

Network+ CertNotes

1. OSI Model

The 7 layers of OSI model are:

- 1. The Application Layer:** Application layer is responsible for identifying and establishing the availability of desired communication partner and verifying sufficient resources exist for communication. Some of the important application layer protocols are: WWW, SMTP, FTP, etc.
- 2. The Presentation Layer:** 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.
- 3. The Session Layer:** 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.
- 4. The Transport Layer:** The Transport Layer is responsible for multiplexing upper-layer applications, session establishment, and tearing-down of virtual circuits. This layer is responsible for flow control, to maintain data integrity.
- 5. The Network Layer:** 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 a pre-determined routing methods. Routers work at Network layer.
- 6. The Data Link Layer:**

Data Link Layer is layer 2 of OSI reference model. This layer is divided into two sub-layers:

 - A. Logical Link Control (LLC) sub-layer.
 - B. 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 a Token passing or Ethernet.
- 7. The Physical Layer:** The actual flow of signals take place through Physical layer. At Physical

layer, the interface between the DTE and DCE is determined. 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).

2. IP Addressing

1. 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	N/W addr range	Max networks	Max hosts/ nodes
A	N.H.H.H	0	0-126	127	16,777,214
B	N.N.H.H	10	128-191	16,384	65,534
C	N.N.N.H	110	192-223	2,097,152	254

- Network address of all zeros means "This network or segment".

- Network address of all 1s means " all networks", same as hexadecimal of all Fs.

- Network number 127 is reserved for loop-back tests.

- Host (Node) address of all zeros mean "This Host (Node)".

- Host (Node) address of all 1s mean "all Hosts (Nodes) " on the specified network.

2. The range of numbers from 224.0.0.0 to 239.255.255.255 are used for multicast packets. This is known as Class D address range.

3. 127.0.0.1 is the local loop back address.

4. In an internetwork, the number of distinct IPs' required are

1. One each per client computer
2. One each per server computer
3. One each per router interface.

For example, your network has 2 servers, 26 clients machines, and 2 router interfaces the total number of IP addresses required are 30.

3. Subnetting

1. Subnetting is nothing but creating networks within a network. Subnetting allows an organization with a single IP address (Class A /ClassB /ClassC) to have multiple subnetworks, thus allowing several physical networks within the organization.

- Default subnet mask for Class A network: 255.0.0.0
- Default subnet mask for Class B network: 255.255.0.0
- Default subnet mask for Class C network: 255.255.255.0

2. The directed broadcast should reach all Hosts on the intended network (or subnet, if sub netted). For example, the directed broadcast address for an IP network 196.233.24.15 with default subnet mask is 196.233.24.255. This is arrived by putting all 1s for the host portion of the IP address.

4. TCP/IP

1. TCP: 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 uses port number 6.

The port number used by TCP is 6 and that of UDP is 17.

2. Telnet, FTP, and TFTP:

1. Telnet is used for terminal emulation that runs programs remotely. Telnet uses TCP/IP protocol.

2. Telnet requires a username and password to access.

3. FTP (File Transfer Protocol) is a connection oriented protocol. It uses TCP/IP for file transfer. Compare this with TFTP (Trivial File Transfer Protocol) that uses UDP (Connectionless protocol). SNMP uses UDP over IP. Tracert, Ping use ICMP as their base protocol. FTP is used to transfer files.

4. Both FTP and Telnet are client-server protocols. Note that TCP/IP is a client-server oriented protocol.

3. The port numbers used by different programs are as below:

I. FTP: Port #21

II. Telnet: Port #23

III. SMTP: Port #25

IV. SNMP: Port #161

It is important to know that FTP, Telnet, SMTP use TCP; whereas TFTP, SNMP use UDP.

4. SNMP is part of TCP/IP protocol suite. It allows you to monitor and manage a network from a centralized place by using SNMP Manager software. The systems or devices that provide the responses are called agents (or MIBs). An SNMP agent is any computer running SNMP agent software.

MIB stands for Management Information Base. It is part of SNMP agent database. A MIB records and stores information about the host it is running on. An SNMP manager can request and collect information from an agent's MIB. Routers are typical MIB agents. SNMP agent generates "trap" messages that are then sent to an SNMP management console, which is a trap destination.

5. 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.

6. Some of the important TCP/IP related diagnostic commands that need to be practiced for Network+ exam are:

PING : Used to ping the remote system (or the local host) to see that the TCP/IP connection is through.

NBTSTAT : This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache.

NETSTAT : Displays protocol statistics and current TCP/IP connections since the server was last booted.

TRACERT : Used to determine which route a packet takes to reach its destination from source.

IPCONFIG : Used to display Windows IP configuration information.

NSLOOKUP : This utility enables users to interact with a DNS server and display resource records.

ROUTE : Used to display and edit static routing tables.

5. WAN

1. WAN (Wide Area Network) devices extend the reach of LAN (Local Area Network) devices. WAN typically span over a wide area, such as over multiple cities / countries. WANS are connected over serial lines that 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".

2. Repeaters, Bridges, and Routers

- I. Repeaters work at Physical layer (Layer 1),
- II. Bridges and simple switches work at Data Link Layer (Layer 2),
- III. Routers work at Network Layer (Layer 3) of ISO Reference Model.

3.

1. The term "Segments" is usually associated with Transport layer
2. The term "Packets" is usually associated with Network Layer and
3. The term "Frames" is usually associated with Data Link Layer

4. Routing protocols job is to maintain routing tables and route packets appropriately. Examples of routing protocols are RIP, IGRP, EIGRP, OSPF. Routers can support multiple independent routing protocols and can update and maintain routing tables for each protocol independently. Routed protocols are used to transport user traffic from source node to destination node. Examples of routed protocols are IP, IPX, AppleTalk.

6. Standards

1. Standard adopted for Ethernet CSMA/CD by IEEE Committee is 802.3. 10BaseT (Fast Ethernet) uses IEEE803.2u standard which incorporates CSMA/CD protocol.

2.

Standard	Compliance
802.3	Standard for 10BaseT Ethernet CSMA/CD
802.3u	IEEE standard for 100BaseT (Fast Ethernet) incorporating CSMA/CD protocol.
802.3z	IEEE standard for Gigabit Ethernet
802.5	IEEE standard for Token Ring networks
802.11	IEEE standard for wireless LAN

7. Connectors and Cables

1. 10BaseT and 100BaseT use RJ-45 type of connector. 10Base2 (also called Thinnet) uses BNC connectors for attaching work stations. BNC-T is used to connect a work station 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.

2. 10BaseT Ethernet specifies UTP cabling. UTP cabling uses RJ-45 connectors to connect the cable to the NIC (Network Interface Card).

3.

1. 10BaseT is an example of STAR topology
2. 10Base2 is an example of BUS topology
3. FDDI is an example of fiber optic network based on ring topology.

10Base2 cable uses 50 Ohm, RG-58 cable also called Thinnet.

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

4. 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.

5. Given below are the distance limitations of Fast Ethernet specification:

100BaseTX ---- Cat 5 UTP, 2 pair ----- 100 meters
100BaseT4 ----- Cat 3,4,5; UTP, 4 pair --100 meters
100BaseFX ----- MMF cable ----- 400 meters

6. The distance specification for various media type 1000BaseXX is as given below:

1000BaseCX --- Copper shielded twisted pair---25 meters
1000BaseT----- Cat 5 UTP, 4 pair-----100 meters
1000BaseSX----- Multimode fiber cable -----260 meters
1000BaseLX----- Single mode fiber cable----- 3 km

7. Thicknet:

The maximum segment length of a 10Base5 Thicknet is 500 meters.

Maximum number of segments:5
Maximum segments with nodes: 3
Maximum number of repeaters: 4
Maximum overall length with repeaters: 2.5 kilometers
Maximum AUI drop cable length: 50 meters

Thicknet uses 15 pin AUI connector.

8. 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

8. Others

1. 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.

2. Spanning Tree Protocol (STP) IEEE Specification 802.1d is used to prevent routing loops. Cisco Catalyst 5000 series switches use BDPUs (Bridge Protocol Data Units) to determine the spanning tree topology. STP uses a Tree Algorithm (STA) to prevent loops, resulting in a stable network topology.