental

organization) has now assumed responsibility for the tasks formerly performed by IANA. ISPs in turn allot IP addresses to small companies, and businesses.

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear. IPv4 addresses use the last 32 bits of the IPv6 address.

IPv6 packet is 128 bits long. It will have basic packet header, and optional extension header. The next header field within an extension header points to the next header in the chain.



IPv6 header contains the following things:

- Version - This field contains the version of the IP used in the packet. It is of 4-bit in IP version 6.
- Traffic class - This is an 8-bits field determining the packet priority. Priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.
- Flow label - This 20 bits specifies the QoS management. Originally created for giving real-time applications special service, but currently unused.
- Payload length - This 16 bits determines the payload length in bytes. When cleared to zero, the option is a "Jumbo payload" (hop-by-hop).
- Next header - This 8-bits field specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.

- Hop limit - This is an 8-bits field newly introduced in IPv6. It replaces the time to live field of IPv4
- Source Address - This 128 bits field determines the logical address of the host that is sending the packet.
- Destination Address - This 128 bits field determines the logical address of the host that is receiving the packet.
- The payload can have a size of up to 64KB in standard mode, or larger with a "jumbo payload" option.

The extension header may include the following:

- Hop-by-Hop options
- Destination options
- Routing (specifies intermediate routers that the route must include forcing an administratively defined path)
- Fragment (Used to divide packets that are too large for the maximum unit (MTU))
- Authentication and Encapsulating Security Payload (ESP)

IPv6 hosts supports the following:

- Loopback address (::::1/128)
- All-nodes multicast addresses (FF01::1 and FF02::1)
- Link-local address (FE80::/10), autoconfigured.

The minimum MTU supported in IPv6 is 1280 octets. The recommended MTU value for IPv6 links is 1500 octets.

3 types of addresses are supported in IPv6:

1. Unicast: one-to-one with various scopes (i.e.: Global, Link, Unique Local, Compatible)

2. Anycast: one-to-nearest (allocated from unicast)

3. Multicast: one-to-many

Broadcast has disappeared as a term, but is considered one form of multicast.

In an IPv6 network, a host can auto-configure its IP address without the help of a DHCP server.

IPv6 to ipv4 transport:

4to6 refers to tunneling of IPv4 in IPv6: It is an Internet inter-operation mechanism allowing Internet Protocol version 4 (IPv4) to be used in an IPv6 only network. 4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels as defined in RFC 2473

6to4 tunneling: It is an IPv6 transition mechanism described in RFC 3056. It enables encapsulation of IPv6 packets into IPv4 for transport across an IPv4 network. 6to4 tunneling allows for automatic IPv6-to-IPv4 address translation, and treats the underlying IPv4 network as one big non-broadcast multi-access (NBMA) network, rather than a collection of independent point-to-point links. A 6-to-4 tunnel works similarly to a manual tunnel, except that the tunnel is set up automatically. 6-to-4 tunnels use IPv6 addresses that concatenate 2002::/16 with the 32-bit IPv4 address of the edge router, creating a 48-bit prefix.

Dynamic Host Configuration Protocol version 6 (DHCP6): is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network.

Miredo is a Teredo tunneling client designed to allow full IPv6 connectivity to computer systems which are on the IPv4-based Internet but which have no direct native connection to an IPv6 network.

Example: The MAC address of a node is 00-0F-66-41-29-C3.

The appropriately formed IPv6 interface id using EUI-64 format

The EUI-64 format interface ID is derived from the 48-bit MAC address by inserting the hex FFFE between the organizationally unique identifier (OUI) field (the upper three bytes) and the vendor code (the lower three bytes) of the MAC address. The seventh bit in the first byte of the resulting interface ID, corresponding to the Universal/Local (U/L) bit, is set to binary 1.

IPv6 Multicast Addresses used by different routing protocols:

- RIPv6: FF02::9
- OSPF speaker: FF02::5
- OSPF DR and BDR: FF02::6

Multicast Address Node Local:

- FF01:0:0:0:0:0:0:1 or FF01::1 All Nodes Address
- FF01:0:0:0:0:0:0:2 or FF01::2 All Routers Address

Link Local:

- FF02:0:0:0:0:0:0:1 or FF02::1 All Nodes Address
- FF02:0:0:0:0:0:0:2 or FF02::2 All Routers Address

- FF02:0:0:0:0:0:0:D or FF02::D All PIM Routers

The following are true about IPv6 address format:

1. The total length of IPv6 address is 128 bits

2. The first 48 bits of the IPv6 global unicast addresses are used for global routing at the Internet Service Provider (ISP) level.

3. 16 bits (after the first 48-bit global unicast address) are used for subnetting, allowing organizations to subdivide their network

4. Multicast addresses are in the range FF00::/8.

Unicast 6to4 addresses (2002::/16): IPv6 uses 6to4 addresses to communicate between two IPv6/IPv4 nodes over the IPv4 Internet. A 6to4 address combines the prefix 2002::/16 with the 32 bits of the public IPv4 address of the node to create a 48-bit prefix - 2002:WWXX:YYZZ::/48, where WWXX:YYZZ is the colon-hexadecimal representation of w.x.y.z, a public IPv4 address. Therefore, the IPv4 address 157.60.91.123 translates into a 6to4 address prefix of 2002:9D3C:5B7B::/48.

Unicast site-local addresses: IPv6 unicast site-local addresses are similar to IPv4 private addresses. The scope of a site-local address is the internetwork of an organization's site. (You can use both global addresses and site-local addresses in your network.) The prefix for site-local addresses is FEC0::/48.

Unicast unspecified address: The IPv6 unicast unspecified address is equivalent to the IPv4 unspecified address of 0.0.0.0. The IPv6 unspecified address is 0:0:0:0:0:0:0:0:, or a double colon (::).

Unicast loopback address: The IPv6 unicast loopback address is equivalent to the IPv4 loopback address, 127.0.0.1. The IPv6 loopback address is 0:0:0:0:0:0:0:1, or ::1

Multicast addresses from FF01:: through FF0F:: are reserved, well-known addresses. To identify all nodes for the node-local and link-local scopes, the following multicast addresses are defined:

FF01::1 (node-local scope all-nodes address)

FF02::1 (link-local scope all-nodes address)

To identify all routers for the node-local, link-local, and site-local scopes, the following multicast addresses are defined:

FF01::2 (node-local scope all-routers address)

FF02::2 (link-local scope all-routers address)

FF05::2 (site-local scope all-routers address)

Address Assignments:

DHCP: DHCP is a successor to BOOT/P protocol. DHCP allows us to dynamically assign IP addresses, subnet mask,default gateway to hosts on a network. In other words, DHCP allows us to IP configure the client computers on a network dynamically at boot time. You have to assign the IP address for your DHCP server statically. A DHCP server can't assign an IP address to itself. Similarly, some other servers which need static assignment of IP addresses are your DNS server, WINS server, and Default gateway. You must assign the IP address of the DHCP Server manually.

Multicast Domain Name Service (MDNS) is an example of a technology that can resolve computer names to their corresponding IP address on a local subnet, without the aid of a DNS server or a WINS server.

BootP and DHCP are dynamic approaches to assigning routable IP addresses to networked devices.

APIPA: Short for Automatic Private IP Addressing is a feature that allows DHCP clients to automatically self-configure an IP address and subnet mask when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself. The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default class B subnet mask of 255.255.0.0. A link-local IP address is a non-routable IP address usable only on a local subnet. APIPA is an example of a technology that assigns link-local IP addresses.

Windows 98 and later versions have an Automatic Private IP Addressing (APIPA) feature that will automatically assign an Internet Protocol address to a computer on which it installed. This occurs when the TCP/IP protocol set to obtain it's IP address automatically from a Dynamic Host Configuration Protocol server, and when there is no DHCP server present or not available.

The Internet Assigned Numbers Authority (IANA) has reserved private IP addresses in the range of 169.254.0.0 -169.254.255.255 for Automatic Private IP Addressing

After the network adapter has been assigned an automatic IP address, a computer can communicate with any other computers on the local network that are also configured by APIPA or have static IP address manually set to the 169.254.x.y (where x.y is the client's unique identifier) address range with a subnet mask of 255.255.0.0.

Microsoft windows 7 defaults to APIPA if a client is configured to automatically obtain IP address information and that client fails to obtain IP address information from a DHCP server.

RIPng, OSPFv3, and EIGRPv6 support IPv6 addressing. Prior versions of OSPF such as OSPFv1 and OSPFv2 does not support IPv6. Similarly, RIP, RIPv2, EIGRP (prior to EIGHTv6) does not support IPv6 addressing. RIPng for IPv6 offers the same benefits as RIP-2 and IPv6 OSPF is an IETF proposed standard.

Previous Contents Next

CompTIA® Network+ Exam Notes : Characteristics Of Routing And Switching

examguides.com/Networkplus/network-plus-5.htm

1. Networking Concepts

1.5 Characteristics of routing and switching

Properties of Network Traffic:

CSMA/CD: In Carrier Sense Multiple Access With Collision Detection (CSMA/CD), a node transmits only after listening to the media, and ensuring that no transmission is taking place. Further, sending nodes detect when a collision occurs and stop transmitting immediately, backing off for a random amount of time before trying again. This results in efficient use of the media since the bandwidth of transmitting the entire frame is not wasted. CSMA/CD is a contention media access method that senses for network traffic before transmission and uses collision-detection and re-transmission techniques.

CSMA/CA: Carrier sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle". CSMA/CA can optionally be supplemented by the exchange of a Request to Send (RTS) packet sent by the sender S, and a Clear to Send (CTS) packet sent by the intended receiver R. Thus alerting all nodes within range of the sender, receiver or both, to not transmit for the duration of the main transmission. This is known as the IEEE 802.11 RTS/CTS exchange. Implementation of RTS/CTS helps to partially solve the hidden node problem that is often found in wireless networking. In CSMA/CA, before a host sends real data on the wire it will "sense" the wire to check if the wire is free.

Collision domain and broadcast domain: It is important to know the difference between a collision domain and a broadcast domain. When you use hubs, all the nodes connected to the hub will be in the same collision domain. However, when you use switches and implement VLANs, each VLAN will be in a separate broadcast domain. The packet forwarding between VLANs is achieved through the use of routing.

As application data is transmitted down the protocol stack across the network media, various protocols adds information to it at each level. This is commonly known as the encapsulation process.

The form that a piece of data takes at any layer is called a protocol data unit(PDU). During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. At each stage of the process, a PDU has a

different name to reflect its new functions.

The reverse process, decapsulation (or de-encapsulation), is performed at the receiving system as the packet travels up through the protocol stack.

Multiplexing means combining multiple streams of information for transmission over a shared medium.

Demultiplexing performs the reverse function: split a combined stream arriving from a shared medium into the original information streams.

Time-division multiplexing (TDM): supports different communication sessions on the same physical medium by causing the sessions to take turns.

Frequency-division multiplexing (FDM): is a scheme in which numerous signals are combined for transmission on a single communications line or channel. Each signal is assigned a different frequency (sub-channel) within the main channel.

Broadband technologies divide the bandwidth available on a medium into different channels. Different communication streams are then transmitted over the various channels. Example: Fiber-optic cabling.

Baseband technologies use all the available frequencies on a medium to transmit data. Ethernet is an example of a networking technology that uses which of the following approach.

Bit rate is a measure of the number of data bits (that's 0's and 1's) transmitted in one second.

Baud rate is the number of times a signal in a communication channel changes state. Baud rate is less than or equal to the bit rate.

Baud rate = 2000 bauds per second (baud/s)

Bit rate =2000 X 2 = 4000bps

Baud rate is calculated using the formula: S = N/r (baud/s)

here, N is the bit rate and r is the number of data elements carried by each signal element.

Baud rate = 2000/2 = 1000 baud/s

Routing Types:

1. Static Routes - Configured by the administrator manually. The administrator must also update the table manually every time a change to the network takes place. Static routes are commonly used when routing from a network to a stub (a network with a single route) network.

A static route adds an entry to the routing table for a specific destination IP address or subnet.

To configure a static route, issue the

ip route prefix mask {*ip-address | interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]*

command in global configuration mode

2. Default Routes - The default route (gateway of last resort) is used when a route is not known or is infeasible. The command is

ip route *0.0.0.0 0.0.0.0 165.44.56.5*

Here 165.44.56.5 is the gateway of last resort to network 0.0.0.0

Default route is used when there is no other known route to a given IP packet's destination. Default route is also known as gateway of last resort.

syntax is for setting default route is: **ip route** 0.0.0.0 0.0.0.0 <next_hop_address>

Router(config)#ip route *0.0.0.0 0.0.0.0 192.168.1.1*

You can also set default route by specifying the interface as :

Router(config)#ip route *0.0.0.0 0.0.0.0 s0*

3. Dynamic Routes - As soon as dynamic routing is enabled, the routing tables are automatically updated. Dynamic routing uses broadcasts and multicasts to communicate with other routers. Each route entry includes a subnet number, the interface out to that subnet, and the IP address of the next router that should receive the packet. The commands to enable rip are:

router rip
network <*major network number*>

Segmentation and Interface properties:

VLAN: A VLAN is a group of devices on one or more logically segmented LANs. All devices working on a VLAN will have same broadcast domain. Like routers, the switches (Layer 2) have ability to provide domain broadcast segmentation called a VLAN. Using VLAN technology, you can group switch ports and their connected users into logically defined communities of interest. A VLAN operating on a Catalyst switch limits transmission of unicast, multicast, and broadcast traffic to only the other ports belonging to that VLAN, thereby controlling broadcasts. The switch can be configured to provide two separate VLANs,

one each for VOIP traffic and data traffic. A layer-2 switch will have only one collision domain. It means, the bandwidth is shared by all the ports in the switch. One way to increase the bandwidth is by segregating traffic by using VLANs. A layer-2 switch will have only one collision domain. It means, the bandwidth is shared by all the ports in the switch. One way to increase the bandwidth is by segregating traffic by using VLANs.

The benefits of VLANS include:

1. Easy Administration resulting in reduced administration costs

2. Increased Security due to broadcast control, if you are using simple hub, you can observe traffic corresponding to any node by simply inserting a Network analyzer.

3. Grouping based on functional requirements irrespective of physical location of nodes,

4. Simplify moves, adds, changes,

5. Distribution of traffic thereby using the network bandwidth more efficiently.

- We can transmit data over lines used for electric power through the utilization of Broadband over power lines (BPL), also known as Ethernet over power lines.
- **Ethernet over HDMI:** This technology is geared toward utilizing unused wiring in the HDMI cable Ethernet rather than needing to run another cable.
- **DOCSIS (Data Over Cable Service Interface Specification)** is an international standard that governs the addition of high-speed data over cable TV (CATV) systems.
- **Power Line Communication (PLC)** is a communication technology that enables sending data over existing power cables.

There are typically two types of addresses used:

1. Logical address: IP address of a node 202.199.100.2 is an example of logical address. The addressing scheme is compliant to IPv4. The address

FEDC:BA98:7654:3210:FEDC:BB98:7654:3210 is compliant to IPv6. IP version 6 addressing scheme is being used due to scarcity of IP addresses using IP version 4. That is, the Internet is almost running out of logical addresses (uniquely identifiable over the Internet) using IPv4. Due to larger number of bits used in IPv6, it can take several billions of logical addresses

2. Physical address: Physical address also called MAC address.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

Format 1 - MM:MM:MM:SS:SS:SS

Format 2 - MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example,

00:A0:C9:14:C8:29

The prefix 00A0C9 indicates the manufacturer is Intel Corporation.

The number 14C829 is the serial number assigned by the manufacturer.

A switch forwards data it receives, to only the port that connects to the destination device. It does this by the MAC address of the devices attached to it and then by matching the destination MAC address in the data it receives.

ARP table: ARP Short for Address Resolution Protocol, the purpose of arp cache table is to minimize network load by minimizing repeat address resolutions. As we know, the purpose of arp is to resolve an IP address to its hardware (MAC) address. The resolved addresses (IP/MAC address pair) are kept temporarily in an arp cache table for future reference. The entries in arp cache can be deleted using proper system commands. If the dynamic entries are deleted, the arp software builds the cache automatically (as and when the need arises), and there is no need to enter these dynamic cache entries manually. ARP cache entries are added to an arp cache table either as static entries (manually entered) or as dynamic (system learned) entries. The cache entries help in minimizing the network load, since it is not necessary to resolve an IP address to hardware address every time a packet is received.

MAC Address Table: MAC is short for Media Access Control. The MAC address is 6 bytes long. The first three bytes identify the manufacturer, and the last three bytes identify the station address. A MAC address is an address, which works on the Data Link Layer (Layer 2 of the OSI Model). The Data Link Layer consists of two sublayers, the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. A MAC address is 48 bits long. MAC address is a unique 12-digit hexadecimal number that is stamped into every network interface card. MAC address is assigned to the NIC and identifies the resource physically.

A sample MAC address looks like **00-0C-F5-5A-98-AD**

Power over Ethernet (PoE) is a technology for wired Ethernet LANs (local area networks) that allows the electrical current necessary for the operation of each device to be carried by the data cables rather than by power cords.

Performance concepts:

Traffic shaping: It is a strategy to optimize performance and manage traffic on a network. For example, if there are any real time applications, they need to be prioritized over regular traffic such as file transfer. Traffic shaping enables a network administrator to prioritize traffic based on performance and user requirements. Traffic shaping, also known as "packet shaping," is the practice of regulating network data transfer to assure a certain level of performance, quality of service (QoS) or return on investment (ROI). The practice involves delaying the flow of packets that have been designated as less important or less desired than those of prioritized traffic streams. Regulating the flow of packets into a network is known as "bandwidth throttling" Regulation of the flow of packets out of a network is known as "rate limiting."

QoS can be quantified by the following methods:

1. CoS: Class of Service. CoS is applied at Layer 2 or at frames level. A 3-bit value (known as priority bits) in the range of 0 to 7 is carried along the frames in a VLAN trunk. 0 represents the lowest priority, and 7 represents the highest priority.

2. IP Precedence: IP Precedence is a 3-bit value represented in the ToS (Type of Service) byte of Layer 3 IP packets. Here also, value 0 represents the lowest priority and 7 represent the highest priority.

3. DSCP: DSCP stands for Differentiated Service Code Point. DSCP. DSCP consists of a 3-bit Selector, and a 3-bit Drop Precedence value. DSCP is backward compatible with IP Precedence, and works at layer 3.

NAT: Short for Network Address Translation offers security by translating internal IP addresses to public IP addresses and vice versa. IP address translation is typically the function of a NAT router. As the name implies, it is used to translate one IP address to another. Typically, NAT is used when you want to translate private range of IP addresses to public (global) range of IP address and vice versa.

For example, you have a local network that uses private IP addresses. You can not access the Internet using private IP addresses. You need to translate the private IP to public IP. NAT just does this. This feature has an added benefit that it hides the actual workstation accessing the Internet behind NAT.

Although Proxy server appear to be similar to NAT, a proxy server actually does the work of connecting to, responding to, and receiving traffic from the Internet. In other words, it actively acts on behalf of the client computer by dissecting the packets and participating in the session. A NAT, on the other hand, merely changes the IP address of traffic coming through it and passes it to the Internet and vice versa. The computer behind the NAT, not the NAT itself, does the work. The NAT is intended to be transparent to the whole process.

The difference between a proxy and a NAT is that the proxy server works on the transport layer (layer 4) or higher of the OSI model, whereas a NAT works on the network layer (layer 3).

Following statements are true about NAT

1. NAT allows several hosts be connected to Internet by using fewer globally unique IP addresses. This in turn results in conserving the scarce public IP addresses. The terms public / global is used in the sense that the IP addresses are globally unique and officially registered.

2. NAT supports load sharing on inside machines. The inside machines are accessed in a round robin fashion, thus sharing load.

3. NAT offers some degree of security since IP addresses are not easily traceable. This is because, the actual host IP that is accessing the Internet is translated into outside IP address and vice versa. Thus, NAT offers protection against hacking.

4. One disadvantage of NAT is that it increases delay. This is obvious since address translation is involved.

5. Another disadvantage of NAT is that, when an application uses physical IP address, it may not function properly. This is because the physical IP address is changed by NAT.

Routing:

IP routing: When routing a packet through an inter network, the MAC (or hardware) addresses change after each hop, where as the logical (IP) addresses of the source and destination remain constant.

While a packet travels through an Internetwork, it usually involves multiple hops. It is important to know that the logical address (IP address) of source (that created the packet) and destination (final intended destination) remain constant, whereas the hardware (interface) addresses change with each hop.

When a router network is powered up, routers communicate with other routers in the network and exchange information according to the routing protocol in use (for example, RIP). Each router then follow algorithms as specified in the routing protocol and arrive at a common routing table. The process of all routers agreeing on a common routing table is called convergence.

Note that some networks may run more than one routing protocol at a given time. Then, the routers will maintain routing tables for each routing protocol separately. One routing protocol is unaware of the other, like ships in the dark.

Routing and Routed Protocols: Routing protocols job is to maintain routing tables and route packets appropriately. Routers can support multiple independent routing protocols and can update and maintain routing tables for each protocol independently.

Examples of routing protocols are RIP, EIGRP, and OSPF.

Routed protocols are used to transport user traffic from source node to destination node.

Examples of routed protocols are IP, IPX,and AppleTalk.

Route summarization: It is also called route aggregation, is a method of minimizing the number of routing tables in an IP (Internet Protocol) network. It works by consolidating selected multiple routes into a single route advertisement, in contrast to flat routing in which every routing table contains a unique entry for each route.

Routers send link-state advertisements (LSAs) to advertise the networks they know how to reach. Routers then use those LSAs to construct the topological map of a network. The algorithm run against this topological map is Dijkstra's shortest path first(SPF) algorithm.

The process of failing over from one route to a backup route is called **convergence**.

Routing loops : A routing loop is a problem which happens when a data packet is continually routed through the same routers over and over. The data packets continue to be routed within the network in an endless circle. A routing loop can have a catastrophic impact on a network, and in some cases, completely disabling the network. Normally Routing Loop is a problem associated with Distance Vector Protocols.

- Routing loops are less of a problem with link-state routing protocols
- Route redistribution supports exchange of routing information on network running different routing protocols.
- Routing metric is a unit calculated by a routing algorithm for selecting or rejecting a routing path for transferring data/traffic.

The following are some of the important characteristics of an autonomous system:

1. An autonomous system consist of routers, that present a consistent view of the routing to the external world.

2. Exterior routing protocols are used for communication between autonomous systems

3. Interior routing protocols are used within a single autonomous system

4. An autonomous system can run both interior and exterior protocol simultaneously. However, Interior protocols such as RIP, IGRP are used for communication within the autonomous system, and exterior routing protocols such as BGP are used for communication between autonomous systems.

The default metric for a redistributed route should be set to a value larger than the largest metric within the AS.

Exterior Gateway Protocol (EGP) is a Routing Protocol which is used to find network path information between different Autonomous Systems. The primary EGP is used in almost all networks is the Border Gateway Protocol (BGP).

Interior Gateway Protocol (IGP) is a Routing Protocol which is used to find network path information within an Autonomous System. Some examples of IGP protocols are: RIP, OSPF, and EIGRP.

Distance vector routing protocols: Distance-vector routing protocols typically use one of two approaches for preventing routing loops:

1. Split horizon: The split-horizon feature prevents a route learned on one interface from being advertised back out of that same interface.

2. Poison reverse: The poison-reverse feature causes a route received on one interface to be advertised back out of that same interface with a metric considered to be infinite.

The following are distance vector protocols:

RIPv1, RIPv2, IGRP, and EIGRP are distance vector protocols. However, EIGRP supports classless routing. IS-IS (Intermediate System-to-Intermediate System) is an OSI link-state hierarchical routing protocol uses link-state information to build routing tables.

Link state routing protocol: Intermediate System-to-Intermediate System protocol (IS-IS) is a link state routing protocol. It is based on a routing method known as DECnet Phase V routing, in which routers known as intermediate systems exchange data about routing using a single metric to determine the network topology.

Administrative distance: It is the feature used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value

The following are the administrative distance default values of protocol

Route Source	Default Distance values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

RIP: This is a simple distance vector protocol. It has been enhanced with various techniques, including Split Horizon and Poison Reverse in order to enable it to perform better in somewhat complicated networks. Maximum hop count supported by RIP is 15. A hop count of 16 or greater is considered unreachable.

Benefits of OSPF routing over RIPv1:

RIP: RIP for IP can be used to automatically update routing tables from other routers. IPX can not be used for TCP/IP traffic. DHCP and NETSTAT are not routing protocols.

OSPF is a link state technology that uses Dijkstra algorithm to compute routing information. It has the following advantages over Distance Vector protocols such as RIP:

1. Faster convergence: OSPF network converges faster because routing changes are flooded immediately and computer in parallel.

2. Support for VLSM: OSPF supports VLSM. However, please note that RIP version2 also supports VLSM.

3. Network Reachability: RIP networks are limited to 15 hops. Therefore, networks with more than 15 hops can not be reached by RIP by normal means. On the other hand, OSPF has practically no reachability limitation.

4. Metric: RIP uses only hop count for making routing decisions. This may lead to severe problems in some cases, for example, that a route is nearer but is very slow compared to another route with plenty of bandwidth available. OSPF uses "cost" metric to choose best

path. Cisco uses "bandwidth" as metric to choose best route.

5. Efficiency: RIP uses routing updates every 30 seconds. OSPF multicasts link-state updates and sends the updates only when there is a change in the network.

Border Gateway Protocol (BGP): BGP is the most commonly used for connecting two or more autonomous networks. RIP, OSPF, EIGRP, and IS-IS are suitable for connecting homogenous networks. BGP is widely used for connecting two or more ISPs together. BGP is recommended only when connectivity is required between two disparate networks. Disconnecting the router from the network may disable some networks from reaching the other networks. It is recommended to configure default route while the router is being configured.

The following are Interior Gateway protocols (IGPs)

OSPF, RIP, RIPv2, EIGRP, IS-IS

BGP is an Exterior Gateway protocol (EGP).

Previous Contents Next

CompTIA® Network+ Exam Notes : Wireless Network Technologies

examguides.com/Networkplus/network-plus-6.htm

1. Networking Concepts

1.6 Wireless technologies

The term wireless refers to the communication or transmission of information over a distance without requiring wires or cables. The devices used for wireless communication may include cordless telephones, mobiles, GPS units, ZigBee technology, wireless computer parts, satellite television, etc. Wireless Networking technologies connect multiple computers, systems and devices together without requiring wires or cables: a wireless local area network or WLAN comes under Wi-Fi. Most of our discussion would be in wireless LANs and related areas as per the broad objectives of the exam.

802.xx standards:

1. IEEE 802.1 : Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging.

2. IEEE 802.3 describes CSMA/CD Ethernet standard.

3. IEEE 802.4 is a standard for Token bus networks.

4. IEEE 802.5 describes Token Ring networks.

5. IEEE 802.10 : Standards for LAN/MAN security implementations.

6. IEEE 802.11: Standard for wireless LAN.

The following are the important features of 802.11 standard:

1. The 802.11g standard supports data rates up to 54 Mbps, whereas 802.11b supports data rates only up to 11 Mbps.

2. The hardware complying to 802.11g operates at 2.4 GHz range

3. The 802.11g equipment is as susceptible to interference as 802.11b.

4. IEEE 802.11g is compatible with 802.11b, but not compatible with 802.11a, or Bluetooth.

5. 802.11n works in both 2.4GHz, and 5GHz bands. The standard supports up to 600Mbits/sec bandwidths. It is downward compatible with 802.11a, 802.11b, and 802.11g standards.

6. 802.11a, and 802.11g use OFDM (short for Orthogonal Frequency Division Multiplexing). IEEE 802.11b uses DSSS (short for Direct Sequence Spread Spectrum) for encoding.

7. IEEE 802.16 : Wireless Networking - "WiMAX"

The data rates supported by various wireless standards are as given below:

TABLE : IEEE 802.11 PHY STANDARDS

Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna Technologies	Maximum data rate
1997	802.11	2.4	20	DSSS,FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4.5	20,40	OFDM	MIMO,up to four spatial streams	600 Mbits/s
2013	802.11ac	5	20,40,80,160	OFDM	MIMO,MU-MIMO,up to eight spatial streams	6.93 Gbits/s

Bluetooth has the lowest data rates (up to 1 Mbps), whereas 802.11ac supports very high data rates.

Important Points to Remember:

802.11 standards are typically used in wireless LAN configurations. Bluetooth supports low speeds up to 1 Mbps over short distances up to a max of 30 feet. The technology is well suited for connecting PDAs or wireless mouse to a computer.

802.11g is compatible with 802.11b. Note that 802.11b is not compatible with either 802.11a or 802.11g. Similarly, 802.11a is not compatible with either 802.11b or 802.11g. Therefore, from compatibility point of view, 802.11g, and 802.11ac have better compatibility.

All Bluetooth, 802.11b, and 802.11g use 2.4GHz spectrum, where as 802.11a uses 5 GHz spectrum. Note that 2.4GHz band is more susceptible to noise compared with 5 GHz because several ISM band compatible devices work in the 2.4GHz frequency band.

IEEE 802.3 defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

Rendezvous, based on open Internet Engineering Task Force (IETF), uses standard networking protocols and zero configuration technology to automatically discover and connect devices over any IP network, such as Ethernet or 802.11-based wireless networks like Apple's Airport.

IEEE 802.11x is the standard that pertains to wireless LANs.

802.11ac is called Gigabit Wi-Fi or 5G Wi-Fi.

802.11ac is a 5-GHz only technology that can use wider channels in the 5-GHz band, more spatial streams, and multi-user MIMO (MU-MIMO) as shown in the figure.

Data Rates for Different Wireless Configurations			
No. of spatial streams	Channel spectral width (MHz)	802.11ac Modulation Scheme MCS 8/9*	802.11n Modulation Scheme MCS 7
1	20	86.7 Mb/s	72.3 Mb/s
1	40	200 Mb/s	150 Mb/s
2	40	400 Mb/s	300 Mb/s
4	40	800 Mb/s	600 Mb/s
1	80	433 Mb/s	N/A
2	80	867 Mb/s	N/A
3	80	1.3 Gb/s	N/A
4	80	1.69 Gb/s	N/A
1	160*	867 Mb/s	N/A
4	160*	3.39 Gb/s	N/A
8*	160*	6.77 Gb/s	N/A
* Optional feature			

Worldwide Interoperability for Microwave Access (WiMAX) is based on 802.16.

- IEEE 802.11 : Wireless LAN (WLAN) and Mesh (Wi-Fi certification)
- IEEE 802.14 : Cable modems
- IEEE 802.15 : Wireless PAN
- IEEE 802.16 : Wireless Networking - "WiMAX"

- IEEE 802.15.1 : Bluetooth
- IEEE 802.14 : Standards for cable television broadband communications.

Previous Contents Next

CompTIA® Network+ Exam Notes : Basic Cloud Concepts

examguides.com/Networkplus/network-plus-7.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

1. Networking Concepts

1.7 Cloud concepts

Given below are some of the widely used Cloud Service models:

1. SaaS (Software as a Service)

2. PaaS (Platform as a Service)

3. IaaS (Infrastructure as a Service)

4. Mobile "backend" as a service (MBaaS)

5. Serverless computing

6. Function as a service (FaaS)

Software as a Service (SaaS): is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. An application service provider (ASP) provides application software access to subscribers. This service is sometimes called Software as a Service (SaaS). In SaaS (Software as Service), typically access is provided to a software application.

Infrastructure as a Service (IaaS): IaaS providers offer computers - physical or (more often) virtual machines and other resources like servers, load balancers, raw block storage, file or object storage, firewalls, IP addresses, virtual local area networks (VLANs), and software bundles.

The following may be considered under this model:

- **Naas (Network as a Service):** The service provider offers services like e-mail and DNS for use by the clients. This might be categorized under Infrastructure As Service.
- **Security as a service (SECaaS):** is a business model in which a large service provider integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own, when total cost of ownership is considered. This also could be categorized as a constituent of Infrastructure As A Service.
- **Storage as a service (StaaS):** It is an architecture model in which a provider provides digital storage on their own infrastructure. Storage as a service can be implemented as a business model in which a large service provider rents space in their storage infrastructure on a subscription basis. This could be categorized as a constituent of Infrastructure As A Service.

Platform as a Service(PaaS): Paas is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser. Platform as a Service allows users to create software applications using tools supplied by the provider. PaaS services can consist of preconfigured features that customers can subscribe to; they can choose to include the features that meet their requirements while discarding those that do not.

Examples to PaaS offers include Operating system, Server-side scripting environment, Database management system, Server Software, Support, Storage , Network access.

Previous Contents Next

CompTIA® Network+ Exam Notes : Network Services

examguides.com/Networkplus/network-plus-8.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

1. Networking Concepts

1.8 Network Services

DHCP Service: DHCP scopes enables ranges of IP addresses, to be defined on a system running a DHCP server application. When a network device is assigned an IP address from an appropriate DHCP scope, that assignment is not permanent. Rather, it is a temporary assignment referred to as a lease . A specific MAC address is mapped to a specific IP address, which will not be assigned to any other network device. This static addressing approach is referred to as a DHCP reservation .

The Internet Protocol Helper (IP Helper) API enables the retrieval and modification of network configuration settings for the local computer.

DHCP scopes enables ranges of IP addresses, to be defined on a system running a DHCP server application.

DHCP relay forwards DHCP requests between the server and the clients.

When a network device is assigned an IP address from an appropriate DHCP scope, that assignment is not permanent. Rather, it is a temporary assignment referred to as a lease .

DNS Services: The core administrative unit in DNS is called a "zone". A zone is a physical file composed of resource records that define a group of domains. A domain is a node in the DNS name-space and all sub-domains below it. DNS is used for host name to IP address

resolution.

Any web server can be made to be present on the public Internet by using an external DNS name and a public IP address. Of course, you need to ensure physical connectivity to the Internet, and a broadband router with ISP connection is a good solution for this. Web server listens to port 80, therefore, you need to enable port 80 (incoming) on the router. HOSTS file is used like DNS for resolving Domain names, whereas LMHOSTS file is used like WINS for resolving NetBIOS names. Note that, if you are using HOSTS file for resolving Domain names, you need to load the HOSTS file on all computers on the network that need to access the domain names. This is in contrast with DNS, which is located on a central server.

The IP address and domain name go in one line for ex: **196.54.202.16 ns.dname.com**

Also note that the HOSTS file is an ASCII file and can be edited using Notepad or any other text editor. HOSTS file resolves the domain name to corresponding IP address. The DNS server needs to be specified for connecting using FQDN (Fully Qualified Domain Name).

The most common type of DNS record is a Host record (also called an A record). In the Internet, a Host record is used to associate a domain name (FQDN - Fully Qualified Domain Name) with an IP address.

An MX record stores the IP address of your SMTP server, so e-mail clients can determine where a message should be sent. They perform a DNS query against a domain's MX record to get the IP address of the organization's SMTP server.

An Alias record's job is to associate an alternate name with a computer for which there is already a Host record. For example, suppose that the host record for relevant looked like this: Relevant Host (A) 200.100.100.199

Alias record is like a redirect. For example, you have a site mydomain.com. However, someone enters www.mysite.com, You want him or her to be directed to the web.mysite.com. Since there is no server on the network named "www," set up an Alias record that associates www with mysite.com. The Alias record looks something like this: www Alias (CNAME) mysite.com

WINS resolves NetBIOS names to IP addresses.

DNS Record Types:

A - specifies IP addresses corresponding to your domain and its subdomains

MX - specifies where the emails for your domain should be delivered

CNAME - specifies redirects from your domain's subdomains to other domains/subdomains

TXT - these records are used to store text-based information related to your domain. One of their most common uses is for SPF data. SPF, or Sender Policy Framework

SRV - Each SRV record has the following form:

where each of the attributes should have a specific value:

- service - the name of the service in question.

- proto - the protocol of the service (usually TCP or UDP).

- name - the domain name that the record should be valid for (Note: it should end with a dot).

- TTL - time to live

- priority - lower values mean more preferred.

- weight - used for records with the same priority (higher value means more preferred).

- port - the number of the port.

- target - the hostname of the machine where the service is running (Note: it should end with a dot).

TTL, Priority, Weight, Port and Target are straight forward and easy to fill out. The values will be given by the company that will generate the SRV Record for you.

Here is an example of an SRV record: _sip._tcp.example.com. 3600 IN SRV 10 60 5060 bigbox.example.com.

WINS is used for NetBIOS name resolution. DHCP is used for assigning IP addresses to client computers dynamically. SNMP is used for remote monitoring of a TCP/IP network.

Previous Contents Next

CompTIA® Network+ Exam Notes : Different Types Of Cabling Standards

examguides.com/Networkplus/network-plus-9.htm

2. Infrastructure

2.1 Different types of cabling standards

Ethernet cables are grouped into sequentially numbered categories ("cat") based on different specifications; sometimes the category is updated with further clarification or testing standards (e.g. 5e, 6a). These categories are how we can easily know what type of cable we need for a specific application.

	Speed	Limitation
CAT3	16 Mbps	Ineffective for Higher - speed networks often found in older 10 BaseT networks, now obsolete.
CAT5	100 Mbps	Range of 100 meters
CAT5e	1000 Mbps	Range of 100 meters
CAT6	10/100/1000 Mbps and 10 Gbps	Range of 100 meters
CAT6e	10/100/1000 Mbps and 10 Gbps	Range of 100 meters
CAT7	10/100/1000 Mbps and 10 Gbps	Range over 100 meters

Important points to remember

Cat 5e or better cable type is used for Gigabit Ethernet network cabling. Cat5e cable contains four twisted pairs of wires for Gigabit Ethernet

Category 3 - Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.

Category 5 - Can transmit data at speeds up to 100 Mbps. Widely used in 100Base-T Ethernet networks.

Category 5e - Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps]). The Cat-5e cable may be used in 1000BaseT Ethernet network. Both Cat -5 and 5e are almost same, except for better noise (cross talk, etc.) specs associated with 5e.

Category 6 cable, commonly referred to as Cat-6, is a cable standard for Gigabit Ethernet and other network protocols that is backward compatible with the Category 5/5e and Category 3 cable standards. The cable contains four twisted copper wire pairs. This is the same as CAT5 and CAT5e copper cable standards. The cable standard is suitable for 10BASE -T / 100BASE-TX and 1000BASE -T / 1000BASE-TX (Gigabit Ethernet).

The Category 7 cable standard has been created to allow 10 Gigabit Ethernet over 100 m of copper cabling. CAT 7 is backwards compatible with traditional Cat5 and Cat6 Ethernet. Cat7 offers strict specifications for crosstalk and system noise than Cat6. Shielding has been added for individual wire pairs on the Category 7 cable. Cat7 has been designed as a standard for Gigabit Ethernet over 100m of copper cabling The cable contains four twisted copper wire pairs, just like the earlier standards.

CAT6 is rated for gigabit Ethernet while CAT6e is thicker and rated for 10 gig Ethernet. Typically CAT5e is sufficient and can also handle gig Ethernet, but noise margin will be less.

Connector Types:

Fiber Connectors: The below figure shows the different fiber connector types .

1. ST connectors: These connectors are the most common type of commercial fiber optic connector. These connectors utilize an exposed plastic tube housing the optical fiber. This requires a connection to a matching cable on the other side, incorporating a connector that mates to the other. These combine in a spring-loaded twist, reminiscent of BNC connectors, and are noted for their reliability. ST connector is very popular in communication applications, such as LANs and CCTV systems.

2. SC-Connector: SC is short for Subscriber Connect is one of the most frequently used connectors. Used in fiber-optic networking, it has caps to prevent laser light reaching eyes. The connector usually in pairs (transmit and receive), often clipped together. connectors have the ferrule that houses the fiber mostly concealed. Probably the most similar

commercial equivalent of To slink, SC connectors does not require a mating cable on the other side. Instead, these snap-on connectors simply push into their jacks with a click. SC connectors use a push-pull design and can be used for simplex or multiplex applications

3. FC connector: It is similar to ST connectors, these fiber optic connector's screws into their mating jacks. Additionally, the tube surrounding the optical fiber is typically shrouded in ceramic or metal, as opposed to being fully exposed. The inner ring of the connector is keyed to ensure positive mating to its corresponding jack. FC connectors are primarily used with single mode fibers and used in telephone, instruments, and high-speed communication links. The style is similar to that of an ST connector, but it uses a threaded connection which makes it better suited for high vibration environments

4. LC cables: latch and release into their jacks in a manner similar to Ethernet connectors. Smaller in form than SC connectors, their durability is not compromised, nor is cost increased. Instead of snapping or thermo forming the connector to the cable, it is glued. This makes it a popular connector for field use. LC connectors are used in private and public networks, and are gaining in popularity due to their small form factor (SFF) optical transmitter/receiver assembly

LC connector is a miniaturized version of the fiber-optic SC connector. It looks just like the SC, but is half the size with a 1.25 mm ferrule instead of 2.5 mm. 1000BASE-FX should use SC, ST, LC, MTRJ or MIC connectors with SC being the preferred option.

Usually, cable modems use F-type female connector to connect to the broadband provider.

ST (Short for Straight Tip) connectors, and SC (short for Subscriber Connect) connectors are typically large connectors. MT-RJ, and LC (short for Local Connector) have small form factor, and allow higher port density. These connectors (MT-RJ and LC) allow higher number of fiber optic connections in a smaller area, and hence desirable when there are a large number of fiber optic terminations to be made.

Copper Connectors:

BNC- T connector: The figure shows a BNC-T connector.

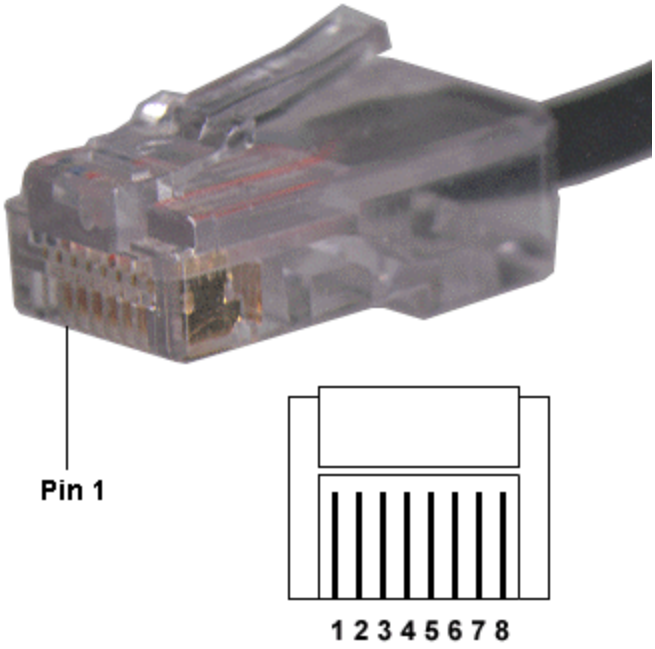
10BaseT and 100BaseT use RJ-45 type of connector. 10Base2 (also called Thinnet) uses BNC connectors for attaching workstations. BNC-T is used to connect a workstation to the Thinnet coaxial cable. The BNC-T(m) connector end mates with the BNC(f) connector on the NIC card. The BNC-T(f) connector ends are attached to BNC(m) cables, that in turn attach to other computers through BNC-T connector. BNC connector is a co-axial connector, and used in 10Base2 networks.

BNC /Thinnet cable: 10Base2 network uses BNC cable as medium for physical transmission of electrical signals. The fig shown below is a BNC cable with male connectors.

RJ-45 : The connector shown in the exhibit is RJ-45 connector.

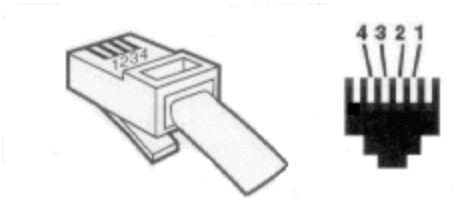
RJ-45 connector is the most commonly used connector in 10BaseT, and 100BaseT networks. RJ-11 connectors are commonly available either with 4-wire or 6-wire, whereas RJ-45 has 8 wires (4-pairs). An RJ-45 connector has 8 connection pins and can accommodate 4 pairs of wires. Typically, a UTP cable with RJ-45 connectors is used to connect the NIC card on the home computer with the DSL broadband modem. RJ-45 connectors have 8 contacts. RJ-45 connector is most commonly used in 10BaseT, and 100BaseT networks. RS-232 is a serial port specification. RJ-48C connectors are 8-pin jacks (think RJ-45) used with T1 lines. Pins 1, 2, 4, and 5 are used for data (1 and 2 for receiving; 4 and 5 for transmitting), and pins 7 and 8 are used for cable shield integrity. Pins 3 and 6 are not used.

- RJ-11 (Registered Jack) connectors are small plastic connectors used on telephone cables.
- RJ-45 connectors are used with twisted-pair cabling. RS-232 (Recommended Standard) is a TIA/EIA standard for serial transmission between computers and peripheral devices
- A common connection type used to connect to a CSU/DSU is an RJ-48C.



The connector shown in the exhibit is a 4-wire RJ-11 connector. RJ-11 connectors are also available in 6-wire.

Two frequently used Firewire connectors are 4-pin connector, and 6-pin connector. A 4-pin connector does not carry power through the connector, whereas a 6-pin connector carries the dc-power required for operating the connected device.



Fiber optics connector

MT-RJ (Mechanical Transfer Registered Jack): This uses a form factor and latch like the RJ-45 connectors, supports full duplex. It costs less than ST or SC connectors, and is easier to terminate and install than ST or SC.

RS-232 (Recommended Standard) is a TIA/EIA standard for serial transmission between computers and peripheral devices such as modems, mice, and keyboards. RS-232 commonly uses a 25-pin DB-25 connector or a nine-pin DB-9 connector.

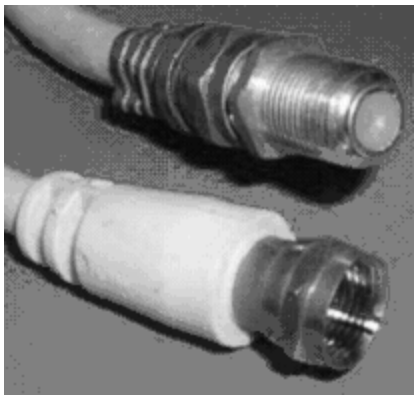
DB 15 connector can be found on sound cards, older AUI network cards and devices, as well as legacy Macintosh monitors. This is commonly referenced as the Game port. This is due to the fact that the most common peripheral for this port was a joystick or video game controller.

DB 37 connector is used sometimes with Cisco networking hardware, and other applications that use RS-449 serial communication.

HD15 is a High Density DB-style connector, so it can also be called an HD DB15. It is used in video applications that support much higher resolutions.

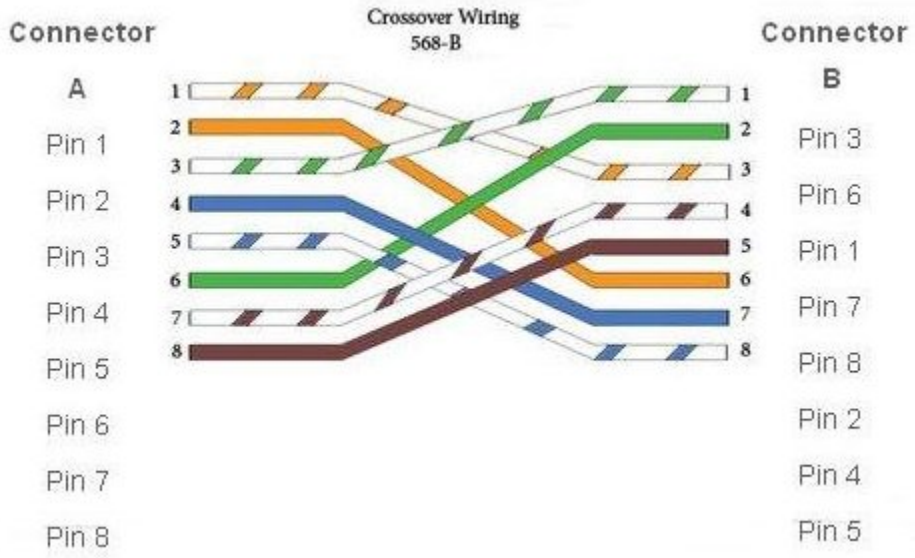
F-type connector: The exhibit shows an F-Connector. F-Connector is widely used in TV and Video displays

Copper termination standards

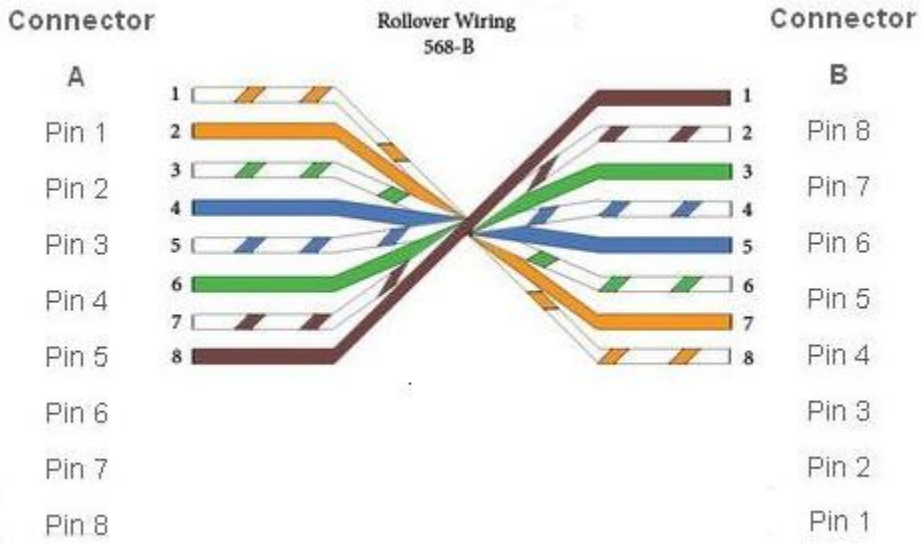


T568A and T568B are the two color codes used for wiring eight-position RJ45 modular plugs. Both are allowed under the ANSI/TIA/EIA wiring standards. The only difference between the two color codes is that the orange and green pairs are interchanged.

TIA/EIA 568a and TIA/EIA 568b:

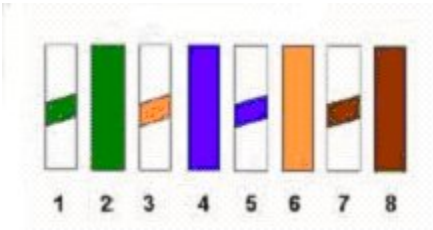


Crossover wiring in T568B



Rollover wiring in T568B

The color coding shown in the figure corresponds to EIA/TIA 568A standard. For EIA/TIA 568B standard, the green and orange wires are interchanged. By following 568A on either end of the cable, you are preparing straight cable. If one end of the cable is 568A and the other end is 568B, the you are preparing a cross cable.



Straight-through cables: These are primarily used for connecting unlike devices. All wire pairs are in the same order on each end of the cable. A straight-through cable is typically used in the following situations:

- Connecting a router to a hub
- Connecting a computer to a swtich
- Connecting a LAN port to a switch, hub, or computer

Crossover cables: These are very similar to straight-through cables, except that they have pairs of wires that crisscross. This allows for two devices to communicate at the same time. Unlike straight-through cables, we use crossover cables to connect like devices.

- Connecting a computer to a router
- Connecting a computer to a computer
- Connecting a router to a router
- Connecting a switch to a switch
- Connecting a hub to a hub

Rollover cables: Rollover cables like other cabling types, got their name from how they are wired. Rollover cables essentially have one end of the cable wired exactly opposite from the other. This essentially "rolls over" the wires. Rollover cables, also called Yost cables, usually connect a device to a router or switch's console port. This allows a programmer to make a connection to the router or switch, and program it as needed. These types of cables are generally not used very much, so are usually colored differently from other types of cables.

USB Connector:

An USB (short for Universal Serial Bus) has the following properties:

- High-speed serial connections (1.5MBytes/sec to 12MBytes/sec)
- Hot-pluggable
- Software designed to recognise USB devices on connection
- Hubs can be used to extend the number of USB compatible devices connected to a computer
- It has 4 pins:
    - VCC - Power (+5 volts, up to 500mA)
    - D- - Data input to computer
    - D+ - Data output from computer
    - GND - Ground

USB connectors are of two types, "type A" - flat type usually used on computer end; "type B" used on devices.

Ethernet deployment standards:

The distance specification for various media type is as given below:

Standard	Media	Max. Length
1000BaseT	Cat 5 UTP, 4 pair	100 meters
1000BaseSX	Multi-mode fiber cable	260 meters
1000BaseLX	Single mode fiber cable	3 km
100Base-FX	Multi-mode fiber cable	2km
10GBase-SR	Multi-mode fiber cable	26-82m
10GBaseER	Single mode fiber cable	40km
10GBaseSW	Multi-mode fiber cable	200M
10GBaseT	Cat 6a (or higher)	100m

Important points to remember

The 100BASE-TX specification defines 100Mbps Ethernet transmission across Category 5 UTP cable and Type 1 STP cable at distances up to 100 meters. 100BASE-TX uses 2 pairs (4 wires) in the Two-Pair wire bundle. Most 100BASE-TX products support category 5 UTP cabling only. Ethernet 10BaseT is the most widely used network based on star topology.

10Base2 cable uses 50 Ohm, RG-58 cable also called Thinnet. 10Base2 is a Bus type topology. Signal traveling on one direction will reflect after reaching the far end, if no termination is provided. Therefore, termination is required at both ends of a 10Base2 Ethernet network.

10Base5 cable uses 50 Ohm, RG-8, or RG-11 cable also called Thicknet.

For connecting two network nodes which are more than 500m apart without any repeater and on a single segment, a 100BaseFX is proper choice. Note that even10Base2 (185m) and 10Base5 (500m) can also achieve this distance if more segments are used using repeaters.

Note that the prefix indicates the maximum speed. For example, 100BaseFX has a maximum speed of 100Mbps, and 10Gbase has a maximum speed of 10Gbps.

Gigabit Ethernet conforms to IEEE 802.3z.

One of the disadvantages of 10Base2 Ethernet is that, any cable break at any point on the network may cause breakdown of the entire network. 10BaseT Ethernet specifies UTP cabling. UTP cabling uses RJ-45 connectors to connect the cable to the NIC (Network Interface Card).

100 pair cables are used as feeder cables for large telephone company installations. 100 pairs of wires are combined in to a large insulated cable for running through the telephone installations.

1000BaseT uses cat 5e or better UTP cable. The standard uses four pairs of wires and support a maximum distance of 100 meters. Supports a maximum speed of 1000Mbps. Note that 100BaseTX uses only 2 pairs of Cat 5 cable.

10Gbase-LW(802.3ae) - supports 10 km, cable type used: Single mode fiber (SMF), typically used with SONET

10Gbase-EW(802.3ae) - supports 40 km, cable type used: Single mode fiber (SMF)

10Base2 can support maximum cable length of 185 meters. The specification for Thinnet is RG 58 A/U or RG 58 C/U co-axial cable. Thinnet uses BNC connectors along with T connectors required to connect to the BNC female connector on the NIC.

The speeds supported by various fiber cables types are as below:

10Gbase-SR: Supports a max speed of 10Gbps up to 300 meters. It uses multimode fiber, 850nm laser.

10Gbase-ER: Supports a max speed of 10Gbps up to 40 kilometers. It uses single-mode fiber, 1310 nm laser.

10Gbase-SW: Supports a max speed of 10Gbps up to 300m. It uses multimode fiber.

10Gbase-T: Supports a max speed of 10Gbps up to 100m. It uses Cat 6a (or higher)

10GbaseT uses UTP cabling and connect to networks using Fast Ethernet. The standard supports a maximum distance of 100 m.

1000BaseT: utilizes all 4 pairs of a Category 5 cable.

10BaseT Ethernet: uses RJ-45 connectors at the ends of the UTP cable.

10GbaseLR: Supports a max speed of 10Gbps up to 10 kilometers. It uses single-mode fiber, 1310nm laser

FDDI: Supports a max speed of 100Mbps up to 10 kilometers. It uses multi-mode fiber.

100BaseT (Fast Ethernet) uses IEEE803.2u standard which incorporates CSMA/CD protocol.

10BaseT (this is part of the IEEE 802.3 specification), has a distance limit of approximately 100 meters (328 feet) per segment.

Copper Cable standards: Category 5 straight cable is used to connect a workstation to a switch or a hub in 100BaseTX Ethernet network. A crossover cable is used to connect a hub/switch to another hub/switch.

You need to use crossover cable to connect two network Hubs, and straight cables to connect workstations to the Hub. A crossover cable directly connects two compatible network devices to each other over Ethernet. Ethernet crossover cables are commonly used when networking two devices in situations where a network router, switch or hub is not present. Compared to standard Ethernet cables, the internal wiring of Ethernet crossover cables reverses the transmit and receive signals.

Termination points:

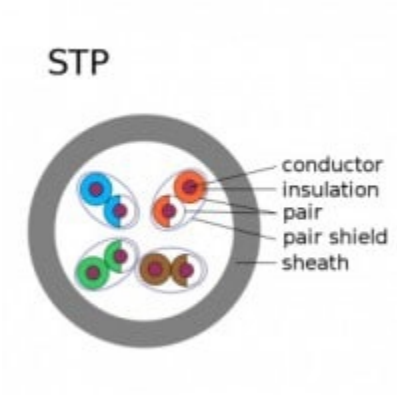
Patch panel: A patch panel is a panel that contains multiple cable connections. The back of the panel has cabling that runs to disparate equipment or networks. The front of the patch panel allows easy access to connect the different equipment (or networks) through the use of short patch cables. One common example of this concept was before automatic telephone switching became widespread; early telephone operators would connect callers to their intended parties manually by plugging in a cable on the switchboard.

Media types:

STP stands for Shielded Twisted Pair and UTP stands for Unshielded Twisted Pair.

Shielded Twisted Pair (STP): STP cables reduce electrical noise and electromagnetic radiation. In other words, they help to keep the signal steady, and reduce interference with other devices. Given below is a diagram showing a typical shielded twisted pair cable

Unshielded Twisted Pair (UTP): UTP cables do not have shielding to reduce interference. They are designed to cancel electromagnetic interference with the way the pairs are twisted inside the cable. Unshielded twisted cables are most widely used for office LANs, though recently wireless LANs are more widely used. Unshielded cables are lightweight, thin and flexible. They are also versatile and inexpensive. A typical UTP cable cross section is shown in the figure below:

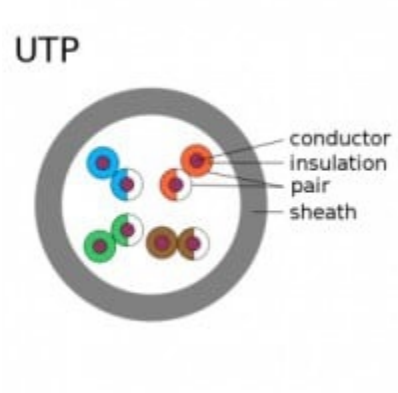


Comparison between STP and UDP

1. Physical: The only difference between the STP and UTP cable is the additional shielding material used in STP cables. The shielding covers the full length of the cable and protects it from any external interference.

2. Cost: Due to the additional material used in a STP cable, it costs more than the UTP cable

3. Considerations: While using STP cable will yield maximum bandwidth despite external conditions, the shielding makes the cable heavier and more difficult to bend.



4. Use: UTP cable typically is used in homes and offices. Some large businesses also use the cable because it is cheaper. Large companies that require maximum bandwidth typically use STP cable. STP cable is used outside to better deal with the elements and equipment that may degrade bandwidth quality.

Previous Contents Next

CompTIA® Network+ Exam Notes : Placement Of Networking Devices On A Network And Install/Configure Them

examguides.com/Networkplus/network-plus-10.htm

2. Infrastructure

2.2 Placement of networking devices on a network and install/configure them

Switch: Switches work at layer 2 of OSI model, which is Data Link Layer. A switch looks at the destination MAC address before forwarding a frame. It may be noted that there are some layer 3 switches. Though these devices are called switches, they typically do the routing. When we say switches, we mean layer 2 switches (or simple switches). A switch uses OSI layer 2 address (MAC Addresses) for forwarding frames. A switch can be used to reduce network traffic by dividing the broadcast domains of a network. Switches are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device

The main function of a content switch is to inspect the network data that it receives so that it can decide where on the network that data (or request) needs to be forwarded to.

Router: The following are true about routers:

- Routers work at the network layer of ISO-OSI model and responsible for forwarding packets based on logical address.
- Routers do not forward broadcasts. Note that typically, switches and hubs forward broadcasts.
- Routers are required when you have more than one subnet in your network.

Hub: Hubs are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data packet is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

The difference between hubs and switches is in how the devices deal with the data they receive. Whereas a hub forwards the data it receives to all the ports on the device, a switch forwards it to only the port that connects to the destination device. It does this by the MAC address of the devices attached to it and then by matching the destination MAC address in the data it receives.

Hubs and switches have two types of ports:

- Medium Dependent Interface (MDI) and
- Medium Dependent Interface Crossed (MDI-X).

The two types of ports differ in their wiring. As the X implies, an MDI-X port's wiring is crossed; this is because the transmit wire from the connected device must be wired to the receive line on the other. Rather than use a crossover cable, you can use the more simple straight-through cable to connect systems to the switch or hub.

Three different types of hubs are widely known. These are:

- Passive hub
- Active hub
- Intelligent hub

Passive hubs do not amplify the electrical signal of incoming packets before broadcasting them out to the network.

Active hubs, on the other hand, amplify the received signal before sending them out. Some people use the terms concentrator when referring to a passive hub and multiport repeater when referring to an active hub.

An intelligent (also called smart) hub typically is stackable (built in such a way that multiple units can be placed one on top of the other to conserve space). It also typically includes remote management capabilities via SNMP and virtual LAN (VLAN) support.

A network hub operates at the physical layer of the OSI model. A router operates at the network layer of the OSI model. A Wireless bridge operates at the data link layer of the osi model. A NIC and Access Point operates at the data link layer of the osi model. There are two main types of switches. Layer-2 switches operate at the data-link layer of the OSI model and are based on bridging technologies. They establish logical connections between ports based on MAC addresses. Layer-3 switches operate at the layer 3(network layer) of the OSI model and are based on routing technologies. They establish logical connections between ports based on network addresses. Layer-3 switches are sometimes called routing switches or multilayer switches.

Firewall: A firewall can be implemented either as a hardware device or using software. A software implementation of firewall typically resides on top of the operating system, and controls the network traffic. A hardware implementation sits separately away from the computer box. One main advantage of hardware firewall is its speed, where as the main advantage of software firewall is its low cost.

The following are the commonly used FireWall technologies:

1. Access Control Lists (ACL): Access Control List (ACL) refers to a list of ports and services that are available on a host (or a network device such as router), each with a list of hosts and/or networks permitted to use the service. Both nodes (work stations or servers) as well as routers can have access lists. Access lists are used to control both inbound and outbound traffic.

2. Packet Filters: This is also known as static packet filtering. Access to a network is controlled by analyzing the incoming and outgoing packets and "allow" or "deny" them based on the IP addresses of the source and destination. Dynamic packet filtering uses stateful inspection. Static packet filter just uses the header information for packet filtering. The main draw back of static packet filter is spoofing.

3. Dynamic Packet Filters: Also referred to as Stateful Inspection, DPF, unlike static packet filters, monitors each session and makes sure they are valid. Note that a static packet filtering uses only the header information in a packet traversing the FireWall, whereas a Dynamic Packet Filter inspects all the interfaces based on a state table. CheckPoint's FireWall-1 uses stateful inspection.

4. Protocol Switching: We know that TCP/IP is the protocol used on the Internet. By using a different protocol on the private network that is connected to the public Internet through a Firewall, we can improve the security of the private network.

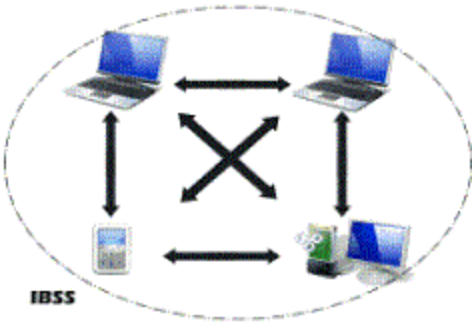
An analog modem, usually just referred to as a modem (short for modulator/demodulator), is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. The modem at the receiving end converts the signal back into a format that the computer can understand. Modems can be used as a means to connect to an ISP or as a mechanism for dialing up a LAN.

Wireless accesspoint:

Wireless LANs consist mainly of two entities: clients or end-user devices and Access Points (AP). Clients' are equipped with devices that allow the user to use the RF medium to communicate with other wireless devices. AP functions like a regular switch or router in wired network for the wireless devices. Moreover, it represents a gateway between the wireless devices and a wired network. The basic structure of a Wireless LAN is called BSS (Basic Service Set) shown in below fig, in which the network consists of an AP and several wireless devices. When these devices try to communicate among themselves they propagate their data through the AP device. In order to form the network, AP keeps broadcasting its SSID (Service Set Identifier) to allow others to join the network.

If the BSS did not have an AP device, and the wireless devices were communicating with each other directly, this BSS is called an Independent BSS and works in mode called "ad hoc mode". Group of BSSs (either BSS or IBSS) can be combined to form an ESS (Extended Service Set). This set is created by chaining this group of BSSs to a single backbone system.

There are three main categories of antennas:



Omni-directional - Omni-directional antennas radiate RF in a fashion similar to the way a table or floor lamp radiates light. They are designed to provide general coverage in all directions.

Semi-directional - Semi-directional antennas radiate RF in a fashion similar to the way a wall sconce is designed to radiate light away from the wall or the way a street lamp is designed to shine light down on a street or a parking lot, providing a directional light across a large area. Yagi antenna is an example of this type of antennas.

Highly-directional - Highly-directional antennas radiate RF in a fashion similar to the way a spotlight is designed to focus light on a flag or a sign. Each type of antenna is designed with a different objective in mind. Phased array antenna is an example of this type of antenna.

Previous Contents Next

CompTIA® Network+ Exam Notes : Use Cases For Advanced Networking Devices

examguides.com/Networkplus/network-plus-11.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Infrastructure

2.3 Use cases for advanced networking devices

Proxy Server: A proxy server, also known as a "proxy" or "application level gateway", is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet.

Proxy servers are used to provide improved performance and security. They can also be used to monitor how employees use outside resources such as the World Wide Web.

A proxy server typically works on the transport layer (layer 4) or higher of the OSI model. A Proxy Server can be used to connect all the work stations on the local network to the Internet. In this case, the proxy does Many-to-One address mapping. i.e. it maps several local IP address to one public IP address for enabling Internet access. A proxy server is typically implemented at the application layer of the OSI model.

Proxy servers work as a intermediary between the two ends of a client/server network connection. Proxy servers interface with network applications, most commonly Web browsers and servers.

Reverse proxy server: Acts as a gateway to an HTTP server receiving requests from client and performs TCP multiplexing

Example : Incoming requests for a corporate Web site

Proxy servers provide three main functions:

1. Firewall and network data filtering support : Proxy servers work at the Application layer (layer 7) of the OSI model. They differ from traditional network firewalls that work at lower OSI layers and support application-independent filtering.

2. Network connection sharing : proxy servers are commonly employed to distribute Internet connections across multiple routers and local intranet networks.

3. Data caching : The caching of Web pages by proxy servers can improve a network user's experience in three ways. First, caching may conserve bandwidth on the network, increasing its scalability. Next, caching can improve response time experienced by clients. With an HTTP proxy cache, for example, Web pages can load more quickly into the browser. Finally, proxy server caches increase content availability.

IDS: IDS stands for Intrusion Detection System. IDS detect unauthorized access attempts. There are basically two main types of IDS being used today

- Network based (a packet monitor),
- and Host based (looking for instance at system logs for evidence of malicious or suspicious application activity in real time).

Both IPS and IDS are closely related, and IPS is considered as an extension of IDS. If the IDS monitors network wide communication, it is called Network based IDS, and if the IDS monitors security on a per host basis, it is called Host based IDS. Network based IDS collects widespread intrusions effectively.

Host-based intrusion detection system (HIDS): HIDS refers to applications such as spyware or virus applications that are installed on individual network systems. The HIDS monitors and creates logs on the local system.

Protocol-based intrusion detection system (PIDS): The PIDS monitors and analyzes protocols communicating between network devices. A PIDS is often installed on a web server and analyzes traffic HTTP and HTTPS communications.

Application Protocol-Based Intrusion Detection System (APIDS): The APIDS monitors application-specific protocols.

Network-based intrusion detection system (NIDS): The NIDS examines all network traffic to and from network systems. If it is software, it is installed on servers or other systems that can monitor inbound traffic. If it is hardware, it may be connected to a hub or

switch to monitor traffic.

Behavior based IDS: A behavior-based system looks for variations in behavior such as unusually high traffic, policy violations, and so on. By looking for deviations in behavior, it can recognize potential threats and quickly respond.

Signature based IDS: A signature-based system, also commonly known as misuse-detection IDS (MD-IDS), is primarily focused on evaluating attacks based on attack signatures and audit trails. Attack signatures describe a generally established method of attacking a system. For example, a TCP flood attack begins with a large number of incomplete TCP sessions. If the MD-IDS knows what a TCP flood attack looks like, it can make an appropriate report or response to thwart the attack. This IDS uses an extensive database to determine the signature of the traffic.

An intrusion prevention system (IPS): An intrusion prevention system is a computer security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. IT is a network device that continually scans the network, looking for inappropriate activity. It can shut down any potential threats. The IPS looks for any known signatures of common attacks and automatically tries to prevent those attacks. An IPS is considered a reactive security measure because it actively monitors and can take steps to correct a potential security threat.

Multi layer switch: A multi-layer switch is one that can operate at both Layer 2 and Layer 3 of the OSI model, which means that the multi-layer device can operate as both a switch and a router. Also called a Layer 3 switch, the multi-layer switch is a high-performance device that actually supports the same routing protocols that routers do. It is a regular switch directing traffic within the LAN; in addition, it can forward packets between subnets.

VPN concentrator: A VPN concentrator can be used to increase remote-access security. This device can establish a secure connection (tunnel) between the sending and receiving network devices. VPN concentrators add an additional level to VPN security. Not only can they create the tunnel, but they also can authenticate users, encrypt the data, regulate the data transfer, and control traffic.

VoIP (voice over IP): VoIP is the transmission of voice and multimedia content over Internet Protocol (IP) networks. VoIP historically referred to using IP to connect private branch exchanges (PBXs), but the term is now used interchangeably with IP telephony.

The important elements and the functions of a VOIP network are given below:

a. IP phone: An IP phone is a telephone with an integrated Ethernet connection. Although users speak into a traditional analog handset (or headset) on the IP phone, the IP phone digitizes the spoken voice, packetizes it, and sends it out over a data network (via the IP phone's Ethernet port).

b. Call agent: A call agent is a repository for a VoIP network's dial plan. For example, when a user dials a number from an IP phone, the call agent analyzes the dialed digits and determines how to route the call toward the destination.

c. Gateway: A gateway in a VoIP network acts as a translator between two different telephony signaling environments. In the figure, both gateways interconnect a VoIP network with the PSTN. Also, the gateway on the right interconnects a traditional PBX with a VoIP network. PBX A Private Branch Exchange (PBX) is a privately owned telephone switch traditionally used in corporate telephony systems. Although a PBX is not typically considered a VoIP device, it can connect into a VoIP network through a gateway.

d. Analog phone: An analog phone is a traditional telephone, like you might have in your home. Even though an analog phone is not typically considered a VoIP device, it can connect into a VoIP network via a VoIP or, as shown in the figure, via a PBX, which is connected to a VoIP network.

e. UC servers are typically software-based applications that run real-time services allowing for instant messaging, VoIP, and other services. Some of the most common are Microsoft Lync Server, Skype for Business, and Cisco's Unified Communications Manager.

f. UC devices are client applications that make the communication possible. Microsoft Lync, for example, includes a client for IM, presence, video calls, desktop sharing, voice, and so on.

g. UC gateways make it possible to expand communication possibilities. Lync Server, for example, includes gateways for Extensible Messaging and Presence Protocol (XMPP), thus making it possible for clients to communicate with XMPP servers.

VoIP PBX:

SIP: The Session Initiation Protocol is a communications protocol for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls. It is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. SIP is used to create, manage and terminate sessions in an IP based network. A session could be a simple two-way telephone call or it could be a collaborative multi-media conference session. This makes possible to implement services like voice-enriched e-commerce, web page click-to-dial or Instant Messaging with buddy lists in an IP based environment. Don't worry if you don't know about these services.

SIP is the IETF protocol for VOIP and other text and multimedia sessions, like instant messaging, video, online games and other services. The SIP is an IETF application layer protocol for establishing, manipulating, and tearing down sessions. A session could be a

simple two-way telephone call or it could be a collaborative multi-media conference session. Used to create and end sessions for one or more media connections, including Voice over IP calls.

Actual voice packets are sent using RTP/RTCP for SIP VOIP calls. RTP opens two ports for communication. One for the media stream (an even port number) and one for control (QoS feedback and media control)- RTCP. Originating source port numbers are dynamically assigned by source host, usually greater than 1023. The following are the recommended port numbers:

H.323: is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network.

RTP: Real-time Transport Protocol is a network protocol for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications. SIP uses RTP and several other protocols for media streaming. RTP is a Layer 4 protocol that carries voice (and interactive video).

SMB: Which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.

Content filter: Internet content filter is used to block specific types of information from being passed on to the user.

NGFW: Common features of a traditional firewall include support for Network Address Translation (NAT), Port Address Translation (PAT), and Virtual Private Network (VPN) termination, as well as being able to provide a high level of availability and performance.

NGFW (short for Next Generation Firewall) offers:

- Application Awareness,
- Stateful Inspection,
- Integrated Intrusion Protection System (IPS),
- Identity Awareness (User and Group Control),
- Bridged and Routed Modes,
- And the ability to utilize external intelligence sources

Previous Contents Next

CompTIA® Network+ Exam Notes : Virtualization And Network Storage Technologies

examguides.com/Networkplus/network-plus-12.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

SCADA/ICS systems are often used to gather and analyze data from remote systems in real time.

Connection Type:

FcoE: It stands for Fibre Channel over Ethernet. It solves the problem of organizations having to run parallel network infrastructures for their local area networks (LANs) and their storage area networks (SANs). As a result, they have to operate separate switches, host bus adapters (HBAs), network interface cards (NICs) and cables for each of these networks.

Fibre Channel, or FC, is a high-speed network technology (commonly running at 2-, 4-, 8- and 16-gigabit per second rates) primarily used to connect computer data storage.

While Ethernet-based standards and protocols are extremely fast, the InfiniBand protocols reduce the workload on server OSs and hardware. This results in faster data transfers with considerably lower latencies. The best choice is therefore InfiniBand.

Fibre Channel over Ethernet (FCoE) developed by Cisco. The main application of FCoE is in data center storage area networks (SANs).

Fiber channel utilizes FCP (Fibre Channel Protocol) transport protocol that transports SCSI commands over Fibre Channel networks.

ISCSI: ISCSI is a way of connecting storage devices over a network using TCP/IP. It can be used over a local area network (LAN), a wide area network (WAN), or the Internet. iSCSI devices are disks, tapes, CDs, and other storage devices on another networked computer that you can connect to.

LUN (logical unit number): It is a number used to identify a logical unit, which is a device addressed by the SCSI protocol or Storage Area Network protocols

Fibre Channel, or FC, is a high-speed network technology (commonly running at 2-, 4-, 8- and 16-gigabit per second rates) primarily used to connect computer data storage.

Differentiated Services Code Point (DSCP) is a field in an IP packet that enables different levels of service to be assigned to network traffic.

Jumbo Frame: A jumbo frame is an Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. Jumbo frames are used on local area networks that support at least 1 Gbps and can be as large as 9,000 bytes. These jumbo frames are sometimes also called "Giants".

Example: You are consulted to plan an internetwork for an organization. How will you determine the number of host IPs' you will be requiring for the proposed internetwok?

Total Number of host IPs' required = One for each NIC (Network Interface Card) + One for each interface on routers.

For routing between two subnets, you need two network cards (NICs). A computer with two or more NICs is called a multi-homed computer. Further, you need to enable IP forwarding, so that packets from one subnet are forwarded to the other subnet as required.

Firewall is an optional software/hardware component, and it mainly intended to restrict packet forwarding according to a preset criteria.

Previous Contents Next

CompTIA® Network+ Exam Notes : Comparing Different Wan Technologies

examguides.com/Networkplus/network-plus-13.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Infrastructure

2.5 Compare different WAN technologies

WAN technologies: It is commonly used with dedicated leased lines include digital circuits, such as T1, E1, T3, and E3. These circuits can use multiplexing technology to simultaneously carry multiple conversations in different 64-Kbps channels. A single 64-Kbps channel is called a Digital Signal 0 (DS0). When one of these circuits comes into your location, it terminates on a device called a channel service unit/data service unit (CSU/DSU).

WAN (Wide Area Network) devices extend the reach of LAN (Local Area Network) devices. WANs typically span over a wide area, such over multiple cities / countries. WANs are connected over serial lines that typically operate at lower speeds than LANs.

Some of the WAN devices are:

1. Routers: Routers are responsible for routing the packets in an internetwork.

2. Modems: Modems connect to public telephone circuits through dial-up.

3. CSU/DSU: Stands for Channel Service Unit / Data Service Unit. CSU/DSUs are used for connecting to Central Office of a Telephone switching company and provides serial WAN connections.

4. Communication Servers: These are used for dial in/out to remote users. Provides RAS (Remote Access Server) functionality.

5. Multiplexers (mux): Multiplexers combine two or more signals before transmitting on a single channel. Multiplexing can be done by sharing "time" or "frequency"

1. Analog modem: Analog modem uses the telecom company's copper wire to connect to the exchange, and most widely used.

2. DSL: DSL uses existing copper telephone lines. DSL technologies typically provide speeds up to 1.544 Mbps.

3. Cable modem: Cable modem uses the same line as cable TV. Possible bandwidth for Internet access reaches up to 27 Mbps.

4. ISDN: ISDN comes in two flavors- BRI and PRI. The most commonly used is BRI, Basic Rate Interface. BRI is composed of two 64-Kbps B (bearer) channels and one 16 Kbps D (delta) channel. ISDN supports both voice and video.

In the figure shown, two LANs are connected together using a Wide Area Network (WAN). If the LANs are in the same building, there is no need to use a WAN link. Therefore, they are geographically separate locations. The routers A and B may use either static routes or dynamic routes to communicate within the WAN. It is not necessary that all hosts on LAN "A" communicate with all the hosts on LAN "B"

Service type:

A CSU/DSU (Channel Service Unit/Data Service Unit): It is a hardware device that converts a digital data frame used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa. For example, if you have a leased digital line (perhaps a T-1 or fractional T-1 line) to a phone company or a gateway at an Internet service provider, you have a CSU/DSU at your end and the phone company or gateway host has a CSU/DSU at its end.

ISDN: The basic rate ISDN has two B channels at 64 Kbps and one D channel at 16Kbps. B channels carry the user data, whereas the D channel is used for out of band signaling

Dial up access means to connect to the Internet or a remote network through telephone line and modem. Since the same line used for a household phone is used for dialup access, it is called the POTS (plain old telephone system) method of access.

PSTN and ISDN require dialup connections to establish communication sessions.

ISDN has two defined interface standards:

- Basic Rate Interface (BRI)
- and Primary Rate Interface (PRI).

BRI ISDN uses three separate channels; two bearer (B) channels of 64Kbps each and a delta channel of 16Kbps. B channels can be divided into four D channels, which enable businesses to have eight simultaneous Internet connections. The B channels carry the voice or data, and the D channels are used for signalling.

PRI is a form of ISDN that generally is carried over a T1 line and can provide transmission rates of up to 1.544 Mbps. PRI is composed of 23 B channels, each providing 64Kbps for data/voice capacity, and one 64 Kbps D channel, which is used for signaling.

CHARACTERISTICS	BRI	PRI
Speed	128Kbps	1.544 Mbps
Channels	2B+D	23B+D
Transmission Carrier	ISDN	T1

T1/T3:

The transmission speed of a T1 circuit (Used mainly in North America) is 1.544Mbps

The transmission speed of an E1 circuit (Used mainly in Europe) is 2.048Mbps.

The transmission speed of a T3 circuit (Used mainly in North America) is 44.736 Mbps

OC3-OC192: OC stands for Optical Carrier and is used to specify the speed of fiber optic networks conforming to the SONET standard. Basic OC-1 supports 51.84 Mbps. OC-x have a speed of 51.84 multiplied by x. For example, OC-3 will have a bandwidth of 51.84 multiplied by 3 or 155.52 Mbps.

Below are the speeds for some common OC levels.

OC level	Speed
OC-1	51.85 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	9.952 Gbps

Transmission rates supported by leased lines are

T1 - 1.544 Mbps

T3 - 44.736 Mbps

E1 - 2.048 Mbps

E3 - 34.368 Mbps

OC3 - 155.52 Mbps

OC12 - 622.08 Mbps

Characteristics of service:

Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption , and compression.

A common Layer 2 protocol used on dedicated leased lines is Point-to-Point Protocol (PPP).

A less common protocol used on dedicated leased lines (as compared to PPP) is High-Level Data Link Control (HDLC). HDLC lacks many of the features of PPP, and in its standards-based implementation, it can only support a single Layer 3 protocol on a circuit.

Frame Relay: Frame Relay is a "Packet Switched" WAN technology.

Access Rate (AR) -The maximum data rate of the user access channel. The speed of the access channel determines how rapidly (the maximum rate) that the end user can transmit data into a Frame Relay network.

Committed Information Rate (CIR) -This is the rate at which a Frame Relay network provider agrees to transfer information under normal conditions. CIR, measured in bits per second (bps), is one of the key negotiated tariff metrics.

Data-Link Connection Identifier (DLCI) -A Frame Relay service provider typically assigns DLCI values, which are used on Frame Relay interfaces to distinguish between different virtual circuits.

Switched Virtual Circuit (SVC) - A virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic.

DMVPN: A dynamic multipoint virtual private network (DMVPN) is a secure network that exchanges data between sites without needing to pass traffic through an organization's headquarter virtual private network (VPN) server or router.

The benefits to DMVPNs are as follows:

- Traffic between remote sites does not need to go through the hub, thus saving resources such as bandwidth and computing resources at the hub.
- They eliminate additional network delays as the traffic can go directly from spoke to spoke.
- Costs for VPN circuits are lower as DMVPN is typically deployed over the Internet.
- They provide a backup mechanism to private networks.

Previous Contents Next

CompTIA® Network+ Exam Notes : Managing The Network

examguides.com/Networkplus/network-plus-14.htm

3. Network Operations

3.1 Managing the network

MDF: MDF, short for Main Distribution Frame, a cable rack that interconnects and manages the cables entering a building. The cables run through a centralized MDF, then distributed to each individual IDF and then on to specific workstations. For example, a building that has several floors may have one MDF on the first floor and one IDF on each of the floors that is connected to the MDF.A Main Distribution Frame (MDF) is a signal distribution frame or cable rack used in telephony to interconnect and manage telecommunication wiring between itself and any number of intermediate distribution frames and cabling from the telephony network it supports.

IDF: IDF, short for intermediate distribution frame, a cable rack that interconnects and manages the telecommunications wiring between an MDF and workstation devices. Cables entering a building run through a centralized MDF, then each individual IDF and then on to specific workstations. For example, a building that has several floors may have one MDF on the first floor and one IDF on each of the floors that is connected to the MDF. An Intermediate Distribution Frame (IDF) is a free-standing or wall mounted rack for wiring or cable from a MDF and leading to individual cables for each piece of equipment such as workstations, personal computers and other end-user devices.

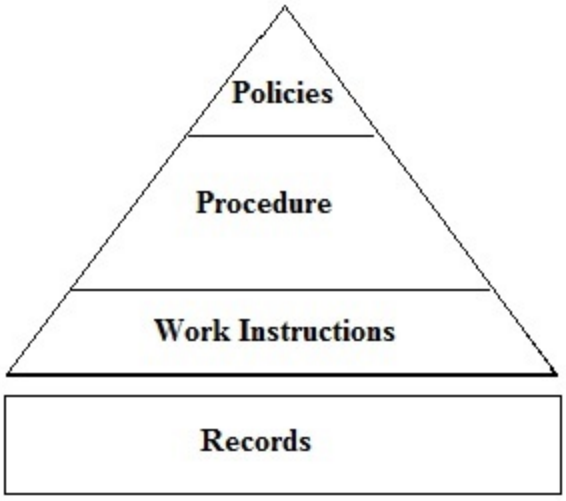
IDF/MDF Documentation: Each and every computer facility will have what's referred to as an MDF short for main distribution facility, and the term facility can refer to a single cabinet, panel, large server room, or switch - it is the location where the network connection is first "distributed" inside the building. The IDF, Intermediate distribution facility, is optional, and generally used when a vertical cross-connect or large horizontal cross-connect is required. In the case of an IDF, cabling is done from the MDF to the IDF, and then the network is "distributed" again from the IDF.

A standard operating procedure, or SOP, is a set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations. Work instructions should be very detailed on "how" to accomplish a specific job, task or assignment.

For example, a work procedure could be developed for assembling a wiring harness for a computer cabinet. Step by step instructions including the tools required, length of the cables, and how to crimp the wires is given in work instructions.

A policy is used as a course of action to guide and influence decisions. Policies are usually enshrined in the organization's quality manual, a top level document, describing your quality processes, and your quality procedures. The figure below shows how the policy framework is distributed within an organization. As you can see, Policies are at the top of the pyramid and records are at the bottom.

Logical vs Physical Diagrams:



Logical Network Diagram: A logical network diagram usually shows network devices like routers, firewalls, and voice gateways. It shows subnets, VLAN IDs, subnet masks and IP addresses. It also shows routing protocols, traffic flows, routing domains, and network segments.

A logical network diagram is used to manage the IP address space within the organization, It is also used to submit network-related proposals to management, since they hide a lot of physical details. They are appropriate for consideration for changes or expansion to the network. In addition, vendors will use logical network diagrams to submit proposals for client's consideration.

Physical Network Diagram: A physical network diagram shows how the network devices are physically connected together. This will include cables, fiber, interfaces, patch panels, and other physical components. It will also show the topology exactly as it exists with physical links between devices. Physical diagram shows port assignments and how the ports are connected to the other device's port.

Rack Diagrams: Rack Diagram is a graphic representation of a rack system, often used as a server and designed to be installed in a framework. A rack diagram is a metal frame used to hold various hardware devices such as servers, Router, Raid, UPS, hard disk drives, modems and other electronic equipment.

Server based networks have advantages like:

1. Central security

2. Central file storage

3. Centrally located printers, tape back up etc

4. Easy administration

Previous Contents Next

CompTIA® Network+ Exam Notes : Disaster Recovery Concepts

examguides.com/Networkplus/network-plus-15.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

3. Network Operations

3.2 Disaster recovery concepts

Availability concepts

Load balancing: It is the process of distributing a server or network load over a multiple servers or networks. An example of load balancing is a clustered solution where each server in a clustered pool shares the load as per the design parameters. Load balancing refers to efficiently distributing incoming network traffic across a group of back-end servers, also known as a server farm or server pool. A load balancer acts as the "traffic regulator" controlling the load on your servers and routing client requests across all eligible servers for optimum capacity utilization and ensures that no one server is overloaded, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it. This feature can take networks to the next level. It increases network performance, reliability, and availability. Multi-layer switches and DNS servers can serve as load balancers.

High availability: It refers to systems that are durable and intended to operate continuously without failure for a long time. Usually, HA servers or systems conform to the strict environmental conditions and have built-in fail-over mechanisms. High availability is

incorporated in the system design so that the up-time of a system is maintained as per the designed standards under all circumstances. High availability is usually design specific where as the fault tolorence is device or network specific.

Power Management:

Power Converter: Converts the voltage from alternating current (AC) to direct current (DC). Power converters are used to step power down from higher voltage to lower voltage.

Power inverter: Converts the voltage from direct current (DC) to alternating current (AC). Power inverters are used to step power up from lower voltage to higher voltage.

Power redundancy: Duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe.

Uninterruptible Power Supply: Provides emergency power to a load when the input power source fails.

- A blackout is a condition where there is total loss of power.
- A brownout is a condition where there is a partial loss of power.
- A voltage surge is said to be occurred when there is a sudden increase in voltage, and the voltage stays high for several seconds.
- A voltage spike is said to have occurred when there is a sudden increase and decrease in voltage. The changes occur in quick succession.

Mean Time to Repair(MTTR): MTTR (mean time to repair) is the average time required to fix a failed component or device and return it to production status.

Mean time to repair includes the time it takes to find out about the failure, diagnose the problem and repair it. MTTR is a basic measure of how maintainable an organization's equipment is and, ultimately, is a reflection of how efficiently an organization can fix a problem.

Mean Time Between Failures (MTBF): The most common failure related metric is also mostly used incorrectly. "Mean time between failures" or "MTBF" refers to the amount of time that elapses between one failure and the next. Mathematically, this is the sum of MTTF and MTTR, the total time required for a device to fail and that failure to be repaired.

SLA Requirements:

Service Level Agreement (SLA): SLA is a document that describes the minimum performance criteria a provider promises to meet while delivering a service. It typically also sets out the remedial action and any penalties that will take effect if performance falls below

the promised standard. It is an essential component of the legal contract between a service consumer and the provider.

Master License Agreement (MLA): MLA is a document created by a software company that defines how their creation can be used .

Memoranda of Understanding (MOU): MOU is a document that expresses mutual accord on an issue between two or more parties. MOU are generally recognized as binding, even if no legal claim could be based on the rights and obligations laid down in them.

SOW: A Statement Of Work (SOW) is a formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client.

Previous Contents Next

CompTIA® Network+ Exam Notes : Scanning,Monitoring And Patching Processes And Summarize Thier Expected Output

examguides.com/Networkplus/network-plus-16.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

3. Network Operations

3.3 Scanning, monitoring and patching processes and summarize their expected outputs

Vulnerability scanning: It is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Port Scanning: The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Patch Management: Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management tasks include maintaining current knowledge of

available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required.

Some important points to remember

A patch is an important component of software update and it usually fixes some known bugs. If you need to apply it on a server, where the downtime is critical, it is recommended practice to install the patch on a lab server first. Install it on the production server once you find it satisfactory.

High Speed Packet Access (HSPA+) is known as a 3G transitional technology that supports legacy architecture.

EDGE, an acronym for enhanced data rates for GSM evolution, is a technology that is backward compliant and provides faster data rates (3G) on the GSM standard. Networks built for Edge are used to deliver streaming data at speeds up to 384Kbps (slow by most standards but faster than GSM).

Long Term Evolution, LTE is a 4G wireless communications standard developed by the 3rd Generation Partnership Project (3GPP) that's designed to provide up to 10x the speeds of 3G networks for mobile devices such as smartphones, tablets, netbooks, notebooks and wireless hotspots.

WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.

HSPA+(Evolved High-Speed Packet Access) is an enhanced version of high-speed 3G wireless networks.

With ADSL, downloads are faster than uploads, which is why it is called asymmetric DSL.

The most common of the DSL varieties is ADSL, which uses different channels on the line. One channel is used for POTS and is responsible for analog traffic. The second channel provides upload access, and the third channel is used for downloads.

The term asymmetric in asymmetric DSL implies the upstream and downstream speeds can be different. Typically, downstream speeds are greater than upstream speeds in an ADSL connection.

The theoretical maximum downstream speed for an ADSL connection is 8 Mbps, and the maximum upstream speed is 1.544 Mbps (the speed of a T1 circuit).

Asymmetric Digital Subscriber Line(ADSL) is an asymmetric service, which means the download speeds are faster than the upload speeds.

vSymmetric Digital Subscriber Line(SDSL) is a symmetric service, in which the upload data throughput from your computer to the internet is the same as your download speed.

Very High Bit-Rate DSL (VDSL) boasts a much higher bandwidth capacity than ADSL or SDSL, with a common downstream limit of 52 Mbps and a limit of 12 Mbps for upstream traffic.

Bandwidth/Throughput: Bandwidth is the maximum amount of data that can travel through a 'channel'. Throughput is how much data actually does travel through the 'channel' successfully. This can be limited by a ton of different things including latency, and what protocol you are using.

Previous Contents Next

CompTIA® Network+ Exam Notes : Remote Access Methods

examguides.com/Networkplus/network-plus-17.htm

3. Network Operations

3.4 Remote access methods

In Remote Access, we mean accessing any centralized office from any remote location. Remote to site VPN is most widely used for accessing a central site remotely and two most widely used encryption protocols for remote access are IPSec and SSL VPNs.

VPN: VPN, short for Virtual Private Network, is a private network formed using public Internet. It is formed between two hosts using tunneling protocols such as PPTP, L2TP, OpenVPN, etc. Using VPN, you can connect two LANs in geographically distant locations together, as if they were located in the same building. The cost of connecting these LANs together is small since public Internet is used for providing the WAN link. A VPN provides a mechanism to access corporate networks safely using Internet. VPN uses encryption to ensure only authorized user can access the corporate resources. A secure tunnel is created through the public network through which the packets are transported between the remote computer and the corporate network.

Point-to-Point Tunneling Protocol (PPTP): PPTP short for Point to Point Tunneling Protocol is Microsoft proprietary VPN protocol. It uses GRE, PPP, MS-CHAP v2, and MS Point to Point Encryption (MPPE). It disables support on the network adapter card for any incoming traffic other than PPTP traffic. On a Multi-homed (more than 2 network cards) Windows Server computer which is also acting as a RAS Server with two network adapter cards, you can configure the card that connects to the Internet for PPTP. The second card (without PPTP), connects to the local network. This arrangement enables local clients to dial out to the Internet.

Remote users, who dial-in to use the network resources must be PPTP- enabled clients.

PPTP is used for establishing a secure connection over the Internet using Virtual Private Network (VPN). In a point-to-point (P-to-P) wireless configuration, the communication link travels from one node directly to one other node.

PPTP is Microsoft ProprietaryProtocol is used to establish a VPN connection between two devices.

L2TP stands for Layer 2 Tunneling Protocol : Tunneling can be based on either a Layer 2 or Layer 3 of OSI Reference model. Layer 2 protocols correspond to the Data Link layer. PPTP and L2TP are examples of Layer 2 tunneling protocols; both encapsulate the payload in a Point-to-Point Protocol (PPP) frame before sending to destination across the network. In layer 2, the unit of transmission is known as frame.

The Layer 2 Tunnel Protocol (L2TP) is a standard that combines the best features of Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP does not provide information confidentiality by itself. L2TP/IPSec, encapsulates L2TP packets in IPSec to provide confidentiality, authentication and integrity. It is now the recommended replacement for PPTP on Microsoft platforms where data encryption is required.

IPSec is normally used in combination with L2Tp for providing confidentiality of communication.

IPSEC: IPSEC stands for IP SECurity, is the protocol developed by IETF and supports secure exchange of packets at IP layer. When using IPSEC, the sending and receiving devices share a public key. IPSEC is the most widely used protocol in Virtual Private Networks (VPNs). IPsec provides Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. It supports secure exchange of packets at IP layer.

Internet Protocol Security (Ipsec): is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec is an example of Layer 3 tunneling protocol. IPSEC encapsulates IP packets in an additional IP header before sending them across an IP network.

ISAKMP : ISAKMP, Short for Internet Security Association and Key Management Protocol defines payloads for exchanging key generation and authentication data. IPSec uses ISAKMP for implementation.

SSL: Secure Socket Layer is primarily used to authenticate Internet users to secure Web sites.

Kerboros is an authentication system used to authenticate users that log on to the network. An SSL VPN is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer (client computer).

RAS is the signalling protocol used between gateways and gatekeepers.

OpenVPN is an open source technology that uses the OpenSSL library and SSLv3/TLSv1 protocols. Very popular however not based on standards (RFC). Uses a custom security protocol and SSL/TLS for key exchange. Provides full confidentiality, authentication and integrity.

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that allows the encapsulation of a wide variety of network layer protocols inside point-to-point links. A GRE tunnel is used when packets need to be sent from one network to another over the Internet or an insecure network. With GRE, a virtual tunnel is created between the two endpoints (Cisco routers) and packets are sent through the GRE tunnel. Similar to VPNs, GRE tunnels can be used to transfer data between remote locations. If you are looking to provide a secure method of connecting remote users to resources stored within a central location, you should probably implement a VPN. However, if you need to pass traffic over an otherwise incompatible network, a GRE tunnel may be the preferred solution.

Microsoft Challenge-Handshake Authentication Protocol (MSCHAP): MS-CHAP is a Microsoft-enhanced version of CHAP, offering a collection of additional features, including two-way authentication. CHAP is an authentication protocol.

Two protocols that provide mutual authentication are

1. EAP-TLS and

2. MS-CHAP.

When using mutual authentication, both server and client authenticate each other. CHAP provides client authentication only PAP uses 2-way handshaking. Passwords are sent in clear text across the link. Therefore, PAP is to be used only when it is not possible to use CHAP.

CHAP uses 3-way handshaking. CHAP uses Challenge/ Response method which provides protection against the password capture while authenticating the user. One should use CHAP whenever it is possible.

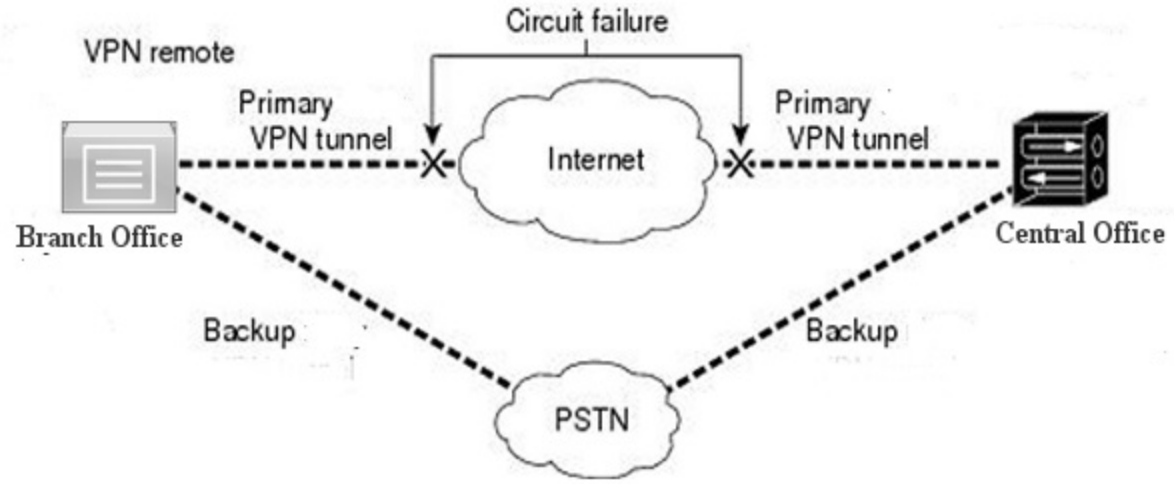
Any system that supports the appropriate dial-in protocols, such as PPP, can connect to a RAS server. Most commonly, the clients are Windows systems that use dialup networking features, but any operating system that supports dialup client software will work. Connection to a RAS server can be made over a standard phone line, using a modem, over a network, or via an ISDN connection.

Remote and Site-to- Site VPN Features:

- In a host-to-site VPN, individual clients (such as telecommuters or travellers) connect to the network remotely. Because the individual client makes a direct connection to the network, each client doing so must have VPN client software installed.
- A host-to-host VPN, allows a two computers to connect to each other directly using secure channel.
- In a site-to-site VPN, whole networks are connected together. It interconnects two sites, as an alternative to a leased line, at a reduced cost.
- A client-to-site VPN (also known as a remote-access VPN) interconnects a remote user with a site, as an alternative to dial-up or ISDN connectivity, at a reduced cost.

Out Of Band Management (OOBM): Usually, remote sites are enabled with out of band access to troubleshoot the router in the event of failure of primary connection. In the diagram shown, above PSTN has been made available for out of band access.

OOBM provides access and control of IT assets outside of the production network. In most cases, this production network is based on Ethernet, but it could also include devices using InfiniBand and fibre channel. The primary use of OOBM is access and control of IT infrastructure when the production network is unavailable, such as cases involving unplanned downtime. The type of assets that require OOBM can include the mission critical routers, switches, KVMs, servers, storage, and appliances that serve as the backbone of the IT. infrastructure.



The figure above shows a schematic of out of band management using backup channel. As shown in the example, if the main VPN connection fails, central office can still access the branch office using PSTN backup link.

VNC (Virtual Network Computing): VNC is a technology for remote desktop sharing, a form of remote access on computer networks. VNC enables the visual desktop display of one computer to be remotely viewed and controlled over a network connection. Remote desktop technology like VNC is useful on home computer networks, allowing someone to access their

desktops from another part of the house or while traveling. It is also useful for network administrators in business environments, such as Information Technology (IT) departments who need to remotely troubleshoot employees' systems.

Remote Equipment: Communication need not be limited between users or between "users and servers". There can also be communication between remote equipment of almost any sort imaginable pumping stations, robotic machines, and so on. The operating systems associated with remote equipment are SCADA (Supervisory Control And Data Acquisition) and ICS (Industrial Control System).

Previous Contents Next

CompTIA® Network+ Exam Notes : Identifying Policies And Best Practices

examguides.com/Networkplus/network-plus-18.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

3. Network Operations

3.5 Identify policies and best practices

Password Policy: It is recommended to have different combination of letters and digits in a password. The password also has 8 alphanumeric characters (considered to be minimum length required for a password). This would make the password difficult to guess. Other options are too easy to guess by a professional hacker.

Most organization specify password policy, such as:

1. The use of both upper-case and lower-case letters (case sensitivity)

2. Inclusion of special characters, such as @, #, $

3. Prohibition of words found in the dictionary

4. Prohibition of use of company name or an abbreviation

5. Prohibition of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common numbers

6. Ensure that the users change the passwords at regular intervals

7. Ensure that the length of the password is above certain minimum characters/digits.

Sometimes, systems create the password for the users or let the user select one of a limited number of displayed choices.

The security policy should clearly state that no one is ever allowed to share his/her password with anyone else.

Secondly, the security policy should state that the help desk can only change or assign a new password after positive identification of the individual requesting the information.

Incident Response Policies

An acceptable use policy (AUP): AUP is a document that outlines a set of rules to be followed by users or customers of computing resources, which could be a computer network, website or large computer system. An AUP clearly states what the user is and is not allowed to do with these resources. It is a simple set of rules that defines how the computer equipment and network can be used. It is generally a very small document that a new employee can read and understand very quickly, so they know what they are signing in.

Data Loss Prevention (DLP): DLP is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR

NDA: NDA short for Non Disclosure Agreement, is an agreement, which sets out the silence on negotiations, negotiation results or confidential documents. A non-disclosure agreement may be unilateral or bilateral, that is it may bind only one party or multiple parties.

Service Level Agreement (SLA) is an agreement between client and service provider for recurring services. The aim is to make the control options for the customer transparent by guaranteed performance characteristics such as scope, reaction time and speed of processing which are described in detail.

CompTIA® Network+ Exam Notes : Intoduction To Physical Security Devices

examguides.com/Networkplus/network-plus-19.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Network Security

4.1 Introduction to Physical security devices

NSA (Short for National Security Agency) is responsible for handling Computer Security Certification.

A **firewall** is a security mechanism, which prevents unauthorized access to a network or a resource on a network. A firewall is a networking device, either hardware or software based, that controls access to your organization's network. This controlled access is designed to protect data and resources from an outside threat. To do this, firewalls typically are placed at a network's entry/exit points - for example, between an internal network and the Internet. After it is in place, a firewall can control access into and out of that point.

A **key fob** is a small, programmable hardware device that provides the key fob holder with access to a physical object such as a computer, storage media, or a networking equipment. Some types of key fobs require physical contact to grant access to the object in question, while other types of key fob can grant access wirelessly. A key fob may also be referred to as a hardware token or security token.

Access cards can serve the dual purpose as an Identification card or badge to employees, allowing them easy access to the building without compromising security. The magnetic strip on the card carries a specific code that unlocks the system when the card is swiped

through the system.

Biometrics is to do with finger print or retina scan. It also serves the same purpose as that of access card, but relies on an employees biometrics to provide access to a building or a resource.

Lock and key is the traditional method of physically securing a building or a cabinet. This is increasingly being replaced by electronic means these days.

Identification badges are used to provide proof of access to others. Proper processes and procedures must be in place for a successful implementation of this prevention tactic. badges are only as good as the enforcement of the badges themselves. In many organizations that implement ID badges, all employees are required to display their ID badge at all times.

Previous Contents Next

CompTIA® Network+ Exam Notes : Authentication And Access Controls

examguides.com/Networkplus/network-plus-20.htm

4. Network Security

4.2 Authentication and access controls

Authentication: Authentication is the process of identifying an individual, usually based on a username and password. Authentication is based on the idea that each individual user will have unique information that sets him or her apart from other users.

Authorization: Authorization is the process of granting or denying a user access to network resources once the user has been authenticated through the username and password. The amount of information and the amount of services the user has access to depend on the user's authorization level.

Accounting: Accounting is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session. Accounting data is used for trend analysis, capacity planning, billing, auditing and cost allocation.

Kerberos: Kerberos is an authentication system used to authenticate users that log on to a network. Kerberos is an authentication service developed at MIT. Its purpose is to allow users and services to authenticate themselves to each other. The modules used by Kerberos include Authentication Sever (AS), Key Distribution Center (KDC), Ticket Granting Ticket Service (TGT), and Network Time Protocol (NTP). Kerberos is the default authentication protocol in Windows 2000 and later Microsoft OSs. Windows uses a negotiation mechanism to determine which authentication protocol will be used. If the Kerberos default fails or isn't supported by one of the client or server components involved in an authentication, Windows will fall back to NTLM.

RADIUS: Radius is a protocol that enables a single server to become responsible for all remote-access authentication, authorization, and auditing (or accounting) services. It is an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. RADIUS implements a client/server architecture, where typical client is a router, switch, or AP and the typical server is a Windows or Unix device that is running RADIUS software.

TACACS+: TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. We must have access to and must configure a TACACS+ server before the configured TACACS+ features on a network access server are available. It provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service authentication, authorization, and accounting independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and routers and the Cisco IOS user interface (for both routers and access servers) can be network access servers.

Access Control:

1. Wireless LAN with speeds above 1 Gbps, which can be achieved comfortably by 802.11ac (802.11ac is capable of 1300 megabits per second (Mbps) which is the equivalent of 162.5 megabytes per second (MBps)).

2. There are basically two types of secure access available, one is client based and the other is clientless. Client based uses IPSec and other similar technologies. It derives its name from the fact that a client program needs to be installed on the user computer to secure the communication. A clientless remote network access typically uses SSL (secure socket layer) available from withing the browser windows. You don't need to install any client separately.

3. A port based network access control, in short, PNAC. IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols.

Port security: The purpose of port security is to prevent access to the LAN from un-authorized hosts. You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

Access Control Lists (ACL): Access Control List (ACL) refers to a list of ports and services that are available on a host (or a network device such as router), each with a list of hosts and/or networks permitted to use the service. Both nodes (work stations or servers) as well as routers can have access lists. Access lists are used to control both inbound and outbound traffic.

MAC Filtering: In computer networking, Media Access Control MAC Filtering (or EUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

Multifactor Authentication (MFA): is a method of confirming a user's claimed identity in which a computer user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism

It is very important to know the distinction between Hashing, Digital signature, and Encryption:

- Hashing produces a small footprint (basically, signature) of the original message. It is used to verify the integrity of a message. Hash is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. In other words, Hash used to ensure that transmitted messages have not been tampered with.
- Typically, the sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message (by using the same formula that was used to produce the Hash by the sender), and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact.
- Encryption is used to translate a message in to secret code. To read an encrypted file, you must have access to a secret key that enables you to decrypt it. Encrypted data is referred to as cipher text.

Two main types of encryption are asymmetric encryption (also called public-key encryption) and symmetric encryption:

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message. A digital signature can be used with encrypted or even un-encrypted message. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

There are three types of cryptographic algorithms that are commonly used. They are:

1. Hashing algorithms

2. Symmetric key-based algorithms

3. Asymmetric key-based algorithms

1. Hashing algorithms: Hashing is not an encryption scheme, but ensures that the transmitted data is not tampered with. Common hash algorithms include the following:

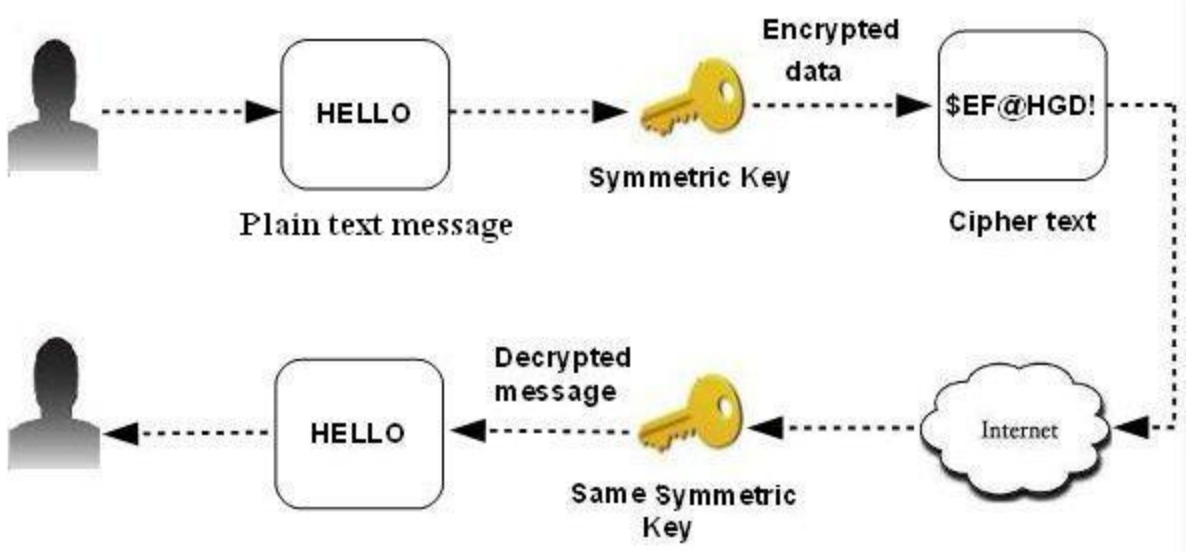
- **Secure Hash Algorithm (SHA, SHA-1):** Developed by NSA, SHA-1 can generate a 160-bit hash from any variable-length string of data.
- **MD4, MD5:** MD series of encryption algorithms generate a hash of up to 128-bit strength out of any length of data.

2. Symmetric algorithms: As the name suggests, symmetric key algorithms use the same key to encrypt as well as decrypt message. Some of the commonly used symmetric key algorithms are:

- **DES (Data Encryption Standard):** DES uses a 56-bit key on each 64-bit chunk of data. It is limited in use due to its short key length.
- **3DES (Tripple DES):** 3DES greatly improves the the security by providing three distinct keys. The total bit strength is 168 bits.
- **AES (Advanced Encryption Standard):** AES is successor to DES, and can create keys from 128-bit to 256-bit length.
- **Blowfish Encryption Algorithm:** It is another flexible, and secure symmetric encryption algorithm. It can perform encryption with encryption key length up to 448 bits. It can encrypt any length of data chunk.
- **IDEA(International Data Encryption Algorithm):** It can encrypt 64-bit blocks of data and uses a 128-bit strength encryption key.
- **RC5, RC6 (Rivest Cipher):** These are the most commonly used encryption security ciphers.

3. Assymetric algorithms: Also known as public key algorithms, these algorithms use asymmetric keys for encoding and decoding a message. Given below are some of the popular asymmetric algorithms:

- **RSA algorithm:** Widely used for encryption and digital signatures. Uses public key and private key for encryption and decryption.
- **Deffie-hellman Key Exchange:** This is one of the early key exchange algorithm.
- **Elliptic Curve Cryptography (ECC):** This is another form of asymmetric key algorithm. One advantage of ECC algorithm is that they have very compact, and more efficient compared to RSA
- **Secret key cryptography:** In this type a plain-text message can be converted into cipher text (encrypted data) and then converted back into plain text using one key. Thus, two devices share a secret key to encrypt and decrypt their communications.



LDAP: The Lightweight Directory Access Protocol is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The LDAP directory service is based on a client-server model. The function of LDAP is to enable access to an existing directory.

Local Authentication: LDAP uses TCP 389 for unsecured communication and 636 for secured communication. An LDAP client starts a session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP port 389. Alternatively, a client may access using secure LDAP communication by using an SSL. This is denoted in LDAP URLs by using the URL scheme "ldaps". The default port for LDAP over SSL is 636.

Various port numbers related to these protocols are as given below:

SMB - 445

POP - 110

IMAP - 143

LDAP - 389

LDAPS - 636

H.323 - 1720

Previous Contents Next

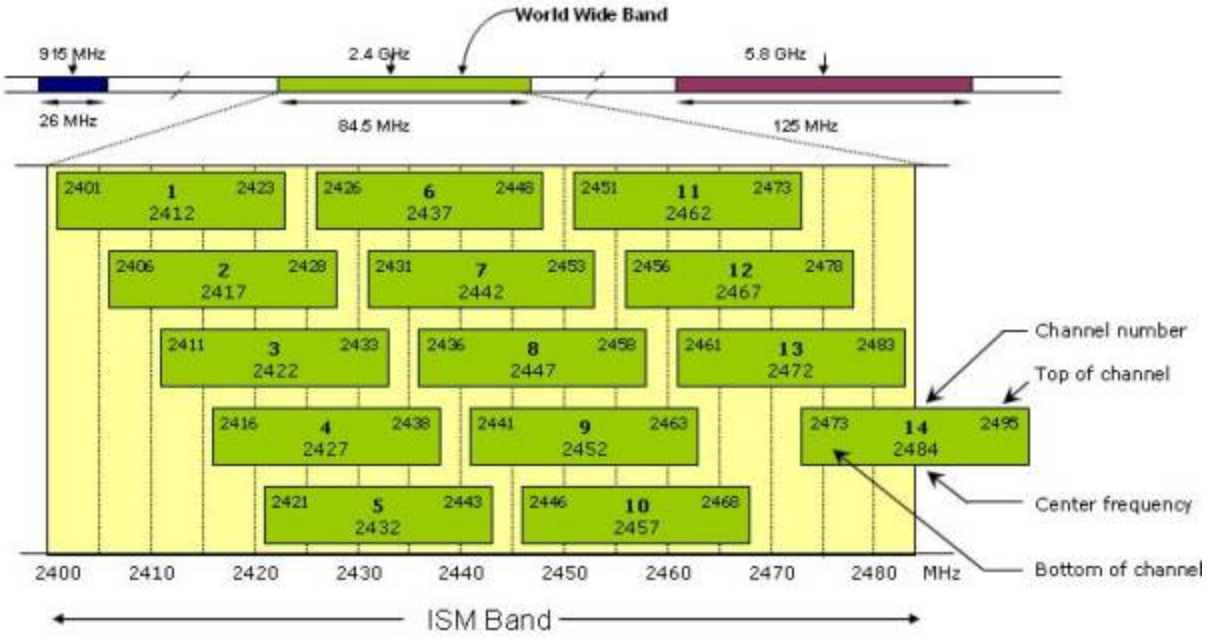
CompTIA® Network+ Exam Notes : Securing Basic Wireless Network

examguides.com/Networkplus/network-plus-21.htm

4. Network Security

4.3 Securing basic wireless network

The ISM band channels allocated for WiFi use are shown in the diagram below. Note that the channels 1,6, and 11 are non-overlapping.



In "ad-hoc" or Independent Basic Service Set (IBSS) configuration there is no backbone infrastructure. An IBSS is one BSS or Basic Service Set. Mobiles can talk to each other without the use of an Access Point (AP). In the Extended Service Set (ESS) configuration, there will be two or more Access Points (APs), and users can freely roam between the Access Points without any disconnection or reconfiguration. BSS will use only one Access Point.

SSID (short for service set identifier): It is a 32- character unique identifier attached to the header of packets when a host connects to a Wireless LAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

WEP (Wired Equivalent Protection): is a security standard for 802.11 WAP networks. WEP key length should be at least 40 bits long. Wireless networks broadcast messages using radio, and therefore more susceptible to eavesdropping than wired networks. WEP was intended to provide confidentiality comparable to that of a traditional wired network. WEP is 802.11's optional encryption standard implemented in the MAC Layer that most radio network interface card (NIC) and access point vendors support. If a user activates WEP, the NIC encrypts the payload (frame body and CRC) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security. The receiving station, such as an access point or another radio NIC, performs decryption upon arrival of the frame. Note that, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies.

WEP encryption: It allows an attacker using readily available software to crack the key within minutes. WEP encryption uses a shared key authentication and sends the same key with data packets being transmitted across the wireless network. If malicious users have enough time and gather enough data they can eventually piece together their own key. Another disadvantage to using WEP encryption is that if the master key needs to be changed, it will have to be manually changed on all devices connected to the network. This can be a tedious task if you have many devices connected to your network.

Wi-Fi Protected Access (WPA and WPA2): is a class of systems to secure wireless (Wi-Fi) computer networks. WPA is forward compatible with the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared.

802.11i includes dynamic key exchange, stronger encryption, and user authentication. It is not backward compatible with WPA. The 802.11i standard is widely known as WPA2. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i

The key features of the WPA protocol are given below:

1. It supports both static and dynamic key distribution

2. It provides Device Authentication, as well as User Authentication.

3. It uses TKIP (Temporal Key Integrity Protocol) encryption for dynamic key exchange. Note that WPA2 uses AES encryption where as WPA uses TKIP. AES encryption is a stronger encryption protocol.

4. WPA is forward compatible with WPA2.

1. WEP uses RC4 stream encryption

2. WPA uses TKIP Encryption.

3. WPA2 uses AES-CCMP Encryption

4. WAP allows a mobile user to connect to a wired network.

5. WAP is extensively used to access the Internet using wireless technologies.

Hotspot: A hotspot is any location where Wi-Fi network access (usually Internet access) is made publicly available. You can often find hotspots in airports, hotels, coffee shops, and other places where business people tend to congregate.

Previous Contents Next

CompTIA® Network+ Exam Notes : Network Security Threats

examguides.com/Networkplus/network-plus-22.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Network Security

4.4 Common networking attacks

Network attacks:

Dos(Denial-of-service): DoS attacks, are explicit attempts to block legitimate users system access by reducing system availability. DoS attacks exploit this to target mission-critical services. Any physical or host-based intrusions are generally addressed through hardened security policies and authentication mechanisms. Although software patching defends against some attacks, it fails to safeguard against DoS flooding attacks, which exploit the unregulated forwarding of Internet packets. The Internet architecture provides an unregulated network path to attack innocent hosts.

Smurf attack is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system

Social engineering: Social engineering is a skill that an attacker uses to trick an innocent person such as an employee of a company into doing a favor. For example, the attacker may hold packages with both the hands and request a person with appropriate permission to enter a building to open the door. Social Engineering is considered to be the most successful tool that hackers use.

Defense against social engineering may be built by:

- Including instructions in your security policy for handling it, and
- Training the employees what social engineering is and how to deal with it.

Examples of social engineering:

1. Phishing: Phishing is the act of sending an e-mail to a user claiming to be a reputed organization (such as a bank) in an attempt to scam the user into providing information over the Internet. The e-mail directs the user to a Web site where they are prompted to provide private information, such as credit card, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Phishing is the practice of enticing unsuspecting Internet users to a fake Web site by using authentic-looking email with the legitimate organization's name, in an attempt to steal passwords, financial or personal information, or introduce a virus attack.

2. Piggybacking: It is another type of social engineering. Here the intruder poses as a new recruit, or a guest to your boss. The intruder typically uses his social engineering skills to enter a protected premises on someone else's identity, just piggybacking on the victim

Virus: A computer virus attaches itself to a program or file so it can spread from one computer to another. Almost all viruses are attached to an executable file, and it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. A virus is a program that propagates itself by infecting other programs residing on the computer system. Viruses are capable of inflicting serious damage to your system, such as erasing your files or your whole disk, or they may just do lighter things like a pop-up a window with a message.

Worm: Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. The danger with a worm is its capability to replicate itself. Unlike Virus, which sends out a single infection at a time, a Worm could send out hundreds or thousands of copies of itself, creating a huge devastating effect. A worm can spread itself (without the help of any other program) over the network from one computer to another. Worms replicate without any user intervention, whereas viruses are known to spread through a user. The replication is based on a security flaw in the Operation System or any other applications running on a system.

Trojan Horse: The Trojan Horse, at first glance appears to be a useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening it because it appears to be receiving legitimate software or file from a legitimate source. A general term, referring to programs that appear

innocent, but actually harmful. For example a download that says "birthday greetings" etc. But when you download and run it, it may do serious damage to your computer system such as damaging important files or even making the computer unusable. The trojan's contents could also be a virus or worm, which then spread the damage.

Logic bomb: A logic bomb is signified by uniqueness of occurrence. It can be a virus or Trojan horse, but activated on the occurrence of an event in the future.

Viruses, worms, and Trojan horses are all harmful pieces of software. The way they differ is how they infect the computers, and spread.

Zero day attack:A zero day attack, also known as a zero hour attack, takes advantage of computer vulnerabilities that do not currently have a solution. Typically, a software company will discover a bug or problem with a piece of software after it has been released and will offer a patch - another piece of software meant to fix the original issue. A zero day attack will take advantage of that problem before a patch has been created. It is named zero day because it occurs before the first day the vulnerability is known.

For detecting spam-ware and virus, one need to install anti spam-ware, and anti virus programs. Installing the latest updates to Operating Systems will protect your system from exploits (like gaining back-door entry), but not necessarily from downloaded virus or spam-ware.

Anti-virus package is required for scanning any virus. A virus is a malicious content that regenerates itself without the knowledge of the user. Some times a virus can be destructive.

Rogue accesspoint: A Rogue Access Point is a Wi-Fi Access Point which is setup by an attacker for the purpose of sniffing wireless network traffic. 802.11 (Wi-Fi) utilizes SSIDs (Service Set IDentifiers) to authenticate NICs to wireless access points. There is no similar protocol for authenticating wireless access points. It is possible to place a rogue wireless access point into an 802.11 network. This rogue wireless access point can then be used to hijack the connections of legitimate network users./p>

War driving: Driving around the town looking for an insecure wireless hot spot is known as War driving. The practice of marking the buildings with unsecured wireless networks is called war-chalking. The practice of sniffing wireless networks is known as war-driving. Tempest was the name of a classified (secret) U.S. government project to study the susceptibility of some computer and telecommunications devices to emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. TEMPEST certification ensures that the building is shielded adequately and the EM radiations are within limits to prevent intruders from accessing the information from outside the building.

Evil twin: An evil-twin is a wireless version of the phishing. The term phishing is a variant of fishing, because attackers are "fishing" for victims. An evil-twin in wireless tries to trick users to connect to fake Wi-Fi by posing like a legitimate wireless network. Users connect to Wi-Fi access points (AP) referencing the network SSID. In this case, a hacker can deploy an AP near the cyber cafe Wi-Fi. Users' wireless client will automatically connect to the preset wireless network on the wireless client. The wireless device itself will connect to the wireless AP that has the strongest signal. If the attacker's AP possess the strongest signal, user devices will then connect to the evil twin. In some cases, the evil-twin AP does not have to provide Internet access, instead, it can act like one's mobile Internet provider and ask for credit card information and/or login and password.

Previous Contents Next

CompTIA® Network+ Exam Notes : Network Device Hardening

examguides.com/Networkplus/network-plus-23.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Network Security

4.5 Network device hardening

There are three basic ways of hardening.

1. Operating system hardening: Here the operating system is hardened (making tough to intrude). Few points that would help in hardening an operating system:

- Changing default administrator account names, and passwords
- Using file access and user access permissions
- Applying any OS hot fixes as and when they are available

2. Network hardening: This involve the following

- Restricting access to network shares
- Disabling/removing protocols and services that are not required.
- Applying Firewalls such as CheckPoint FireWall or NAT (Network Address Translation)
- Restricting wireless access where it may lead to vulnerability

3. Application Hardening: Applications such as DNS servers, Web server, Mail servers, File and print servers can be hardened by the following means:

- Applying latest patches and hotfixes
- Installing anti-virus software where applicable, such as mail server
- Changing the default user names and passwords that the applications use.

All Microsoft Windows operating systems Windows 95 and above contain built in support for File and Printer Sharing. This networking feature is useful on home networks but can be a security concern on public networks. It is preferred to disable this feature if connected to the Internet.

Disabling Unused ports: Disable Unused Ports. A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. For example, if a Catalyst 2960 switch has 24 ports and there are three Fast Ethernet connections in use, it is good practice to disable the 21 unused ports.

Previous Contents Next

CompTIA® Network+ Exam Notes : Common Mitigation Techniques And Their Purpose

examguides.com/Networkplus/network-plus-24.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Network Security

4.6 Common mitigation techniques and their purpose

Network Segmentation:

The following are the advantage of network segmentation:

Extending the network - When the maximum physical limitations of a network has been reached, routers may be added to create new segments to allow additional hosts onto the LAN.

Reduce Congestion - As the number of hosts on a single network increases, the bandwidth required also increases. By segmenting the LAN, you can reduce the number of hosts per network. If traffic consists of communications between hosts on the same segment, then bandwidth usage is substantially reduced.

Isolate network problems - By dividing the network into smaller segments, you reduce the overflow of problems from one segment to the next. Hardware and software failures are some of the problems that can be reduced to affect smaller portions of the network.

Improve Security - By utilizing segments, a network administrator can ensure that the internal structure of the network will not be visible from an outside source. Privileged packets will only be broadcast on the subnet it originated from, not throughout the network.

VLANs - LAN switches can group individual ports into logical switched workgroups called VLANs, thereby restricting the broadcast domain to designated VLAN member ports.

A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. Segmentation of network may not help in the event of broadcast storm.

DMZ: DMZ stands for DeMilitarized Zone. Normally, resources that are intended to be accessible over the Internet are prone for hacking or abuse. By separating these resources that are intended to be accessed over the Internet, it is possible to improve the security of internal private network. In a DMZ, you place all the resources accessible over the Internet through a FireWall. The FireWall separates the DMZ from the internal network.

Your network has 100 nodes on a single broadcast domain. You have implemented VLANs and segmented the network to have 2 VLANs of 50 nodes each. The resulting broadcast traffic effectively decreases by half.

By implementing VLANs

1. The effective broadcast traffic decreases, since VLANs do not forward the broadcast traffic from one VLAN to another.

2. The security can be improved by implementing a router (A layer 3 device) to route the packets among VLANs.

Honeypot: Honeypots are designed such that they appear to be real targets to hackers. That is a hacker can not distinguish between a real system and a decoy. This enables lawful action to be taken against the hacker, and securing the systems at the same time.

Penetration testing: Penetration Testing also called pen testing is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Switch port protection:

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

During the process of Spanning-Tree Algorithm execution, some redundant ports need to be blocked. This is required to avoid bridging loops. To choose which port to use for forwarding frames, and which port to block, the following three components are used by the Spanning-Tree Protocol:

1. Path Cost: The port with lowest path cost is placed in the forwarding mode. Other ports are placed in blocking mode.

2. Bridge ID: If the path costs are equal, then the bridge ID is used to determine which port should forward. The port with the lowest Bridge ID is elected to forward, and all other ports are blocked

3. Port ID: If the path cost and bridge ID are equal, the Port ID is used to elect the forwarding port. The lowest port ID is chosen to forward. This type of situation may arise when there are parallel links, used for redundancy.

BPDU guard: Here if any BPDU (superior or not) is received on a port configured with BPDU guard, the port is immediately put into errdisable state. The port is effectively shutdown and it must either be enabled manually or by use of a timeout function. By default, it is disabled on all ports.

Root guard : When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a superior BPDU. By default, it is disabled on all switch ports.

Flood guard: A flood guard protects against Denial of Service (DOS) flooding attacks. A SYN attack or a SYN flood is one example of a DOS flooding attack. ARP spoofing is falsifying ARP responses, typically used to perform a localized man-in-the-middle attack, not a flood. DNS poisoning is used to falsify the IP address received when a fully qualified domain name (FQDN) is resolved. Domain Name System (DNS) poisoning is used in pharming attacks as well as man-in-the-middle attacks, not flooding. MAC hijacking occurs when an attacks spoofs their MAC address as that of someone else, this is not a flooding attack.

DHCP snooping: DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

Shortest Path Bridging (SPB) is specified by the IEEE 802.1aq standard and is intended to simplify the creation of robust networks by enabling multipath routing.

Rapid Spanning Tree does addition to or removal of Layer 2 links in the network.

Previous Contents Next

CompTIA® Network+ Exam Notes : Explain The Network Troubleshooting Methodlogy

examguides.com/Networkplus/network-plus-25.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

5. Network Troubleshooting and Tools

5.1 Explain the network troubleshooting methodology

Given below is the sequence of steps recommended to be followed while solving a network problem:

1. Information gathering - Identify symptoms and problems

2. Identify the affected areas of the network

3. Determine if anything has changed

4. Establish the most probable cause

5. Determine if escalation is necessary

6. Create an action plan and solution identifying potential effects

7. Implement and test the solution

8. Identify the results and affects of the solution

9. Document the solution and the entire process

Smart jack: A smart jack is a network interface device (NID) that is used between the service providers network and the internal network. NIDs usually have some kind of loop back mechanism that enables the wiring to be tested up to the demark point at the customer premises.

Remote Access Server: The remote access server allows users to gain access to files and print services on the LAN from a remote location. For example, a user who dials into a network from home using an analog modem or an ISDN connection will dial into a remote access server. Once the user is authenticated he can access shared drives and printers as if he were physically connected to the office LAN.

Question: *In your organization, an employee has just resigned. You want to ensure that the employee will not be able to access his account henceforth. However, you want to re-assign the account to another person joined in his place so that you don't need to assign permissions to network resources again. What would you do?*

Answer: *The options available when an employee resigns are:*

1. Keep the account as is

2. Disable the account temporarily, and re-asign after changing the password

3. Delete the account

The first option "Keep the account as is" is not recommended for security reasons.

The second option "Disable the account temporarily" is recommended, but not fully secure. This is because, though the password is changed, the account name is same. However, if you want all the security permissions to be available without losing any time, this would be the best option.

The third option "Delete account" is most secure, but may involve some overhead. When an account is deleted, the SID or UID associated with the account is deleted. Therefore, even if you create another account with the same name, you still loose all previously assigned security permissions.

SOW: A statement Of Work (SOW) is a formal document that captures and defines the work activities, deliverable, and timeline a vendor must execute in performance of specified work for a client.

Memoranda of understanding(MOU): MOU is a document that expresses mutual record on an issue between two or more parties. MOU are generally recognized as binding, even if no legal claim could be based on the rights and obligations laid down in them.

Material Safety Data Sheet (MSDS): It is a formal document containing important information about the characteristics and actual or potential hazards of a substance.

Master License Agreement (MLA): It is a document created by a software company that defines how their creation can be used .

Previous Contents Next

CompTIA® Network+ Exam Notes : Given a scenario, use the appropriate tools for completing the job

examguides.com/Networkplus/network-plus-26.htm

5. Network Troubleshooting and Tools

5.2 Given a scenario, use the appropriate tools for completing the job

Hardware tools:

1. A wire crimper is used to crimp the connectors with LAN cables

2. A tone generator/tester is normally used to locate a cable physically by passing signals through a cable and sensing the signals along the cable using a sensitive receiver.

3. A media tester is used to test a cable for connectivity, loss etc.

4. A patch panel is used to connect incoming and outgoing lines of a LAN. It allows circuits to be arranged neatly by plugging the cables in a pre-designed fashion.

5. Time Domain Reflectometer is used to locate cuts or breaks in a cable.

6. Wire snips are tools designed to cleanly cut the cable.

7. Wire stripper tool is designed to remove the sheathing from a cable to expose the inner wires and to make sure that a clean contact can be made.

8. Cable crimper can be used to attach a connector to the end of a UTP cable.

Network adapter: Following are required while selecting a network adapter.

1. Type of network that it is going to be attached to, e.g.. 10BaseT, 100BaseT etc.

2. Connector type required to attach to the media, i.e. whether it requires RJ-45 / BNC etc

3. Bus type on the Mother board of the computer, e.g.. ISA, EISA, PCI etc.

Whether the driver is provided to support the operating system installed on the computer.

OTDR: OTDR, short for Optical Time Domain Reflectometer can be used for testing a fiber optic cable network. An OTDR injects a short, intense laser pulse into the optical fiber and measures the back-scatter and reflection of light as a function of time. The reflected light

characteristics are analyzed to determine the location of any fiber optic breaks or splice losses.

Question: *A telecommunications provider has just deployed a new OC-3 circuit at a customer site. You tested the cable from provider end up to the demark using internal loopback and found that the connectivity is present. However, you observed a significant number of dropped packets and errors on the circuit. Which of the following should you do to rule out any problem at the physical layer?*

Answer: *The problems are most likely to be found by using a loopback plug and an OTDR. OTDR, short for Optical Time Domain Reflectometer finds any problems like nicks in the optical cable. It is used as a troubleshooting device to find faults, splices, and bends in fiber optic cables by displaying the amplitude of the reflected light against time. It works by injecting a series of optical pulses into the fiber under test and extracting, from the same end of the fiber, light that is scattered or reflected back from points along the fiber. Thus, an OTDR can detect light loss and pinpoint trouble areas, making repairs easy.*

VOM, short for Volt/Ohm Meter is used with copper cables. Cable tester is typically used with copper cables. Optical cables are immune to electrical noise.

OC level	Speed
OC-1	51.85 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	9.952 Gbps

Punchdown block:

Two types of punchdown blocks used are type 66 and type 110.

Type 66 is an older design used to connect wiring for telephone systems and other low-speed network systems and is not as widely used as type 110. The 66 block has 50 rows of IDC contacts to accommodate 25-pair twisted-pair cable. Block 66 was used primarily for

voice communication. Although it was approved for Category 5 and greater, it is not really suitable for anything greater than 10BASE-T due to crosstalk problems. However, there are specialized CAT5e certified 66 blocks available that do meet CAT5e termination standards.

In the network wiring closet, the 110 block is used to connect network cable to patch panels. 110 connections can also be used at the other end of the network cable at the RJ-45 wall jack. 110 blocks are preferred over the older 66 blocks, the 110 block improves on the 66 block by supporting higher frequencies and less crosstalk. Therefore, it supports higher-speed networks and higher grade twisted-pair cable. The termination will be T568A or T568B, depending on which wiring standard is used.

A 110 block is a punch-down block used to connect wiring for telephone systems, data network wiring, and other low-voltage wiring applications. The 110 block improves on the 66 block by supporting higher frequencies and using space more efficiently. A punch-down tool is used to force solid wire into metal slots on the 110 block.

A 110 block is a type of punch block used to terminate runs of on-premises wiring in a structured cabling system. The designation 110 is also used to describe a type of insulation displacement contact (IDC) connector used to terminate twisted pair cables, which uses a punch-down tool similar to the older 66 block.

The figure shows a 110 punch down block tool

Loop-back adapter: It is provided by Microsoft to enable the installation of protocol stack even when there is no Network Interface Card installed. You can also use the loop-back adapter to troubleshoot the problems with the protocol stack, if any, without actually connecting to the network.

Toner probe: A toner probe is a simple cable continuity tester. It consists of two pieces of equipment. One is the tone generator and the other is the probe. One end of the cable is hooked to the tone generator, and the other end is observed for tone using a matching probe. It is also called "fox and hound" wire tracer.

TDR(Time Domain Reflectometer): It is a tool that finds faults in metallic cables like twisted wire pairs and coaxial cables. A similar device, OTDR (short for Optical Time-Domain Reflectometer) is used for testing fiber optic cables.

Fire extinguishers: Fire extinguishers are portable systems. There are four classes of fire extinguishers - A, B, C and D - and each class can put out a different type of fire.

Class A extinguishers will put out fires in ordinary combustibles such as wood and paper

Class B extinguishers are for use on flammable liquids like grease, gasoline and oil

Class C extinguishers are suitable for use only on electrically energized fires

Class D extinguishers are designed for use on flammable metals

Multi-purpose extinguishers can be used on different types of fires and will be labelled with more than one class, like A-B, B-C or A-B-C.

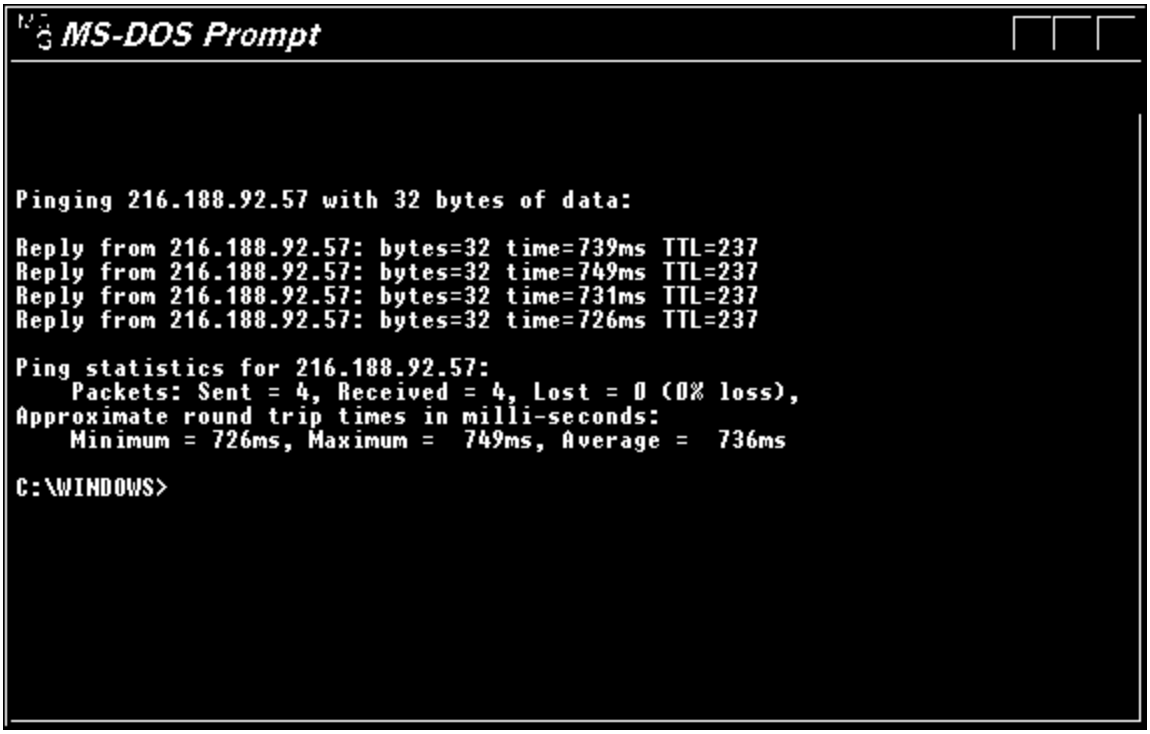
Cable tray : Cable tray is an assembly of metalwork which is used to support insulated electric conductors; similar in function to a metal cable duct, but consisting of a ladder-like metal framework on the bottom and sides, with the top open.

Cable duct: Cable duct is a pipe, either earthenware or concrete, through which prestressing wires or electric cable are pulled.

Command line tools

Some of the important diagnostic commands are explained below

PING: Used to ping the remote system (or the local host) to see that the TCP/IP connection is through. The following fig shows output from ping command.



You can use the ping command to:

- Ping your computer (by address, not host name) to determine that TCP/IP is functioning. (Pinging your computer does not verify that your network adapter is functioning.)
- Ping the local router to determine whether the router is running.
- Ping beyond your local router.

Question: *You are unable to connect to the remote server on a TCP/IP network from your workstation. You suspect some problem with the installation of your workstation. Which is the preferred sequence of steps for troubleshooting?*

Answer: *Here, you suspect a problem with the installation of your local work station. The first step would be to make sure that the TCP/IP stack has been installed properly. This can be done by pinging the local host (127.0.0.1). If you are successful, the TCP/IP stack has been installed properly. Now, you can verify the subnet mask by pinging the Default Gateway. If your subnet mask is not configured properly, you will not get a ping reply from the default Gateway. If you are successful, in pinging the default gateway, you can ping the remote server or any intermediate node to check the connectivity.*

NBTSTAT: This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache. It Displays protocol statistics and current TCP/IP connections since the server was last booted. NETSTAT is used to review all inbound / outbound connection to a server.

NSLOOKUP: This utility enables users to interact with a DNS server and display resource records.

ROUTE: Used to display and edit static routing tables.

IPCONFIG: Internet Protocol Configuration in Microsoft Windows is a console application that displays all current TCP/IP network configuration values and can modify Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.

The following fig shows the output of ipconfig command.

```
Command Prompt
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c497:5026:d18:845d%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

ipconfig /all: Displays the full TCP/IP configuration for all adapters. Without this parameter,

ipconfig displays only IPv6/IPV4 addresses, subnet mask, and default gateway values for each adapter. The command IPCONFIG/ALL shows additional parameters such as host name, DNS servers etc. compared to IPCONFIG command which doesn't show these details

```
MS-DOS Prompt

        Host Name . . . . . . . . . . : VYADLA1
        DNS Servers . . . . . . . . . : 203.124.235.15
                                        203.124.250.69
        Node Type . . . . . . . . . . : Hybrid
        NetBIOS Scope ID. . . . . . . :
        IP Routing Enabled. . . . . . : No
        WINS Proxy Enabled. . . . . . : No
        NetBIOS Resolution Uses DNS : No

0 Ethernet adapter :

        Description . . . . . . . . . : PPP Adapter.
        Physical Address. . . . . . . : 44-45-53-54-00-00
        DHCP Enabled. . . . . . . . . : Yes
        IP Address. . . . . . . . . . : 203.124.234.38
        Subnet Mask . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . : 203.124.234.38
        DHCP Server . . . . . . . . . : 255.255.255.255
        Primary WINS Server . . . . . : 209.9.63.36
        Secondary WINS Server . . . . : 209.9.63.35
        Lease Obtained. . . . . . . . : 01 01 80 12:00:00 AM
        Lease Expires . . . . . . . . : 01 01 80 12:00:00 AM

C:\WINDOWS>_
```

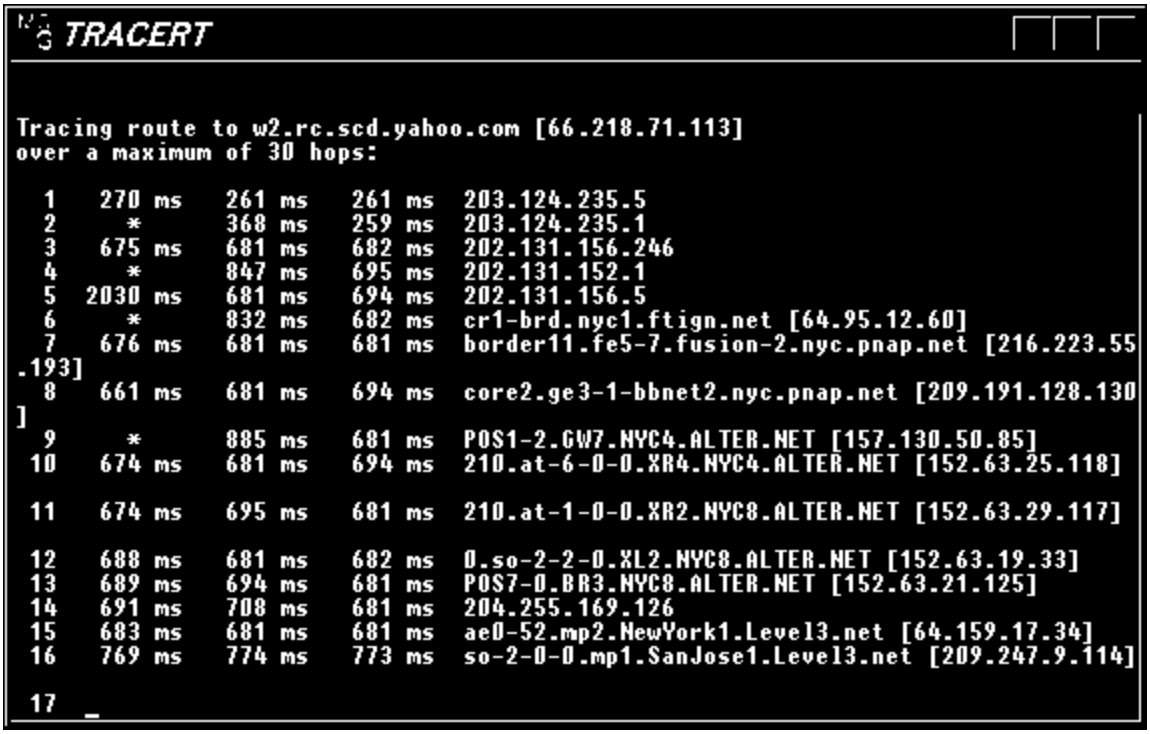
ifconfig (short for interface configuration) is a system administration utility in Unix-like operating systems to configure, control, and query TCP/IP network interface parameters from a command line interface (CLI) or in system configuration scripts. Ifconfig is used to

configure and display network interfaces. If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only. If a single -a argument is given, it displays the status of all interfaces, even those that are down.

TRACERT: Used to determine which route a packet takes to reach its destination from source. The tracert utility traces the path to the destination. It is accomplished by controlling the TTL (Time To Live) of the packets in the increments of 1 (one). When the TTL reaches 0, the router sends back an error message saying that the TTL has elapsed. This information is used to find the intermediate devices over the path to destination. Note that some routers may be programmed not to respond to TTL 0 packets. In such event, you may not receive any response.

Tracert and Ping use ICMP as their base protocol. ICMP messages are carried in IP datagrams. The command tracert/traceroute displays the time taken while a packet reach the destination. You will be able to see the time taken by each hop, and identify the faulty link.

The following fig shows tracert command output



Software tools:

Protocol analyzer: Protocol analyzer can be used to capture the packets over a period of time and can be analyzed. It allows you to display the received frames, or generate frames for testing and debugging. It is also possible to create a statistics such as frame size distribution,

utilization or protocol statistics. A protocol analyzer is used to monitor and troubleshoot problems such as suspicious activity on the network, verification of network load and type of traffic, artificially injecting load on to a network for the purpose of load testing, and other hard to detect problems with the network.

Certifier, or a certification tester: It is used to examine whether the network complies with ISO or TIA standards as applicable. Some certifiers will also have the capability to test the email, DNS, and DHCP servers for proper response times.

Port Scanner: Port scanner is a device that is used to verify any insecure ports.

The functions of different hardware/software components are:

1. NIC: Stands for Network Interface Card. It is a piece of hardware that interfaces your computer to the external networking media. It sits in one of the slots (eg. PCI slot) on your computer motherboard.

2. NIC driver: NIC driver is responsible for interacting with the operating system and the NIC hardware. Normally, the NIC hardware manufacturer provides the NIC driver software.

3. Operating System (OS): Operating System means Computer OS. For example, Windows XP is a Computer Operating System.

4. Network Operating System (NOS): Network operating system interacts with the Computer operating system, and the network resources. Sometimes, both Computer OS and the Network OS may be combined. An example is Windows 2000 Server. It has both Computer OS as well as Network OS built into the Server OS. An example where the Network OS is installed separately is Novell Netware OS. The Network OS sits separately on a computer and interacts with client computers running different Operating Systems such as Windows XP etc

Bandwidth shaper: as the name implies, provides monitoring and controlling of network bandwidth usage.

Netstumbler: can be used to sniff wireless networks during war-driving. The software tool provides several details of a wireless network such as SSID.

Personal firewall: A personal firewall is software that resides on the end users computers. This is different from a regular firewall, in the sense that a personal firewall is geared to protect a single user computer.

Server rail racks: These are the rails that hold the servers within the rack.

Two-post racks: As the name implies, the servers are attached to the rack system at two locations (one on each side).

Four-post racks: The servers are attached to the rack system at four locations (two on each side).

Free-standing racks: can remain in the appropriate upright position on its own without help from external forces or without being bolted or attached to the wall.

Wi-Fi Analyzer: As more networks go wireless, you need to pay special attention to issues associated with them. Wireless survey tools can be used to create heat maps showing the quantity and quality of wireless network coverage in areas. They can also allow you to see access points (including rogues) and security settings. These can be used to help you design and deploy an efficient network, and they can also be used (by you or others) to find weaknesses in your existing network (often marketed for this purpose as Wi-Fi analyzers).

Previous Contents Next

CompTIA® Network+ Exam Notes : Troubleshooting Common Wired Connectivity And Performance Issues

examguides.com/Networkplus/network-plus-27.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

5. Network Troubleshooting and Tools

5.3 Troubleshoot common wired connectivity and performance issues

Network Connection LED

Question: *Your home office is using a broadband modem for accessing the Internet. A workstation is connected to the broadband modem through a router. The link LEDs at both ends of the cable connecting the router and the workstation are off. Which of the following is the most likely problem?*

Solution: *The link LEDs are associated with the physical layer of connectivity. Therefore, it is very likely that either the cable is bad or the network interface hardware is bad. Note that IP address is a logical address, and it has no bearing on the physical connectivity of the cable link.*

Attenuation: Attenuation is the loss of signal strength when electrical signals travel along a conductive wire.

Crosstalk: Crosstalk can be minimized by proper shielding of cables. Near-end crosstalk (popularly known as NEXT) is an error condition that normally occurs when connectors are attached improperly to twisted pair cabling. NEXT is usually caused by crossed or crushed

wire pairs. Two conductors only need to be close enough so that the radiating signal from one of the wires can interfere with the signal traveling on the other.

When using Category 5 cables, connectors, and patch panels one must test the network for compliance with rated speed by using cable tester. Otherwise, a Cat6 cable network may provide only speeds offered by cat 3 network.

Latency defines the amount of time it takes for a packet to travel from source to destination.

Previous Contents Next

CompTIA® Network+ Exam Notes : Troubleshooting Common Wireless Connectivity And Performance Issues

examguides.com/Networkplus/network-plus-28.htm

5. Network Troubleshooting and Tools

5.4 Troubleshoot common wireless connectivity and performance issues

Scenario 1: A small office has a wireless Access Point with several computers connected to it. However, some of the users complain that the connection was slow at times. What are the likely reasons?

Antenna Mismatch and Wireless phone: Note that the connectivity was slow or intermittent. If there were any mode/SSID mismatch, there wouldn't be any communication at all. It is also likely that the wireless phones, filing cabinets, and antenna mismatch errors are adding to the problem.

Antenna Types:

There are broadly two types of wireless networking antennas. These are

- Omni antenna
- Yagi antenna.

Omni antennas, as the name implies are omni (omni means "all") directional. They radiate power in all directions uniformly. On the other hand, Yagi antennas are directional. These antennas radiate more power in a given direction and require alignment. Wrong alignment or misalignment may result in total communication loss. Omni antennas are used for access point communication. The mobile user may be located at any point within the radio distance. Therefore, there is no directional preference, and hence Omni antennas are used. Yagi antennas are used for back-haul networks. To connect different access points. By using directional antenna, you can increase the distance/bandwidth between the communication points.

Two frequently used measurement units of antenna gain are

- dBd
- dBi

dBd refers to measurement with respect to a dipole antenna. dBi refers to the measurement with respect to an isotropic antenna. Normally, dBd is used for low frequencies (typically below 1GHz).

Scenario 2: Paul is a member of accounting group. All other members of the accounting group are able to print to a network printer. He is not able to print to the network printer. His group permissions are set correctly. However, he is able to access File services and other servers. What is the most likely problem?

Solution: Note that all other members of the group are able to access the network printer. Therefore, it can be safely assumed that there is no problem with the group permissions. Also, Paul is able to access file services, which means that the IP address, subnet mask, and default gateway are configured properly. The most likely reason is that the User permissions for Paul are not configured correctly for access to the network printer.

Scenario 3: A network administrator has newly installed wireless network using WAP enabled router in a restaurant. WEP is enabled for security purpose. However, wireless client computers are not able to access the Internet. The link LEDs on the wireless network cards are solid. What is the likely problem?

Solution: Check WEP settings

Note that the link LEDs are ON. Therefore, there is no problem with physical connectivity. The next step would be to check whether the WEP (Wired Equivalent Privacy) settings are okay. WEP settings on the router and the computers accessing the WAP should match, otherwise the client computers may not be able to communicate with the router.

Wrong SSID/SSID mismatch:

Scenario 4: Several client computers are connected to a network using WAP (Wireless Access Point). The WAP , in turn, is connected to a broadband Internet modem through a router. However, none of the computers on the wireless LAN are able to access the Internet during specific times. What is the likely reason?

Solution: Note that the wireless computers are able to communicate over the Internet intermittently. Therefore, the problem with IP address, MAC address or SSID can be ruled out. It is likely that the connectivity between the WAP and the router is intermittent, and needs to be checked.

Scenario 5: A user reports that the wireless network is slow and is able to see and access shared folders that not known to the user. Other wireless users do not see any problem. What is the likely reason?

Solution: It is most likely that the SSID is not configured properly on the users computer. If there is any problem with WAP device, other users would have had problems.

Scenario 6: Several client computers are connected to a network using WAP (Wireless Access Point). The WAP in turn is connected to a broadband Internet modem through a router. Only one of the computers is not able to access the Internet, nor able to see other computers on the wireless network. Other computers on the wireless LAN are functioning normally. Which of the following is the likely reason?

Solution: SSID (short for service set identifier) is a 32-character unique identifier attached to the header of packets when a host connects to a Wireless LAN. The SSID differentiates one WLAN (Wireless LAN) from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

If the connectivity between the WAP and the router is bad, then none of the computers on the wireless LAN would have worked.

Scenario 7: An office user is able to access local network drives over the WiFi, but unable to access the Internet. A sysadmin troubleshoots the issue and observes the following output of the ipconfig command:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Belkin
   Link-local IPv6 Address . . . . . : fe80::c527:527f:45bb:54a8%16
   IPv4 Address. . . . . . . . . . . : 192.168.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::51b5:7d2d:8867:bb82%13
   IPv4 Address. . . . . . . . . . . : 192.168.42.189
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.42.129
```

(Some output omitted intentionally)

What would MOST likely allow the Internet to be accessed?

Solution: The user computer is connected to the WiFi as well as the LAN adapter. He should be able to access the Internet by disabling WiFi adapter. Most apps default to WiFi for accessing the Internet. Alternatively, you need ForceBindIP if you want to specifically force particular applications to use a particular adapter, rather than letting Windows sort it out itself.

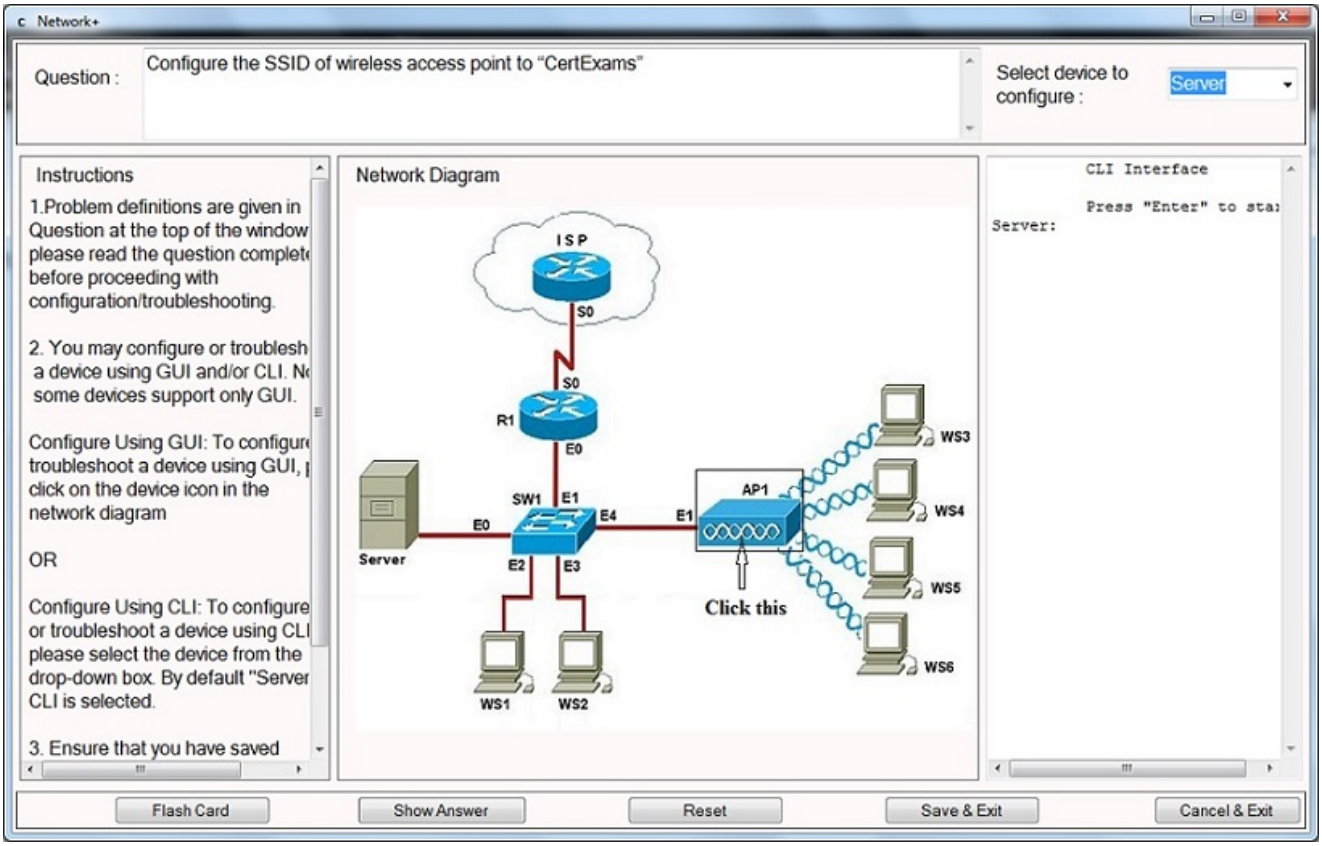
Wireless Access Point Configuration and Security Mismatch:

Example 1. Configure the SSID of wireless access point to "netplus" Network Name (SSID) is basically the device's wireless network name and is one way of securing your wireless network. The SSID is shared by all devices in your wireless network and therefore, has to be unique since this will identify your wireless network from the rest.

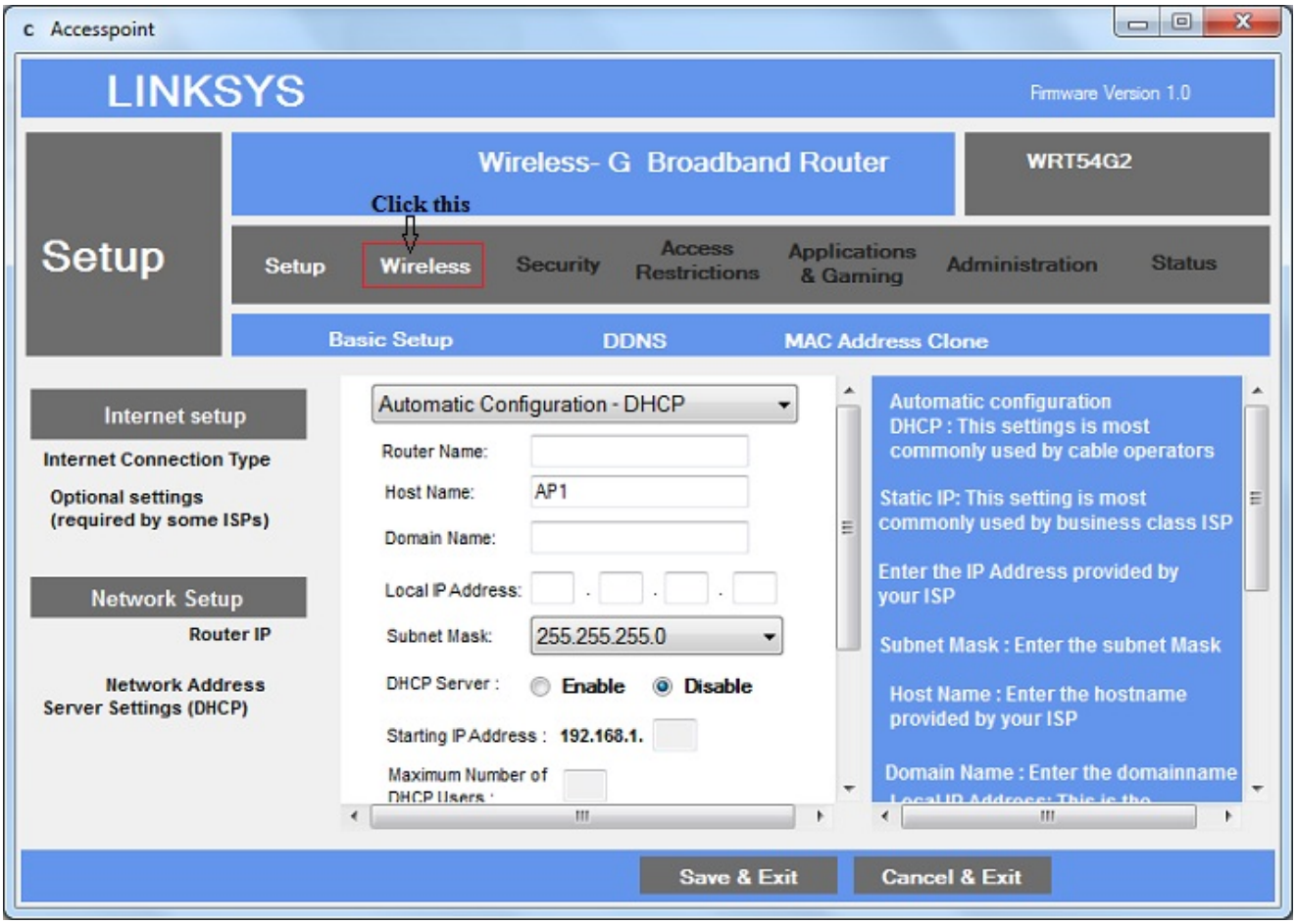
To change the wireless network name of your router, follow the steps below.

Note: SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

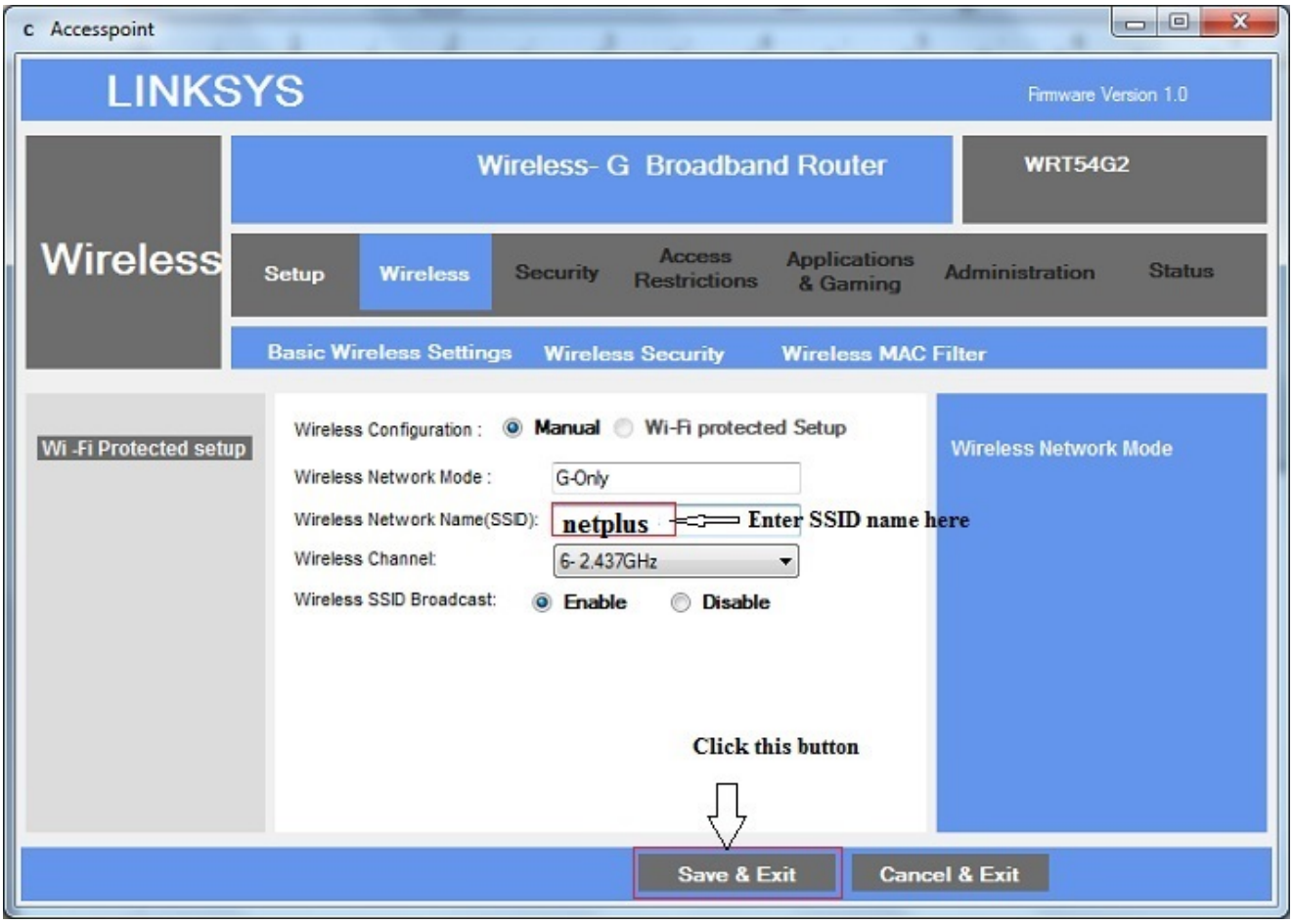
Solution: 1. Click on AP1 in the network diagram , this will pop-up Graphical Device Interface (GDI) of AP1.



2. In Wireless Access Point window click "Wireless" tab



3. In Wireless tab window look for "Wireless Network Name" (SSID), and enter the SSID name "netplus" in the box provided. Click on "Save & Exit" button.

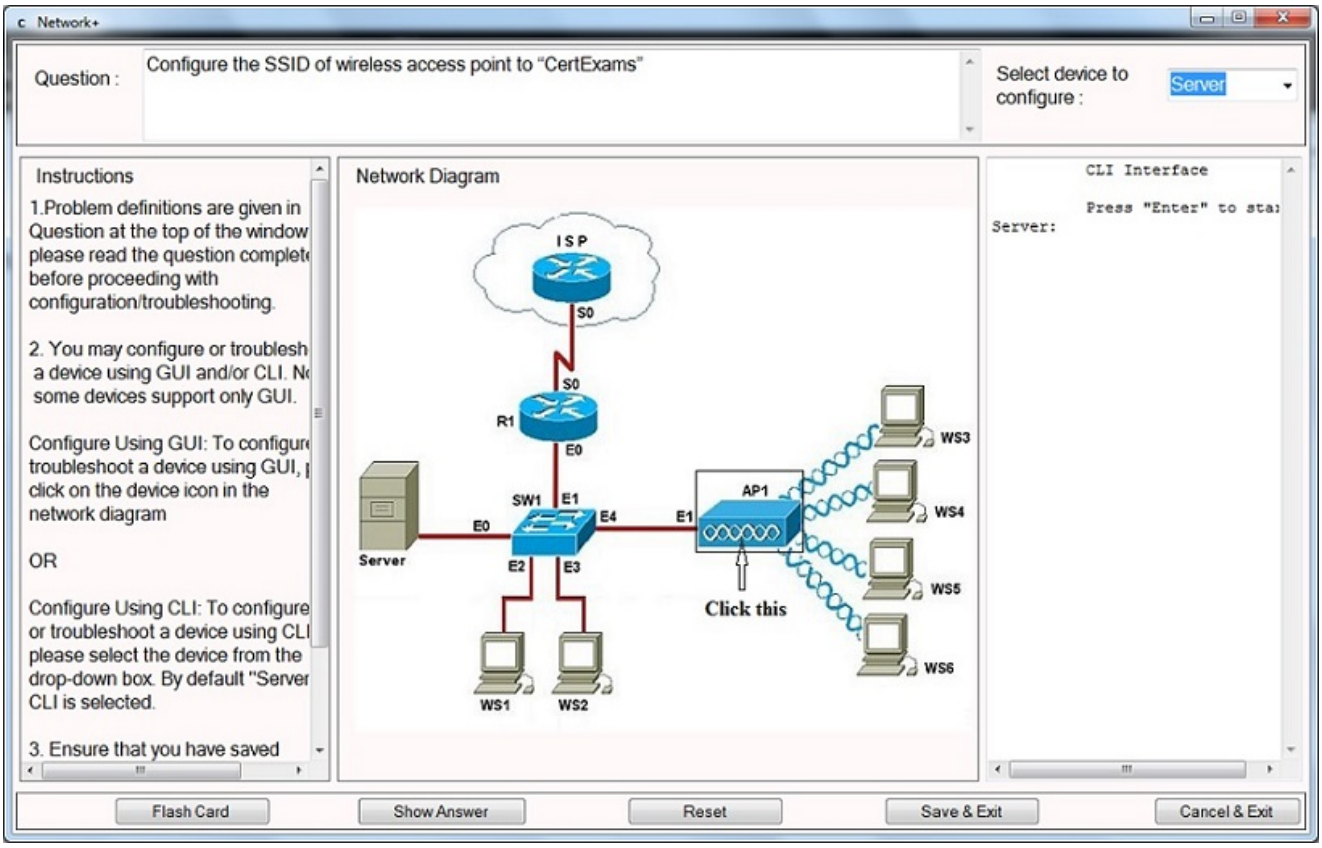


Example 2: Configure the Ip address and subnet mask of wireless access point to 192.168.1.3 and 255.255.255.0 respectively.

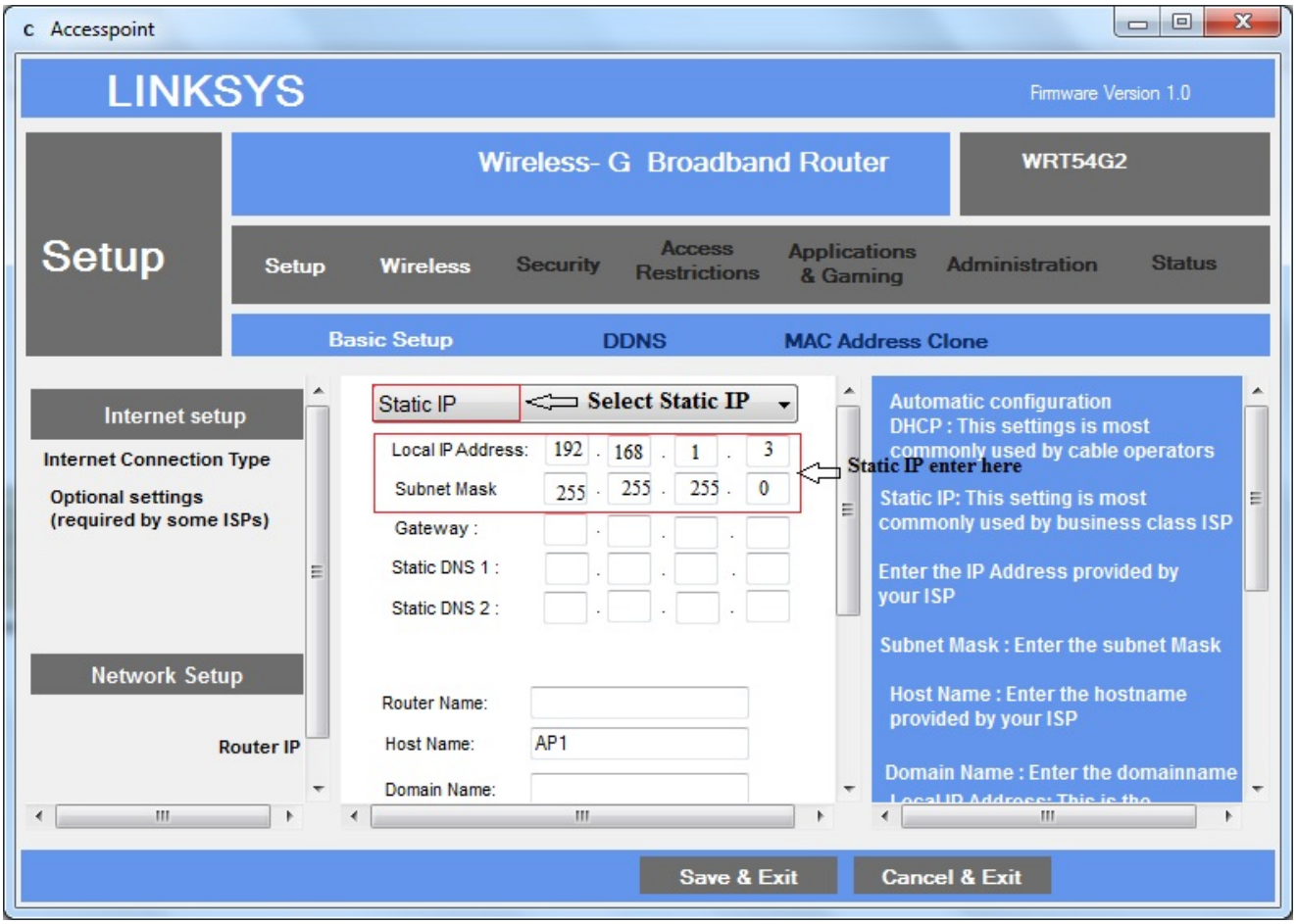
Solution: Assigning a static IP address on an access point allows you to use the same IP address all the time regardless of where it is connected, making it easier to access its web-based setup page for any configuration changes. Besides, if the WAP is acting as a gateway, you need to assign the IP address to the WAP statically, as the connected workstations will have this IP address as their default gateway.

To configure IP address and subnet mask of wireless Access Point follow below steps

1. Click on AP1 in the network diagram , this will pop-up Graphical Device Interface (GDI) of AP1.



2. Set the IP address as 192.168.1.3 in Local IP address field and enter subnet mask as 255.255.255.0 and click "Save & Exit" button.



Note: The exercise is typical for a particular brand of home router and may differ slightly from device to device. When you are configuring any other brand/make routers, please read the manufacturer's documentation provided along with the device.

For more labs and examples you can download Network+ LabSim from the following link.

http://www.simulationexams.com/LabSim/network-lab-simulator.htm

Previous Contents Next

CompTIA® Network+ Exam Notes : Troubleshooting Common Network Service Issues

examguides.com/Networkplus/network-plus-29.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

5. Network Troubleshooting and Tools

5.5 Troubleshoot common network service issues

Incorrect gateway:

Scenario1: Two Servers Venus and Jupiter are connected together through a router. The existing configuration is as given below:

```
-----------------------------------------------------
Venus:
IP address: 202.54.16.5
Subnet mask: 255.255.255.128
Default gateway:202.54.16.1
Jupiter:
IP address: 128.44.216.24
Subnet mask: 255.255.240.0
Default gateway: 202.54.16.1
Router:
IP address to network Venus: 202.54.16.1
IP address to network Jupiter: 128.44.216.1
-------------------------------------------------------
```

The servers are unable to communicate with each other. What is the most likely problem?

Solution: The default gateway on a host should be on the same subnet as that of the host. Otherwise, it is not reachable. For the subnet that Jupiter is residing, the default gateway is incorrectly given.

Scenario2: You are on your company's intranet running on TCP/IP. You are able to access the computers on the local subnet. But you are not able to access any computer on remote subnet. Which interface you need to suspect first to determine the problem?

Solution: Here, you are able to access the computers on the local subnet. However, you are not able to access the computers on remote subnets. Since you are not able to access any of the computers on the remote subnet, you need to ping the default gateway first. The default gateway might have been configured improperly on your computer.

Incorrect Netmask:

Scenario1: A Windows XP user complains that she cannot connect to any other computers on her local subnet even when using correct IP addresses. However, she can ping 127.0.0.1 and receive a reply.

Other users on her subnet do not report having any trouble. All client computers on the network are WINS-enabled. What is the most probable cause of the problem?

Solution: The most likely cause is that the subnet mask is not configured properly. If the TCP/IP stack is not installed properly, you will not be able to ping the local host (127.0.0.1). Also, even if the default gateway is wrongly configured, you will at least be able to ping the computers on the local subnet.

Default Gateway:

Scenario1: You have several computers on a network. All the computers are working on the same subnet. You have configured a router as one of the nodes and the router is connecting to your ISP. You find that none of your computers are able to browse the Internet, though they are able to access the other computers on the network. While diagnosing, you find that you are able to telnet to the router from any of the computers on the subnet, using the router's IP address. What is the likely cause?

Solution: Default Gateway on client computers can be assigned : Manually on each client Computer

To assign the default gateway manually on each client computer, you modify the TCP/IP Properties tab of ' Control Panel > Network' on each client computer. Through the use of DHCP Options

For assigning default gateway on client computers automatically, your NT Server should be running DHCP service. You configure the DHCP Options menu to enable default gateway.

When there are large number of client computers, it will be easier to configure the IP addresses and default gateway on client computers through the use of DHCP Service.

WINS (Windows Internet Name Server) is used for NetBIOS name resolution.

Since you are able to communicate with other computers, your NetBIOS name resolution OK. Also, you are able to Telnet, which precludes the possibility of TCP/IP protocol problems.

Scenario2: A network admin intends to build a router using a Linux computer for his two-subnet network. He has inserted two network cards, and connected one hub for each subnet. Workstations on a given subnet are able to communicate with each other. However, none of the workstations are able to communicate with any other workstation on the second subnet, and vice versa. All the workstations are able to ping respective router (Linux computer) interface, and communicate with the Linux computer. What is the likely problem?

Solution: Note that the workstations on a given subnet are able to communicate with each other, as well as with the Linux computer. Therefore, there is no problem with the networking portion of each subnet. It is likely that the IP protocol forwarding was not enabled on the Linux computer acting as the router.

Scenario3: A network of 10 computers is configured with physical star topology using a 12 port hub. But it is a bus configuration from logical point of view. The link to a computer in the 6th spot has broken. What are the consequences of the cable break?

Solution: The physical configuration is a star network. Therefore, all the computers except the computer on the broken network segment can communicate with each other.

Previous Contents