STUDY GUIDE

CompTIA

Network+

(N10-003)

Robert J. Shimonski

Network+ Certified and Recertified Since Exam Inception
Network+ Best Selling Book Author
CompTIA.org Subject Matter Expert (SME) and Exam Developer

ExamForce

About the Author

Robert J. Shimonski (CompTIA HTI+, Security+, Server+, e-Biz+, Inet+, **Network+**, A+, TruSecure TICSA, Cisco CCDP, CCNP, Cisco Firewall Specialist, Nortel NNCSS, Microsoft MCSE, MCP+I, Novell Master CNE, CNE 4/5/6, CIP, CIBS, IWA CWP, Prosoft MCIW, SANS GSEC, GCIH, Symantec SPS and NAI Sniffer SCP is a Network Manager for a leading manufacturing company. Robert's technical specialties include network infrastructure design with the Cisco and Check Point product lines, Systems Engineering with Microsoft and Novell technologies and troubleshooting with **Sniffer** technologies.

Robert has served as a Subject matter Expert (SME) for CompTIA.org, the creators of the Network+ exam. Robert has helped not only beta test just about every certification created through CompTIA, but also helped CompTIA to create exam questions for exams such as HTI+ and eBiz+. He was selected based on his networking expertise and history of developing highly needed top quality material for most of the leading certification software vendors and book publishers worldwide.

Robert is also a best-selling author (www.rsnetworks.net) of many security related articles and published books to include: "Sniffer Network Optimization and Troubleshooting Handbook" from Syngress Media Inc (ISBN: 1931836574), Security+ Study Guide and DVD Training System (ISBN: 1931836728) and the newly upcoming and highly anticipated Network+ study guide (ISBN: 1931836426) based on the new 2005 objectives, all from Syngress Media Inc.

About the Exam

CompTIA Network+ Certification is awarded after passing one exam created by CompTIA, one of the world's leaders in certification testing. The CompTIA Network+ certification is an international industry credential that validates the knowledge of networking professionals with at least nine months of experience in network support or administration or adequate academic training. Nine months is recommended, not mandatory. A typical candidate would have CompTIA A+ certification or equivalent knowledge, but this is not a prerequisite, just helpful if the candidate is new to certification testing and networking in general. An accepted foundation-level, vendor-neutral certification for networking professionals, many IT certifications integrate CompTIA Network+ into their curriculums. There are approximately 135,000 CompTIA Network+ certified professionals worldwide. The skills and knowledge measured by this examination were derived from an industry-wide job task analysis and validated through an industry-wide survey of more than 2,500 participants. The Network+ exam is one of the most sought after certifications in CompTIA's arsenal of certification programs, right next to one of the biggest leaders, which is A+. Network+ has half a decade of existence behind it, and if prepared for properly, is a credential that never expires, that you can hold and build on and be proud of achieving.

There are four major topic areas (domains) that make up 100% of this exam:

- Domain 1.0: Media and Topologies (20%)
- Domain 2.0: Protocols and Standards (20%)
- Domain 3.0: Network Implementation (25%)
- Domain 4.0: Network Support (35%)

Objectives

Domain 1.0 - Media and Topologies 20%

1.1 Recognize the following logical or physical network topologies given a diagram, schematic or description:

- Star
- Bus
- Mesh
- Ring

1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (token ring), 802.11 (wireless), and FDDI (Fiber Distributed Data Interface) networking technologies, including:

- Speed
- Access method (CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) and CSMA/CD
- (Carrier Sense Multiple Access/Collision Detection))
- Topology
- Media

1.3 Specify the characteristics (For example: speed, length, topology, and cable type) of the following cable standards:

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

1.4 Recognize the following media connectors and describe their uses:

- RJ-11 (Registered Jack)
- RJ-45 (Registered Jack)
- F-Type
- ST (Straight Tip)
- SC (Standard Connector)
- IEEE1394 (FireWire)
- Fiber LC (Local Connector)
- MTRJ (Mechanical Transfer Registered Jack)
- USB (Universal Serial Bus)

1.5 Recognize the following media types and describe their uses:

- Category 3, 5, 5e, and 6
- UTP (Unshielded Twisted Pair)
- STP (Shielded Twisted Pair)
- Coaxial cable
- SMF (Single Mode Fiber) optic cable

- MMF (Multimode Fiber) optic cable

1.6 Identify the purposes, features and functions of the following network components:

- Hubs
- Switches
- Bridges
- Routers
- Gateways
- CSU/DSU (Channel Service Unit/Data Service Unit)
- NICs (Network Interface Card)
- ISDN (Integrated Services Digital Network) adapters
- WAPs (Wireless Access Point)
- Modems
- Transceivers (media converters)
- Firewalls

1.7 Specify the general characteristics (For example: carrier speed, frequency, transmission type and topology) of the following wireless technologies:

- 802.11 (Frequency hopping spread spectrum)
- 802.11x (Direct sequence spread spectrum)
- Infrared
- Bluetooth

1.8 Identify factors which affect the range and speed of wireless service (For example: interference, antenna type and environmental factors).

Domain 2.0 Protocols and Standards 20%

2.1 Identify a MAC (Media Access Control) address and its parts.

2.2 Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions.

2.3 Identify the OSI (Open Systems Interconnect) layers at which the following network components operate:

- Hubs
- Switches
- Bridges
- Routers
- NICs (Network Interface Card)
- WAPs (Wireless Access Point)

2.4 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability and naming conventions:

- IPX/SPX (Internetwork Packet Exchange/Sequence Packet Exchange)
- NetBEUI (Network Basic Input/Output System Extended User Interface)
- AppleTalk/AppleTalk over IP (Internet Protocol)
- TCP/IP (Transmission Control Protocol/Internet Protocol)

2.5 Identify the components and structure of IP (Internet Protocol) addresses (IPv4, IPv6) and the required setting for connections across the Internet.

2.6 Identify classful IP (Internet Protocol) ranges and their subnet masks (For example: Class A, B and C).

2.7 Identify the purpose of subnetting.

2.8 Identify the differences between private and public network addressing schemes.

2.9 Identify and differentiate between the following IP (Internet Protocol) addressing methods:

- Static
- Dynamic
- Self-assigned (APIPA (Automatic Private Internet Protocol Addressing))

2.10 Define the purpose, function and use of the following protocols used in the TCP/IP (Transmission Control Protocol/Internet Protocol) suite:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- FTP (File Transfer Protocol)
- SFTP (Secure File Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol) HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- POP3/IMAP4 (Post Office Protocol version 3/Internet Message Access Protocol version 4)
- Telnet
- SSH (Secure Shell)
- ICMP (Internet Control Message Protocol)
- ARP/RARP (Address Resolution Protocol/Reverse Address Resolution Protocol)
- NTP (Network Time Protocol)
- NNTP (Network News Transport Protocol)
- SCP (Secure Copy Protocol)
- LDAP (Lightweight Directory Access Protocol)
- IGMP (Internet Group Multicast Protocol)
- LPR (Line Printer Remote)

2.11 Define the function of TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports.

2.12 Identify the well-known ports associated with the following commonly used services and protocols:

- 20 FTP (File Transfer Protocol)
- 21 FTP (File Transfer Protocol)
- 22 SSH (Secure Shell)
- 23 Telnet

- 25 SMTP (Simple Mail Transfer Protocol)
- 53 DNS (Domain Name Service)
- 69 TFTP (Trivial File Transfer Protocol)
- 80 HTTP (Hypertext Transfer Protocol)
- 110 POP3 (Post Office Protocol version 3)
- 119 NNTP (Network News Transport Protocol)
- 123 NTP (Network Time Protocol)
- 143 IMAP4 (Internet Message Access Protocol version 4)
- 443 HTTPS (Hypertext Transfer Protocol Secure)

2.13 Identify the purpose of network services and protocols (For example: DNS (Domain Name Service), NAT (Network Address Translation), ICS (Internet Connection Sharing), WINS (Windows Internet Name Service), SNMP (Simple Network Management Protocol), NFS (Network File System), Zeroconf (Zero configuration), SMB (Server Message Block), AFP (Apple File Protocol) and LPD (Line Printer Daemon)).

2.14 Identify the basic characteristics (For example: speed, capacity and media) of the following WAN (Wide Area Networks) technologies:

- Packet switching
- Circuit switching
- ISDN (Integrated Services Digital Network)
- FDDI (Fiber Distributed Data Interface)
- T1 (T Carrier level 1)/E1/J1
- T3 (T Carrier level 3)/E3/J3
- OCx (Optical Carrier)
- X.25

2.15 Identify the basic characteristics of the following internet access technologies:

- xDSL (Digital Subscriber Line)
- Broadband Cable (Cable modem)
- POTS/PSTN (Plain Old Telephone Service/Public Switched Telephone Network) Satellite
- Wireless

2.16 Define the function of the following remote access protocols and services:

- RAS (Remote Access Service)
- PPP (Point-to-Point Protocol)
- SLIP (Serial Line Internet Protocol)
- PPPoE (Point-to-Point Protocol over Ethernet)
- PPTP (Point-to-Point Tunneling Protocol)
- VPN (Virtual Private Network)
- RDP (Remote Desktop Protocol)

2.17 Identify the following security protocols and describe their purpose and function:

- IPSec (Internet Protocol Security)
- L2TP (Layer 2 Tunneling Protocol)
- SSL (Secure Sockets Layer)

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- 802.1x

2.18 Identify authentication protocols (For example: CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol), RADIUS (Remote Authentication Dial-In User Service), Kerberos and EAP (Extensible Authentication Protocol)).

Domain 3.0 Network Implementation 25%

3.1 Identify the basic capabilities (For example: client support, interoperability, authentication, file and print services, application support and security) of the following server operating systems to access network resources:

- UNIX/Linux/Mac OS X Server
- Netware
- Windows
- Appleshare IP (Internet Protocol)

3.2 Identify the basic capabilities needed for client workstations to connect to and use network resources (For example: media, network protocols and peer and server services).

3.3 Identify the appropriate tool for a given wiring task (For example: wire crimper, media tester/certifier, punch down tool or tone generator).

3.4 Given a remote connectivity scenario comprised of a protocol, an authentication scheme, and physical connectivity, configure the connection. Includes connection to the following servers:

- UNIX/Linux/Mac OS X Server
- Netware
- Windows
- Appleshare IP (Internet Protocol)

3.5 Identify the purpose, benefits and characteristics of using a firewall.

3.6 Identify the purpose, benefits and characteristics of using a proxy service.

3.7 Given a connectivity scenario, determine the impact on network functionality of a particular security implementation (For example: port blocking/filtering, authentication and encryption).

3.8 Identify the main characteristics of VLANs (Virtual Local Area Networks).

3.9 Identify the main characteristics and purpose of extranets and intranets.

3.10 Identify the purpose, benefits and characteristics of using antivirus software.

3.11 Identify the purpose and characteristics of fault tolerance:

- Power
- Link redundancy

- Storage
- Services

3.12 Identify the purpose and characteristics of disaster recovery:
- Backup/restore
- Offsite storage
- Hot and cold spares
- Hot, warm and cold sites

Domain 4.0 Network Support 35%

4.1 Given a troubleshooting scenario, select the appropriate network utility from the following:
- Tracert/traceroute
- ping
- arp
- netstat
- nbtstat
- ipconfig/ifconfig
- winipcfg
- nslookup/dig

4.2 Given output from a network diagnostic utility (For example: those utilities listed in objective 4.1), identify the utility and interpret the output.

4.3 Given a network scenario, interpret visual indicators (For example: link LEDs (Light Emitting Diode) and collision LEDs (Light Emitting Diode)) to determine the nature of a stated problem.

4.4 Given a troubleshooting scenario involving a client accessing remote network services, identify the cause of the problem (For example: file services, print services, authentication failure, protocol configuration, physical connectivity and SOHO (Small Office/Home Office) router).

4.5 Given a troubleshooting scenario between a client and the following server environments, identify the cause of a stated problem:
- UNIX/Linux/Mac OS X Server
- Netware
- Windows
- Appleshare IP (Internet Protocol)

4.6 Given a scenario, determine the impact of modifying, adding or removing network services (For example: DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name Service) and WINS (Windows Internet Name Service)) for network resources and users.

4.7 Given a troubleshooting scenario involving a network with a particular physical topology (For example: bus, star, mesh or ring) and including a network diagram, identify the network area affected and the cause of the stated failure.

4.8 Given a network troubleshooting scenario involving an infrastructure (For example: wired or wireless) problem, identify the cause of a stated problem (For example: bad media, interference, network hardware or environment).

4.9 Given a network problem scenario, select an appropriate course of action based on a logical troubleshooting strategy. This strategy can include the following steps:

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

Domain 1.0 - Media and Topologies

Chapter 1

Quick Jump To:

- Objective 1.1
- Objective 1.2
- Objective 1.3
- Objective 1.4
- Objective 1.5
- Objective 1.6
- Objective 1.7
- Objective 1.8

Medias and Topologies make up the technologies that in which data travels. In this section of the study guide we will cover such technologies to include but not limited to, cabled and wired technologies. This section of the study guide covers 20% of the overall exam.

Exam Objectives Covered:

1.1 Recognize the following logical or physical network topologies given a diagram, schematic or description:

a. Star
b. Bus
c. Mesh
d. Ring

1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (token ring), 802.11 (wireless), and FDDI (Fiber Distributed Data Interface) networking technologies, including:

a. Speed
b. Access method: (CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
c. Access method: CSMA/CD (Carrier Sense Multiple Access/Collision Detection))
d. Topology
e. Media

1.3 Specify the characteristics (For example: speed, length, topology, and cable type) of the following cable standards:

a. 10BASE-T and 10BASE-FL
b. 100BASE-TX and 100BASE-FX
c. 1000BASE-TX, 1000BASE-CX, 1000BASE-SX and 1000BASE-LX
d. 10GBASE-SR, 10GBASE-LR and 10GBASE-ER

1.4 Recognize the following media connectors and describe their uses:

a. RJ-11 (Registered Jack)
b. RJ-45 (Registered Jack)
c. F-Type
d. ST (Straight Tip)
e. SC (Standard Connector)
f. IEEE1394 (FireWire)
g. Fiber LC (Local Connector)
h. MTRJ (Mechanical Transfer Registered Jack)
i. USB (Universal Serial Bus)

1.5 Recognize the following media types and describe their uses:

a. Category 3, 5, 5e, and 6
b. UTP (Unshielded Twisted Pair)
c. STP (Shielded Twisted Pair)
d. Coaxial cable
e. SMF (Single Mode Fiber) optic cable
f. MMF (Multimode Fiber) optic cable

1.6 Identify the purposes, features and functions of the following network components:

a. Hubs
b. Switches
c. Bridges
d. Routers
e. Gateways
f. CSU/DSU (Channel Service Unit/Data Service Unit)
g. NICs (Network Interface Card)
h. ISDN (Integrated Services Digital Network) adapters
i. WAPs (Wireless Access Point)
j. Modems
k. Transceivers (media converters)
l. Firewalls

1.7 Specify the general characteristics (For example: carrier speed, frequency, transmission type and topology) of the following wireless technologies:

a. 802.11 (Frequency hopping spread spectrum) FHSS
b. 802.11 (Direct sequence spread spectrum) DSSS
c. Infrared
d. Bluetooth

1.8 Identify factors which affect the range and speed of wireless service (For example: interference, antenna type and environmental factors).

1.1 Recognize the following logical or physical network topologies given a diagram, schematic or description:

In this objective you will be expected to know how to describe the following topologies, know their pros and cons as well as how to select which topology should be used for any situation. In this section we cover the Star, Bus, Mesh and Ring topologies.

Star Topology

A Star Topology is physical network topology that has all connections terminating into a centralized concentrator as seen in the illustration. A switch (normally used to create a Star topology) is used to have all devices centrally connect to a device that will record its MAC address after the flooding stage, once completed; each device can communicate with other devices on the Star. Star topologies are easy to add on to as well. You can add up to 5 more devices to this particular switch. As well, you can uplink this star into another portion of the network.

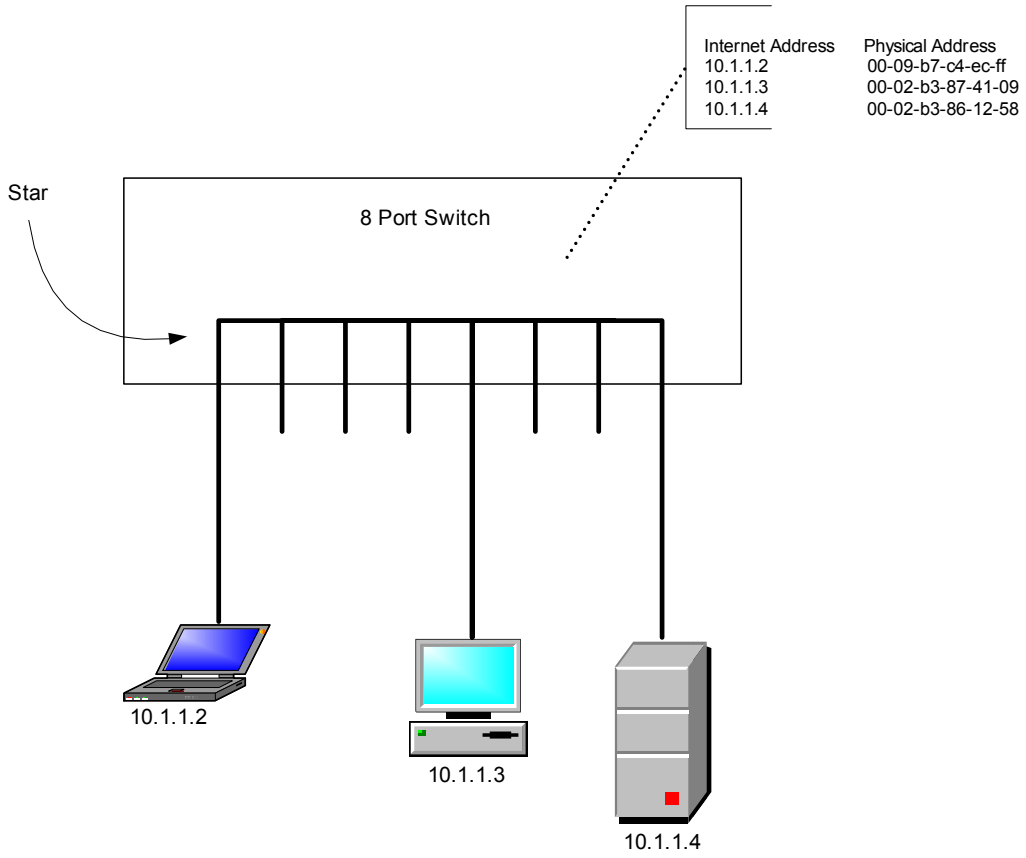


Fig: *Star Topology*

Star Topology commonly uses 10BaseT, 100BaseT. Easy and cheap cabling is used for a Star topology. Unshielded (or Shielded - STP) Twisted Pair (UTP) cabling can be used. It is easy to maintain a Star, considering that you only need to ensure that you have a concentrator and good cabling connections into the device. It is also easy to grow the network with this topology. As long as you follow standards and rules set forth by the IEEE, a star is very easy to expand to facilitate network growth.

The bandwidth on the network is not fully optimized because there is a large amount of broadcast based traffic, either via Flooding, ARP, CSMA/CD, which are all normal processes that are covered later in this guide, but they still use up available bandwidth.

There are limitations as to what can be done with a Star topology. For one, each node that connects to the Star can be no farther than 100 Meters (approximately 330') from it without the use of a repeating device to regenerate the signal. Only 1024 nodes can be added to a single LAN. This cannot be added to without breaking up the LAN into smaller segments. There is also a 5-4-3 rule which dictates that there will be no more than 5 network segments broken down by 4 segmentation devices (switches) and no more than 3 of them can be populated by nodes. Again, these are not show stoppers to using the technology, it is just essential that you know what those limitations are so that you do not overstep them and degrade performance of the network.

Bus Topology

A Bus Topology is pretty outdated and although normally not installed anymore, you will still find it out there in your travels as a network+ technician. A Bus is nothing more than what you may already know about from PC based Planer Boards. Signals are sent along the bus to get to and from Disks, memory, CPU and so on. The network Bus is similar in theory. Data travels along the Bus to get from node to node. In the Illustration, you can see how this is laid out.

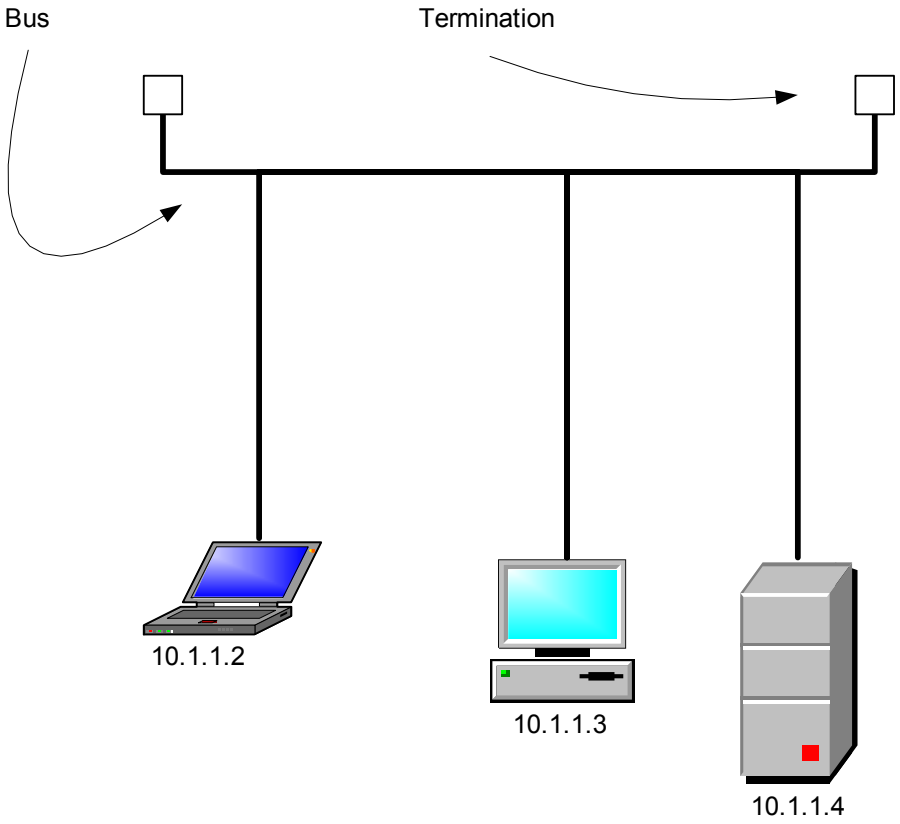


Fig: *Bus Topology*

Not widely seen, no longer widely deployed, a Bus topology was commonly seen before Star topologies became cost efficient (being able to by a hub, bridge or switch) and today, most of what is left is deemed legacy. This is in widely seen with 10Base2 (thinnet) and 10Base5 (thicknet).

The Bus is normally formed up from a 50 Ohm coaxial cable which connects all the computers in the LAN. This is seen in the illustration. Each segment is terminated at both ends by 50 Ohm resistors. This is done so as to prevent reflections from the discontinuity at the end of the cable. Each segment is also normally run to earth ground at one end for electrical safety.

Good for small networks because you can forgo the cost of a concentrator device, but honestly, since it would be almost impossible to find thinnet for sale to use with all the connection hardware, and most 5 port hubs can be bought for under 40 US dollars, it is not uncommon to see small networks still use a Star topology. Bus topologies are old and outdated but still in use!

It is very hard to troubleshoot Bus topologies because any break in the bus can be a break in the network, as well, this break needs to be isolated or located to a specific connection point and repaired. It is easy to crash, considering that one break on the network can potentially bring down the whole network.

Mesh Topology

A Mesh Topology is a topology that means nothing more than two ways to every path, or a redundant path. A good example of a Mesh topology is seen in the illustration. Inside the cloud in the illustration shows what is called a Mesh. Each site connected to the MPLS (Multi Protocol Label Switching) Wide Area Network (WAN), connects into a cloud that is meshed so that any site wanting to talk to another site has the shortest distance to choose from, so in the case of a host on the 10.1.1.0 network wanting to talk to a host on the 10.1.2.0 network, the path is clear, the traffic sent from one host to the other enters the routers, leaves the routers and goes into the cloud where within the cloud a mesh network is setup to get the traffic from point A to B very quickly and efficiently. Most commonly shown in Network+ books as a bunch of PCs connected with a bunch of lines to each other, this just is not realistic. Who connects PCs in this fashion? A mesh network is most commonly seen in MPLS networks, and other WAN.

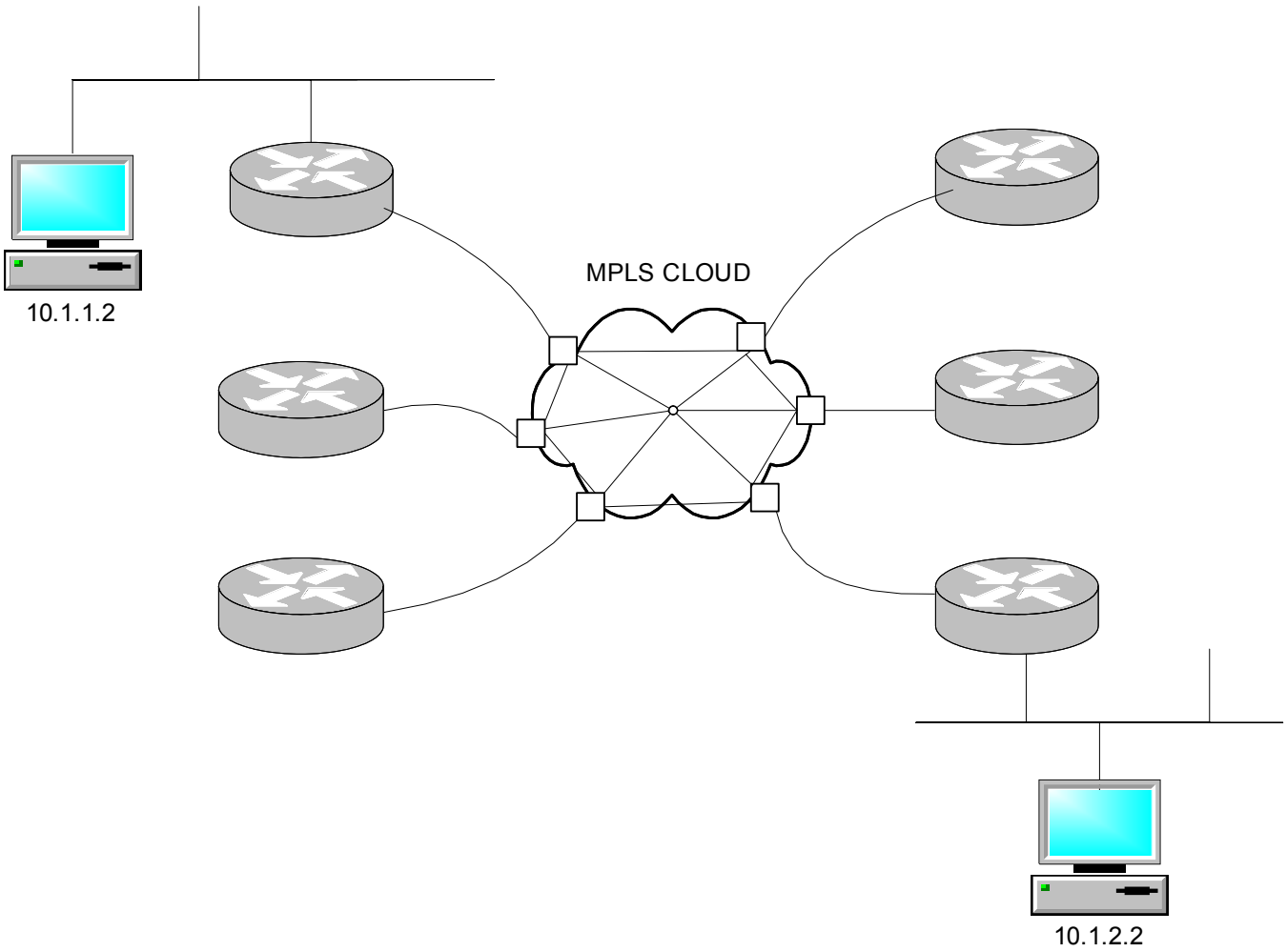


Fig: *Mesh Topology*

A mesh is expensive for a few reasons. One, telecommunications lines will always cost more than your standards LAN technologies like Ethernet, Fast Ethernet, etc. Two, there is redundancy involved, which always means extra cost. Whenever you make something redundant, most times you are adding to it which inevitably costs money. Every device on your network is connected to every other device on your network. This creates a nice blanket of redundancy, but you will pay for it.

A Mesh (or also commonly called a *Full Mesh*) is a topology that is also difficult to design, implement and manage. With multiple paths to choose from through the network, it is imperative that it is designed and implemented then managed correctly to ensure that the return on investment (ROI) is there, if not, then you have a large network that is not efficient.

The biggest benefit is for disaster recovery purposes (multiple paths through the network), as well, the second biggest benefit is with speed. Since there is a mesh, a path can be found through the network quickly, and the path chosen (if designed and implemented correctly) should be the quickest from the source to the destination.

Mesh topologies are normally never found on PCs can be configured for clustered servers with multiple NICs, and WAN topologies such as MPLS.

Ring Topology

A Ring Topology is based on the design that all nodes on the network are connected into the concentrator via a circle as seen in the illustration. It is hard to conceptualize this because the concentrator used looks like a switch or a hub so you would confuse this with a Star topology, but the internal configuration of the concentrator shows that with a Ring topology, the internals of the concentrator are laid out logically like a ring and a token passes throughout from node to node ready for work. In the concentrator (in older IBM, Token Ring days, these were known as Multi Station Access Units or MAUs for short), there is no shared media, like with a Star. NO contention takes place because the nodes on the Star would be contending for time on the network via CSMA/CD. Rings are deterministic.

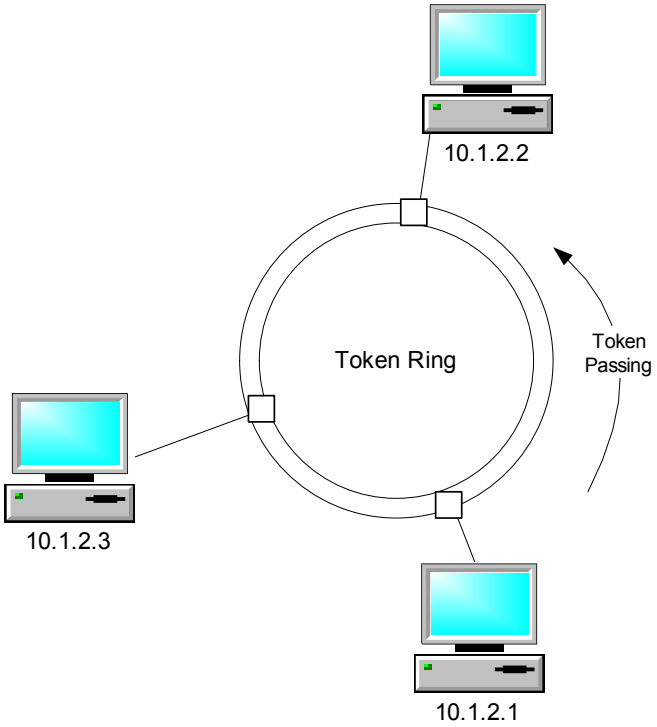


Fig: *Ring Topology*

Local LAN Rings are not used very often any more, but like a Bus, they are still out there and require someone's attention. Rings (Token Ring, SONET Ring, FDDI Ring, etc) are usually these days kept to specific segments of your network like the *Backbone* or *Core* where reliable high speed data transfer is required. Also, many legacy Mainframes (IBM) that still exist many times have a Token Ring NIC installed. Many times, this may be the Ring topology on your network you have work with. Most Token Ring Local Area Networks have been replaced by the more common Star topologies which means high speed switches and Category 5 UTP based cable. Rings also use this cabling, but can also be found using very old TYPE based cabling design and created by IBM. This cabling resembles the 10Base5 thicknet used in older networks rolled out years ago.

Since most folks are not rolling out Token Ring these day or that they are using it in small niche sections of their network or in high speed areas, it should be known already that this equipment is costly compared to what you can get to build a Star topology. Rings are also falling by the wayside because many companies are standardizing their technologies to reduce administrative overhead and to reduce costs.

NOTE: You need to know the topologies well enough to distinguish them from each other on the exam. Make sure you remember the key points that make them similar as well as different. Be able to see a diagram and know what topology you are referencing from the diagram.

1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (token ring), 802.11 (wireless), and FDDI (Fiber Distributed Data Interface) networking technologies, including:

In this objective you will be expected to know the main features of some IEEE standards and other technologies paying respect to their speed, how they access the network, their topologies and media used.

802 Standards

802 standards have some unique history to them, especially the name. The IEEE which stands for Institute of Electrical/Electronic Engineers can be found at their home base online: www.ieee.org.

The first meeting of the IEEE Computer Society "Local Network Standards Committee", Project 802, was held in February of 1980. If you think about the month and the year, it may help you remember. 80 was the year, it was the 2nd month (February), hence 802. Project 802 began to grow and now over 20 years later, we can see from the table below, their work continued to grow with their efforts, expanding into Wireless, Security, and Fiber Optics.

Why a need for such a group? A set of standards was released to keep the networking world down the path to standardization so that we did not have a few companies rolling out their own versions of Ethernet which is essentially what did in fact happen. To keep things standardized (and under the operation of the board of engineers assigned to help suggest changes, ratify changes, etc), meant that vendors can now develop product (like Network Interface Cards) against one standard instead of many. It just makes things easier all around. The following table lists out all the major 802 based standards that you will need to know for the Network+ exam.

802.1	Bridging & Management
802.2	Logical Link Control
802.3	CSMA/CD Access Method
802.4	Token-Passing Bus Access Method
802.5	Token Ring Access Method
802.6	DQDB Access Method
802.7	Broadband LAN
802.8	Fiber Optic LAN/MAN
802.9	Integrated Services LAN Interface
802.10	Security
802.11	Wireless (this encompasses – 802.11, 802.11a, 802.11b, 802.11g)
802.12	Demand Priority Access
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metropolitan Area Networks

A good online view of these standards can be found here.

You must know what the 802 standards are, and why they are important. You should know each one by memorization. It would be important to remember them all, but the key 802 standards you will want to know off the top of your head is 802.2, 802.3, 802.5, 802.10 and 802.11. In the table, wireless was expanded on to show all groupings within the 802.11 committee, you can now see that .a, .b and so on are all separate groups under the main 802.11 committee. You will want to know the very key ones such as Wireless.

Access method: (CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

Access methods are just that, the method used to access the network medium. CSMA/CA, which is short for *Carrier Sense Multiple Access/Collision Avoidance* represents a standard for a network protocol which allows for any node connected to the network transmit data without colliding into another node sending data at the same time because the collision is avoided via the process. All techniques have a pro and con set associated with them. Collision Avoidance does just that, it avoids collisions that would force a resend which would cause more network traffic, but – to facilitate this functionality, CSMA/CA has more overhead which in turn creates more traffic on the network.

Access method: CSMA/CD (Carrier Sense Multiple Access/Collision Detection))

Access methods are just that, the method used to access the network medium. CSMA/CD is short for *Carrier Sense Multiple Access/Collision Detection*, which represents a standard for a network protocol which allows for any node connected to the network transmits data, but each node has to listen for its turn on the network to do so. This means that all nodes contend for time on the network. This is basically a set of rules (and algorithms) which will determine how nodes respond when any two nodes attempt to use a data channel simultaneously. If two nodes talk simultaneously, you get what is called a collision.

So, one would ask, "How does each station know when to transmit?" Well, that is easy if you know the standard. Standard Ethernet networks use CSMA/CD so if in use, then the standard will enable an algorithm in which a node transmitting on the network can detect that a collision has taken place, it will know how recover from it. After detecting a collision, a node will wait a random delay time and then attempt to re-transmit the message. If the device detects a collision again, it waits two times as long and ill try to re-transmit the message again. The term for this is known as exponential back off.

802.2

The IEEE formed a committee to create 802.2. The IEEE 802.2 standard is identical for all network topologies so it does not matter if you have Star or Bus. It provides a standard interface between the protocols such as IPX and IP and the different network types like Ethernet.

It is imperative to remember that 802.2 is the LLC (Logical Link Control.) You should also know that the packets generated by the LLC layer are called PDUs (Protocol Data Units). LLC is a sublayer of the Data Link layer of the OSI model. The other sublayer is the MAC or Media Access Control sublayer.

802.3

The IEEE formed a committee to create 802.3. The IEEE 802.3 standard was originally developed by Xerox. It was eventually standardized as the IEEE 802.3 based on the Ethernet DIX standard. The DIX standard comprised of companies who originally created the specification which are Digital, Intel, and Xerox, hence DIX.

The IEEE 802.3 standard covers all Ethernet based networks such as 10 megabits per second (Mbps), 100 Mbps, and 1000 Mbps networks. One thing to consider is that Ethernet is NOT Fast Ethernet; they are different standards, so they rate different subcommittees.

In 1995, the IEEE defined the 802.3u Fast Ethernet standard (100BaseTX, 100BaseT4, 100BaseFX.). In 1998, the IEEE defined the 802.3z Gigabit Ethernet over Fiber standard, and later in the year, 802.3ab Gigabit Ethernet over UTP was developed. 802.3 is based on CSMA/CD

These are but just a few examples of different subcommittees and all the work that goes into standardizing traffic – and this is just the Data Link layer!

802.5

The IEEE formed a committee to create 802.5. The IEEE 802.5 standard defines Token Ring. A Token Ring is a local area network (LAN) based on the CSMA/CA access method which makes it deterministic. This means that all nodes are connected to the ring (as seen in the Ring topology section of this study guide) and a bit (or token) passing scheme is used to keep collisions out of the network, this happens because the token is passed to whomever wants to transmit data and that node uses that time to send its data. This is how collisions are prevented, because they actually do not take place. Nodes are not contending for space on the network, so they just wait their turn within the Ring.

In reality, Token Ring (and 802.5 for that matter), is not really implemented new anymore, you will see more legacy implementation of it, most likely connected to an IBM mainframe in your companies infrastructure. The IBM Token Ring protocol (which was not a standard at that time and more proprietary technology) led to a standard version, specified as 802.5 by the IEEE. Token Ring (mostly because of its reliability) is one of the most widely used network technologies right below Ethernet. Ethernet gained steam because it was cheaper, easier to implement and quicker to troubleshoot. Token Ring has continued through the years into switching-based rings and has become a really solid technology but it has lost its momentum so like was just mentioned, it is not implemented as much as it used to be in years past.

A Token Ring is a local area network (LAN) based on the CSMA/CA access method which makes it deterministic. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second.

802.11

The IEEE formed a committee to create 802.11. The IEEE 802.11 standard is based around wireless technologies. In 2001, the IEEE standardized 802.11 wireless technologies. Coming out at a whopping megabit per second, Wireless was more about awe than a great technology. Not having to use wires astonished everyone as wireless technology seemed to open a million new doors in the IT industry (and it did). The problem was it was slow, unsecure, and totally unreliable. Now wireless is getting better with speeds up to 54 Mbps reachable in just about any home and company who can purchase the equipment. There have also been many enhancements to make it more reliable and secure. Another great aspect over time is that now it is cheaper as well, when first released, wireless was a bit costly. The IEEE released 802.11. Soon after, 802.11b was released to the public as a standard that would bring more benefits to the 802.11 standard. First, a bigger speed increase. 802.11b will operate at 11 Mbps. It only got (and still gets) each day. Today, we have 802.11g hardware accessible to the general public and their homes, we have coffee shops and airports where you can get a wireless link from an Access Point (AP) and get internet access and check your email.

- 802.11= 1 Mbps
- 802.11b = 11 Mbps (ISM band)
- 802.11a = 54 Mbps UNNI band
- 802.11g = 54 Mbps ISM band
- 802.11, 802.11b and 802.11g are compatible
- 802.11a requires different antennas (and hardware) as it operates in a different radio band

The farther away you get from an access point directly affects the coverage you have, as well as the speed of your connection.

NOTE:	You need to know that 802.11 will also consist of 802.11, 802.11a, 802.11b, and 802.11g. The most common standard in use today for wireless networks, the 802.11b standard defines DSSS networks that use the 2.4GHz ISM band and communicate at speeds of 1, 2, 5.5 and 11 Mbps. Understanding wireless for the exam is important, but at the Network+ level, you do not need to be a Wireless Network Engineer to pass the exam, but with current industry trends and how mobile the workforce is getting, it would be to your best interests to visit the links I provided in the Links and Resources section of this study guide. There are short articles and primers in there that will reinforce all that you need to fundamentally know to understand how wireless networking takes place. This knowledge will help you to pass the Network+ exam and feel confident while sitting the exam that you have covered most everything that you will need to know on the exam about wireless technologies.

1.3 Specify the characteristics (For example: speed, length, topology, and cable type) of the following cable standards:

In this objective you will be expected to know the following cabling standards as well as certain characteristics that make them up. This means understanding what each piece of 10BaseT really means. The 10 symbolizes that maximum transmission speed. This would mean that 10BaseT operates at 10 Mbps. The Base, defines the signal method. Since it is 10 Base T that signifies that it is using Baseband technology, (instead of Broadband for instance). The T symbolizes the media type. In this instance, T signifies Twisted Pair be used.

This is not always true. 10Base2 would mean that this thinnet solution would be able to reach a maximum distance of 200 meters. This is actually false as the maximum distance is really 185 meters. It probably would have sounded silly to say 10Base185 so they probably just rounded it up. ☺

10BASE-T, 10BASE-FL, 100BASE-TX and 100BASE-FX, 1000BASE-TX, 1000BASE-CX, 1000BASE-SX, and 1000BASE-LX

For the Network+ exam you need to know the following cable standards. Beyond the scope of the exam, to be a well prepared Network Technician, Engineer, Analyst or Manager, you will find knowing these characteristics can quickly help you in a jam when trying to order and purchase networking equipment, trying to order cable or design and implement a network. Yes, you can most likely pull out a chart and get this information from there, but for the exam, the test wants to ensure that you can pretty much pull the following from memory come test time. It also helps you know at the very least, the fundamentals of what cable standards are found on most networks today and how to correctly, identity the right connectors and see what the maximum distances you can run copper cabling or fiber.

Standard	Media Type	Cable Length	Transfer Speed	Connector
10BaseT	Cat3 or higher UTP	100 meters	10 Mbps	RJ45
100BaseTX	Cat5 or higher UTP	100 meters	10 Mbps	RJ45
100BaseFX	Fiber optic	100 meters	10 Mbps	Fiber optic
1000BaseT	Cat5 or higher UTP	100 meters	10 Mbps	RJ45
1000BaseSX	Fiber optic	100 meters	10 Mbps	Fiber optic
1000BaseLX	Fiber optic	100 meters	10 Mbps	Fiber optic
1000BaseCX	Fiber optic	100 meters	10 Mbps	Fiber optic

- Cat = Category. Category 5e cabling. Cat5e cabling.
- UTP is Unshielded Twisted Pair
- STP is Shielded Twisted Pair

SC and ST connectors are optical fiber connector types. SC and ST are commonly found on networking equipment such as Nortel, 3Com or Cisco switches and hubs. Fiber optics connections are actually quite diverse. A search on the web will show you at least a dozen or more types of connections that can be created for many different needs, so you are not going to need to memorize optical fiber connectors for the exam beyond what is commonly known and seen. It does make sense to research this anyway, so you know for future reference all the different types of connections you can make (and why) with optical fiber.

10BaseFL is an older 10 Mbps fiber based technology. This is primary where you would see older ST based connectors in use.

NOTE: Memorizing this chart will ensure that you are ready come test time to rattle off the fundamentals of cabling standards in use today (copper and fiber) and what connecters they use, their maximum distance in meters, what the media type is and their designation. Since 10G

10 Gigabit Ethernet (10GBASE-SR, 10GBASE-LR and 10GBASE-ER)

For the Network+ exam you will need to know the fundamentals of 10 Gigabit Ethernet. In 2002, the IEEE finalized work on the 802.3ae standard which defines a version of Ethernet with a nominal data rate of 10Gbps, ten times faster than Gigabit Ethernet at 1000 Mbps.

10GBaseSR will support short distances over multi-mode (mm) fiber optic cable. It also has a range of between 26m and 82m depending on cable type, and it supports 300m operation over a new 2000MHz.km multi-mode (mm) fiber.

10GBaseLX4 uses wavelength division multiplexing (WDM) to support ranges of between 240m and 300m over multi-mode (mm) cabling. It also supports 10km over single-mode (sm) fiber, as does 10GbaseLR. 10GBaseER standard supports 40km over single-mode (sm) fiber.

10 Gigabit Ethernet is new and gaining acceptance as time moves on. We shall hopefully see a commercial version in the making, but only time will tell. Since there are many different methods of using 10 Gigabit Ethernet (such as over a LAN or a WAN), it remains to be seen where 10 Gigabit

Ethernet is heading and where it may end up. For the Network+ exam, make sure that you visit the Links section of the study guide to visit the 10 Gigabit Ethernet Alliance site so that you can get up to date information come exam time. As with any very new (and changing) technology, when you go to sit an exam, it always makes sense to see what may have changed or what is new.

NOTE: Make sure at a minimum, you know the fundamentals of 10GBaseSR, 10GBaseLR and 10GBaseER.

1.4 Recognize the following media connectors and describe their uses:

In this objective you will be expected to know the most commonly used connectors and all the factoids about them such as characteristics, use or design.

RJ-11 (Registered Jack)

The RJ-11 connector is something that you have probably been looking at for years and perhaps if you never knew its definition, only now know what it is formally called. Every time you pick up your telephone at home, it is a good chance that somewhere on that phone or base unit is a RJ-11 connection. An RJ-11 connector is primarily used in the United States and its surrounding territories, so internationally it may not be as widely known or seen. It is not commonly used for data networks, although it can be used, it is recommended that you use newer technology, which is currently the RJ-45 connector. RJ-11 connectors are most commonly seen and used on PSTN (Public Switched Telephone Network) which is nothing more than the international telephone system based on copper wires carrying analog voice to the homes of people worldwide depending on where it is deployed.

RJ-45 (Registered Jack)

RJ-45 is short for Registered Jack-45. This is a cable termination that specifics an eight-wire connector which is used to connect computers and create a network. These are the most commonly seen termination types you are likely to see. RJ-45s are found on Token Ring and Ethernet networks. Telecommunications connections used on a WAN most commonly are seen with RJ-45 connections. Commonly confused with RJ-11s, RJ-45s are easy to distinguish from RJ-11s by simply looking at the width; the wider termination is an RJ-45.

F-Type

F or F-Type connectors are most commonly seen with Coaxial cable termination. Seen at the end of RG58 or RG59 coaxial, F-Type connectors normally have screw on capabilities for cable TV, and when order with no corrosive material, can last indefinitely. Make sure you can identify what cable type the F-Type connector is used with.

ST (Straight Tip)

An ST connector is most commonly found on fiber optic cable. ST stands for *straight tip* and is the older version of the most commonly used fiber connector, now the most common is SC. The tip of the fiber is terminated with a ST connector that has a *screw on* type of locking mechanism. You need to seat the fiber connector and *Stick and Twist* it on. You can remember the type of connector it is from ST - Stick and Twist.

It is one of the most commonly found fiber termination, and it has a BNC type connector look at feel. Keep in mind that you must handle the fibers with great care, as they are quite sensitive and can break very easily.

SC (Standard Connector)

An SC connector is most commonly found on fiber optic cable. SC stands for *standard connector* and is the newer version of the most commonly used fiber connector. The tip of the fiber is terminated with a SC connector that has a *click in* type of locking mechanism. You need to seat the fiber connector and *Stick and Click* it on. You can remember the type of connector it is from SC - Stick and Click.

It, too, is one of the most commonly found fiber termination. It is most commonly seen on equipment such as Cisco GBICs, which are used to connect fiber optics into the switch chassis. It clicks into position when you push it to seat it. Also, just as you must treat ST connectors gently, make certain that you handle SC connectors with care as they are sensitive and can break very easily as well. Again, handle fibers with great care.

IEEE1394 (FireWire)

A very fast external bus standard that supports data transfer rates of up to 400Mbps (in 1394a) and 800Mbps (in 1394b). Products supporting the 1394 standard go under different names, depending on the company. Apple, which originally developed the technology, uses the trademarked name FireWire. Other companies use other names, such as i.link and Lynx, to describe their 1394 products.

A single 1394 port can be used to connect up 63 external devices. In addition to its high speed, 1394 also supports isochronous data which is delivering data at a guaranteed rate. This makes it ideal for devices that need to transfer high levels of data in real-time, such as video devices.

Although extremely fast and flexible, 1394 is also expensive. Like USB, 1394 supports both Plug-and-Play and hot plugging, and also provides power to peripheral devices.

Fiber LC (Local Connector)

An LC connector is most commonly found on fiber optic cable. LC stands for *local connector*. The tip of the fiber is terminated with a LC connector that has a *click in* type of locking mechanism. You need to seat the fiber connector by pushing it in and snapping it on. You can remember the type of connector it is from LC - Lock and Click.

LC connectors were not on the older version of the Network+ exam and making a debut on the 2005 version. Since coverage is new, here are some fundamental factoids.

- LC Connectors are low-loss, high-performance connector types.
- A small-form-factor (SFF) design based on a 1.25-mm ceramic ferrule
- A latching mechanism is used that emulates the use of a RJ-45 modular plug and jack.
- A duplex configuration that offers a high-density fiber-to-fiber pitch
- The lowest insertion loss among SFF connectors at 0.1 dB average
- A high return loss of 55 dB in single mode
- No-polish/no-epoxy versions for fastest application
- Epoxy/polish versions for maximum performance
- Both single-mode (sm) and multimode (mm) product ranges

MTRJ (Mechanical Transfer Registered Jack)

Seen as MTRJ or MT-RJ, this jack is a fiber optical duplex connector like the LC, but it requires zipcord when you make a patchcord and is bulky with the clip that holds two of them together. It looks like two connectors clipped together, not a duplex connector. What should be used is a smaller, neater connector using the new smaller cable designs which would seem more acceptable.

The MT-RJ is a much cleaner, more integrated, even aesthetic design, that can use smaller 1.6 and 2 mm cables, but the ferrule has been the cause of many issues, including creating great difficulty for test equipment manufacturers interfacing to it and users testing them properly.

The MT-RJ is a great design, but with the 2.5 mm ferrules at the chosen spacing, it is only compatible to its own jack, not the SC, FC or ST which use the same ferrule, which was an advantage of the FDDI and ESCON connectors.

USB (Universal Serial Bus)

USB ports are wide spread on today's computers. It is used to connect a great range of devices including mice, keyboards, web cams, and external hard drives. USB standard 1.1 supports data transfers of 12 Mbps whereas USB 2 supports transfer rates of 480 Mbps.

NOTE: LC and MTRJ are new to the Network+ exam; make sure you know the details. All connectors listed in this section of the study guide can be viewed by going to any online search engine and typing in "cable connector resellers", or the connecter type and you will find many sites that have pictures of all the hardware and what they look like. This will do you a great deal of good come test time.

1.5 Recognize the following media types and describe their uses:

In this objective you will be expected to know media types such as Category 5e (Cat5 for short) cable which is very commonly seen and work with as a Network+ certified technician. You will need to recognize certain characteristics about the media to answer questions directly related to them. In this section we cover Cat5 cable, which is most commonly seen, as well as other media types.

Category 3, 5, 5e, and 6

Category type cable comes in many variations. Variations are caused by enhancements, so of course, cabling will evolve with time. Category 3 cable is the minimum level cable you can use with data for instance, no a Fast Ethernet LAN. Category 5 Cable (UTP) (Unshielded Twisted Pair) is a multipair (4 pair) high performance cable that consists of twisted pair conductors that transfer your data. Category 5 UTP cabling systems are by far, the most common (compared to SCTP) in the United States. Basic Cat5 cable was designed for characteristics of up to 100 MHz. Category 5 cable is typically used for Ethernet networks running at 10 or 100 Mbps. Here are some other types of cabling that you will need to know about for the Network+ exam:

Category 5e Cable (enhanced) is the same as Category 5, except that it is made to somewhat more stringent standards. The Category 5 E standard is now officially part of the 568A standard. Category 5e is recommended for all new installations, and was designed for transmission speeds of up to 1 gigabit per second (Gigabit Ethernet).

Category 6 is the same as Category 5e, except that it is made to a higher standard. The Category 6 standard is now officially part of the 568A standard.

Category 7 is the same as Category 6, except that it is made to a higher standard. Category 7 standard is still in the works (as of this writing) and is not yet part of the 568A standard.

UTP (Unshielded Twisted Pair)

UTP essentially means the twisting of the pairs in the cable just mentioned so that the cable gets a certain amount of immunity from the infiltration of unwanted interference.

STP (Shielded Twisted Pair)

STP is nothing more than the Shielded version to keep more interference out. The shield covers the cable jacket housing, as well; there are even RJ-45 connectors that use shielding.

Coaxial cable

Coaxial cable is all different kinds of networks worldwide. Coaxial cable is able to transfer data more efficiently than Twister Pair, but it is generally more difficult to work with and a little more expensive to make.

SMF (Single Mode Fiber) optic cable

In optical fiber technology, single mode fiber is optical fiber designed for the transmission of a single beam of light as a carrier and is used for long-distance signal transmission.

MMF (Multimode Fiber) optic cable

In optical fiber technology, multimode fiber is optical fiber designed to carry multiple light beams concurrently, each at a slightly different reflection angle within the optical fiber core. Multimode fiber transmission is used for relatively short distances because the modes tend to disperse (called modal dispersion) over long distances.

1.6 Identify the purposes, features and functions of the following network components:

In this objective you will be expected to know the following network components and some key features about them. We will cover hubs, switches, routers and firewalls among other things. You should know all these items well enough to distinguish key functionalities between them, such as a hub broadcasts out all ports each time to get data from source to destination. There is no memory, whereas with a switch, a MAC address is kept in memory which is associated by the node plugged into the port. After the initial *flooding* of the switch to learn what is out there, broadcast traffic is kept to a minimum with a switch. It is factoids like this that you need to know and have down cold for the exam.

Hubs

One of the most common connection based network components ever created, hubs are located in homes, offices, buildings and networks almost everywhere. Hubs, (the predecessor of the switch) were based on the Star topology where you have a central concentrator that your nodes connect to and operate from. A hub falls in two categories, passive and active. Active hubs have a plug so that it has an outside power source, passive hubs do not. Active hubs are covered on the Network+ exam. A hub is nothing more than a multiport repeater. Not covered on this version of the exam as a testable objective, it still benefits you to understand what a repeater does so you can understand what a hub does. A repeater is nothing more than a signal amplifier. It does not just amplify (this is actually the wrong terminology), it actually *regenerates* the signal to its original (and strong) form. Because of the distance limitations you learned of in this section of the study guide (such as 10BaseT is limited to 100 meters). After 100 meters, the

signal will degrade. Since it is Baseband technology, the signal is either strong (which is a one), or it is off (and that is a zero). If the signal degrades, ones and zeros (binary math 1s and 0s) can become garbled and that equals corrupted data.

A repeater takes the signal that may be falling short and regenerate it into its former strength. Now that you know what a repeater is, think of a hub as the same things, but with more than two ports, one to bridge up to segments to get more distance out of your LAN. Those days are gone, that equipment is just a memory in most cases, but the technology is essentially the same. It just evolved. Fast forward to the year 2005. We can find a hub or technology that surpasses it in just a great many homes and businesses in the world. Before we talk about switches, where we are today, we need to cover a hub. Hubs are used to connect segments of a LAN, create a LAN for nodes to connect to and participate on. A hub contains multiple ports, usually 4 or more. Most hubs are contained to 24 or 28 ports and anything about that is either modular or stackable.

A hubs operation is simple. When a packet arrives at one port, it is sent to all the other ports on the hub so that all segments of the LAN can see all packets. This is how communication takes place. Hubs do not have memory associated with them so they do not contain any type of MAC or CAM table to use for forwarding of data from one part to another without having to broadcast out all ports to find a destination. This is what a switch does. Sometimes hubs are refereed to as switching hubs if you are talking about a switch. This in my opinion is stupid, just call it a hub or call it a switch. Just remember that there is another term, the switching hub which means it is a switch.

Switches

A switch is the step up from the hub. Operating at faster speeds, some outfitted with ASIC chips to increase speed and efficiency (and a great many other benefits), switches are the way of the future. Switches operate by filtering and forwarding packets between LAN segments or from node to node. Switches operate at the data link layer (layer 2) of the OSI model and sometimes the network layer (layer 3) of the OSI model which means that there is an integrated router function into the switch. These are commonly known as *Layer 3 Switches* because they just do not operate at the Data Link layer, but above it, in the Network layer where routing decision can be made.

Bridges

A Bridge is a device that connects two local-area networks (LANs), or two segments of a LAN in order to segment it because the collision domain is too large. . A Bridge is a an older version of what a switch is. When Hubs were in use primary and Switches did not officially exist, there were Bridges. Rarely seen on today's networks, Bridges served one major purpose. It acted like a switch (it kept a MAC table), but it segmented a LAN that may have been all hubbed and have a large amount of collisions and broadcasts because of such a large area that all nodes must occupy. To make the network smaller, more management, it is wise to segment it by a Bridge.

Bridges are old technology, but the principals are primarily the same as a switch, only a switch has many ports (and other features) whereas a Bridge normally only have 2 ports to segment a large network in half to improve performance.

Routers

Routers move up one layer in the OSI model to the Network layer. On this layer, IP packets are sent to destination networks based on routing decisions made by routers across paths in which they connect and help control. Either via static or dynamic routing decisions, packets are sent from one network segment to another. As a packet enters the router, it is examined, a route is looked up for the destination address

requested and it is either forwarded or ICMP helps you to know why it was not. Either way, understand that a router is nothing more than a traffic cop that takes data in and sends it out to where it is intended to go.

Routers can connect multiple Ethernet LANs, Token Ring, ISDN, Frame Relay, Internet connections to use for Internet access, the media types and connections are almost limitless as routers become more and more modular over time. Routers will use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts as was just mentioned. It is imperative that you understand the fundamental make up of what a router does and how it operates for the Network+ exam.

Gateways

A gateway is a node on a LAN that serves as an entrance (or exit) to another network. When you open up a Command Prompt on Windows 2000 or XP Professional desktop and type in ipconfig, you will see what is called a Default Gateway entry in the output.

NOTE: Windows 9x and Me use winipcfg, Linux uses ifconfig, Windows NT, 2000, 2003, and XP use ipconfig.

Whether in your home or place of work, it is almost certain that you will always have some form of gateway if you ever want to do anything outside the access of that local network. A LAN is contained unto itself; it is only when you add a router to the LAN and give the LAN an exit point (either over the public Internet or over private telecommunication lines used to interconnect business units in a company) that you need a gateway. Most times the gateway is that router's Ethernet port and normally one of the IP addresses configured for that LAN segment is the IP assigned to it that all requests are sent to when no other path is known. If you have a request for a PC with an IP of 10.2.2.10, you may not be able to communicate with that IP if you are not on that specific IP subnet assigned to that LAN. What if your IP range was 10.1.1.0 /24? Then you can see the issue, 10.1.1.0 and 10.2.2.0 will not communicate without a router between them. So, you get a router. You have two Ethernet ports on the router. You configure each router Ethernet port with an IP. Port 1 has 10.2.2.1 and port 2 has 10.1.1.1. You then configure (in this case you most likely do not need to because they are directly connected to each other in the router) a route from each port to the other. Now, when you are on LAN 10.1.1.0 and need to communicate with 10.2.2.0, you know that whatever is not found on the local LAN will go to your default gateway assignment (the router with an Ethernet interface on that LAN assigned with an IP of 10.1.1.1) picks up the packet, knows to send it to the other port 10.2.2.1. Then, that side knows to put it out on the LAN to be picked up by the destination node addressed. This is what a gateway essentially is. Other devices can act as gateways, like Layer 3 switches, Firewalls, Proxy Servers and so on. As long as they perform this basic functionally as I described, then they can be called a gateway as well.

CSU/DSU (Channel Service Unit/Data Service Unit)

Short for Channel Service Unit/Data Service Unit, A CSU/DSU is a device that takes a signal from a telecommunications provider and multiplexes (or channelizes) it. To understand what a CSU/DSU, it is very important to at a minimum understand what a T1 is. See the links section for most of what it is you need to know about a T1, but for a general explanation within what you need to know for the exam, a T1

is a type of WAN based telecommunications technology that is broken into 24 separate channels called DS0s. This is why you may hear that 24 channels were used (at 64K each) to equal a grand total of approximately 1.544 Mbps worth of throughput for a full T1. This way if you needed to order lets say, 128K of bandwidth, you would need 2 channels, instead of ordering a full T1.

The CSU is a device that connects a terminal to a digital line. Typically, the two devices (CSU/DSU - you can think of this as a very high-powered and expensive modem) are packaged as a single unit. The DSU is a device that performs protective and diagnostic functions for a telecommunications line.

Such a device (CSU/DSU) is required for both ends of a T-1 or T-3 connection, and the units at both ends must be set to the same communications standard. As well, other factors also come into play, like signaling methods, protocol encapsulation types and so on. Make sure for the Network+ exam you understand the fundamentals of a T1 and how it operates with a CSU/DSU.

NICs (Network Interface Card)

Network Interface Cards, often called NICs for short, is one of the most commonly used and preferable methods of attaching devices to a network. A NIC is nothing more than an expansion board for your PC that you install to give you access to your local network. If you are on a 100Mbps fast Ethernet LAN, you will need to purchase a card compatible with your LAN requirements. Also, you will need to know what type of LAN you are on; a Token Ring NIC is very different from an Ethernet NIC. Lastly, you will need to know what you are connecting it to, a laptop or PC. ISA slot or PCI? This is one of the reasons why the CompTIA A+ certification was a minor prerequisite for the Network+ certification. If you have a laptop, you will most likely need a PCMCIA card if a NIC is not integrated into your motherboard. Most are set up this way.

Here are some facts you may need to know about NICs for the Network+ exam.

The NIC is manufactured with a unique identifier called a MAC address. Most times, the first half of the MAC address is the *vendor ID* and the second half is the *unique identifier*. Every MAC address on a network needs to be unique because the MAC address is what is resolved via Arp resolution traffic between the nodes. If a duplicate exists, then there is a conflict and a conflict means that one node will not be able to transmit. This is why the NIC has what is called a BIA (Burned in Address) so that each one can be unique. Occasionally, duplicates show up over time, but there are ways to update the card to fix it or just update it because it is obviously very old.

Remember that MAC addresses operate on the Data Link layer of the OSI model, and that they give you access to the network. Also, remember that NICs are expansion cards, but do not concentrate on that fact of it being a card, concentrate on what it does fundamentally, which is to provide a unique identifier to each node on a network. This way they can be accurately located through MAC tables on local switches, arp caches in routers and other nodes and so on. Understanding what it does helps you make the transition from certifications like Network+ to high level certifications like the Cisco CCIE. This way when you start to install network hardware from a vendor such as Cisco, you know that Switches have a MAC associated with them to identify them uniquely on the network for management purposes. What about the default gateway we just talked about? Well, the router's Ethernet port has a MAC associated with it. This means that it is essentially a network interface. The only difference is that it is probably an integrated port of a card. This way when you start to install those T1s just mentioned, you know what a WIC is when you order it – a WAN Interface Card for the router.

ISDN (Integrated Services Digital Network) adapters

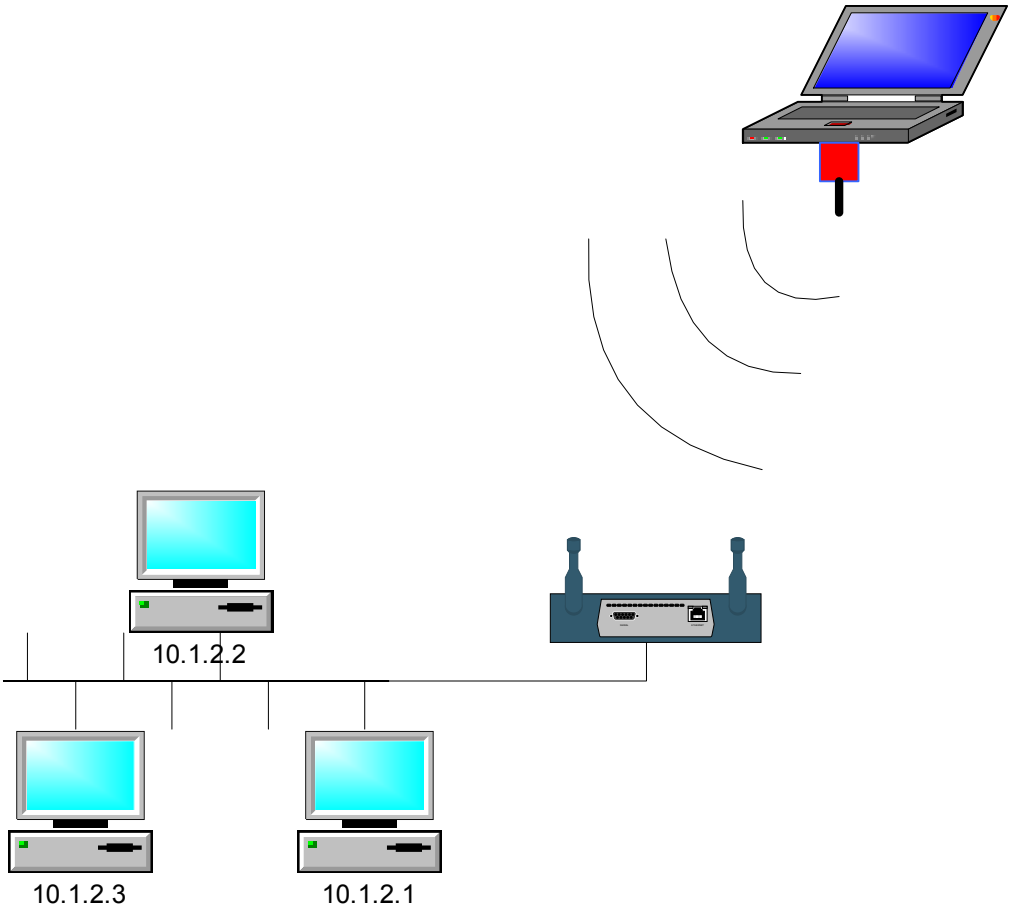
ISDN is the abbreviation of integrated services digital network. ISDN is a Wide Area Network (WAN) based telecommunications technology. We just talked about the CSU/DSU; we had installed a T1 line. Well, lets say we only used a couple of channels (2) and ran pure Digital on it with one extra channel in line to give us control over the session for good reliability, this technology would essentially be the foundations of ISDN.

ISDN, an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires is commonly seen in the corporate office of companies around the world. Mostly used for Wide Area Network links from one company to another, ISDN is unique in that it is *call initiated* and *call terminated*, so you only pay for what you use. ISDN which uses telephone number like entities called SPIDS which means Service Provider ID, to dial from peer to peer to bring up the line when interesting traffic such as some streaming video needs to be sent across it. Once the call is deemed over due to inactively, the call is ended and so is the billing for that usage.

ISDN supports data transfer rates of 64 Kbps (64,000 bits per second). There are two types of ISDN: **Basic Rate Interface (BRI)**, which consists of two 64-Kbps B-channels and one **D-channel** for transmitting control information, and **Primary Rate Interface (PRI)** which consists of 23 B-channels and one D-channel (U.S.) or 30 B-channels and one D-channel (Europe). The B channel is used for control. You can bundle multiple ISDN BRIs or PRIs to expand on your bandwidth usage. It is also worth noting that adapters are defined by which country you are in and what standards are in place.

WAPs (Wireless Access Point)

Short for Wireless Access Point (and abbreviated further by just saying AP or Access Point), an AP is a hardware device that will allow you to associate to it, and access a Wireless network. The goal thereafter is to get to a wired network. As you can see in the next illustration, it is very possible to join a Wired LAN segment as long as an Access Point is connected (and configured properly) so that roaming or mobile users (such as the laptop seen in the graphic) can participate on your network and share resources.



APs are important for providing heightened wireless security and for extending the physical range of service a wireless user. APs have many critical roles they play. Some worth mentioning include that they operate in different modes such as infrastructure mode and ad-hoc mode. Ad hoc would be more of a peer to peer network where devices such as Bluetooth wireless network equipment like keyboards and mice will operate. In 802.11b networks, the Access Point serves as the way into the wired network. That would be infrastructure mode. Ad Hoc would be if two PCs configured their Wireless NICs to Ad hoc mode to share resources together. Access Points should be used in infrastructure mode; this provides the best way to provide control, security, quality enhancements and management tools. Access Points need clients to be associated to them in order to get them on the Wired LAN, and they also have MAC addresses assigned to them.

NOTE: WAP is also short for the Wireless Application Protocol, a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smartphones and communicators. It is scary when the IT industry is almost out of Acronyms that we have to start to share them with other meanings. ☺

Modems

Short for modulator-demodulator. A modem is a device or program that enables a computer to transmit data over communications mediums such as the PSTN. (Public Switched Telephone Network)

Computer information is transmitted in digit and telephone lines send data off over analog waves. There has to be a device that translates one from the other so that connection can be made. A Modem is nothing more than a device that takes a computers digitally formatted information and converts it into whatever the telephone lines expect, an analog wave in this case. Do not get hung up on the fact that modem means –digital to analog translation- because cable based ISPs are selling their converters for your home and calling them modems as well. A cable modem is much the same, it takes your Ethernet link and translates it to the coaxial based technology in which it uses to split your internet access with your TV's movie channels. This is merely another example of a translation from one technology to another. Mo/dem – modulate, demodulate.

Transceivers (media converters)

Short for transmitter-receiver, a transceiver is a hardware device that both transmits and receives analog or digital signals. Also known as a media converter, transceivers are nothing new in the networking world. Most hub, switch and router manufactures used to put an AUI port on most devices so that a transceiver can be mounted to change the technology that was going to be used with the router, switch or hub. A transceiver, if you will, is nothing more than an early attempt at the network vendors to go module. If you needed a router, and it is going to cost a lot of money, it is important to know what the future brings for that router. Is technology creeping up way too fast? If I install a router and I know that 100 Mbps is in this year, but Gigabit Ethernet may be big in the next year, I may want to give myself and opportunity to be able to upgrade that router. This is where interface cards come in. The older method for doing this was with media converters. Media converters allowed a hardware vendor to put a universal port on a device and then sell converters. This allowed you to use a port for multiple things. One of the most commonly seen of these uses was with you have a switch with transceiver added to give it Fiber Optic interfaces. Now that Switch can be used if needed whereas had the port and the transceiver not been an option, the switch would have to be replaced. A good example of when this was very popular was with the now outdated Cisco 2500 router line series that used transceivers to add Ethernet interfaces to the router.

Firewalls

A firewall is a device that controls traffic sent from a source to a destination and either allows it or disallows it based on a rule. A simpler term would be to equate the firewall to a traffic cop. Firewalls perform many roles, many can act as routers, and all firewalls are not created equally:

Packet filters

Packet filters look at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway

This applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

Circuit-level gateway

This applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server
This intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert and today's firewalls can do a lot more like advanced logging, and VPN connection to remote sites through encrypted tunnels.

One mistake many make is thinking s firewall means you are secure. A firewall is only one tool in the arsenal needed to be a security analyst. For more information on this topic visit the links section for information about CompTIA's Security+ program and free material you can use to study for it.

NOTE: Knowing the details of all these devices is essential to taking the Network+ exam.

Knowing that all the devices we just leaned about are converging each and every day is essential to you being a Network+ technician. One good example to drive this fact home is that you can now order Internet access from a provider, go to the store and purchase a Router that also has a 4 port switch, a Wireless Access Point, and a Firewall all in one device under 100 dollars. How can this be? Well, this is the point, everything can function separately or be piled into one box, so make sure you take note of this so you can see the subtle differences in a production network environment. A Router can now switch packets from interface to interface to save time, a Switch can now have a layer 3 component integrated into it so that it can route packets taking the data off the high speed backplane instead of having to go back out on the LAN to see a router, a firewall can route, a router can have a firewall module installed. For the exam, concentrate on that each is separate, but firmly know that the sky is the limit on what a vendor will cram into one box these days.

Also, note that all of these devices actually paint one big picture. The node has a NIC, the NIC connects to a hub or switch, the switch builds up the LAN and the LAN connects to the WAN via the router, the router sends the data to a remote LAN (or website, FTP server) and then the end to end communication takes place. The router may have a T1 link connected, hence the need for the CSU/DSU to multiplex the used channels, you may have a firewall behind the Internet access router for added security.

Lastly, it is imperative that you know this exam is product knowledge neutral so when you see a question relating to this section about routing or switching, knowing Cisco will only help you, not knowing it wont hurt you because vendor specific commands and such will not show up on the exam.

1.7 Specify the general characteristics (For example: carrier speed, frequency, transmission type and topology) of the following wireless technologies:

In this objective you will be expected to know the following about Wireless technologies. You will have to understand 802.11 in a more granular fashion based on the signaling methods used. Infrared and Bluetooth are also covered.

802.11 (Frequency hopping spread spectrum) FHSS

FHSS is the acronym for frequency-hopping spread spectrum. FHSS is one of two types of spread spectrum radio, the other being direct-sequence spread spectrum which is covered next in this study guide.

FHSS is a transmission technology used in LAWN transmissions where the data signal is modulated with a narrowband carrier signal that *hops* in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies.

802.11 (Direct sequence spread spectrum) DSSS

DSSS is the acronym for direct-sequence spread spectrum. DSSS is a transmission technology used in LAWN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio.

Infrared

Infrared is the standard that specifies transmitting data over infrared light waves. The Infrared Data Association (http://www.irda.org/) is a group of device manufacturers that developed a standard for transmitting data via infrared light waves have specified IrDA.

IrDA will enable you to have data transfer from one device to another without any cables. If you have PCs and a Printer all with IrDA ports, you can create a small infrared network at home. IrDA ports support roughly the same transmission rates as traditional parallel ports. One restriction on their use is that the two devices must be within a few feet of each other. Another restriction is that there must be a clear line of sight between the two devices.

Bluetooth

Bluetooth is a short-range radio technology aimed at creating a very easy to set up, small in nature, wireless network. It is normally used for mobile devices sharing a close proximity. Wireless mice and keyboards commonly use Bluetooth. Products with Bluetooth technology must be qualified and pass interoperability testing by the Bluetooth Special Interest Group prior to release. Bluetooth's founding members include Ericsson, IBM, Intel, Nokia and Toshiba.

1.8 Identify factors which affect the range and speed of wireless service (For example: interference, antenna type and environmental factors).

In this objective you will need to know how to assess your Wireless Service. Wireless performance amounts to how well you wireless network is operating. For example, if you experience delays, slowdowns when downloading files or frequent disconnections, you may have to assess your situation. You may have interference from something or you may be using the wrong equipment. Here we will cover factors that you may experience when working with Wireless networks.

When attempting to achieve the best wireless performance you can, you should consider some of the following things.

- Place your base station, gateway, or router near the center of your intended wireless network area to minimize eavesdropping.

- Place wireless components in each others direct line of sight.

- Place wireless components higher to the ceiling to avoid obstacles which will help to achieve better reception.

- Avoid placing wireless components where they can be blocked by large objects.
    - Building components, such as fireplaces, concrete or masonry walls and floors, metal framing, UV film, and metallic paint are all things that will reduce your radio signal strength.

- Metal reduces signal strength. Avoid putting equipment near it.

- Avoid placing wireless components close to electro-magnetic devices, especially those with frequencies in the 2.4-gigahertz (GHz) range (such as cordless phones.)

- Keep in mind that other wireless networks can create interference with each other.

Domain 2.0 - Protocols and Standards

Chapter 2

Protocols and Standards cover all the important items you will need to master to be able to see how networking takes place, how protocols function and why standards are so critical within the networking arena. In this section of the study guide we will cover such technologies to include but not limited to, TCP/IP and ports. This section of the study guide covers 20% of the overall exam.

Exam Objectives Covered:

2.1 Identify a MAC (Media Access Control) address and its parts

2.2 Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions

2.3 Identify the OSI (Open Systems Interconnect) layers at which the following network components operate:

a. Hubs
b. Switches
c. Bridges
d. Routers
e. NICs (Network Interface Card)
f. WAPs (Wireless Access Point)

2.4 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability and naming conventions:

a. IPX/SPX (Internetwork Packet Exchange/Sequence Packet Exchange)
b. NetBEUI (Network Basic Input/Output System Extended User Interface)
c. AppleTalk/AppleTalk over IP (Internet Protocol)
d. TCP/IP (Transmission Control Protocol/Internet Protocol)

2.5 Identify the components and structure of IP (Internet Protocol) addresses (IPv4, IPv6) and the required setting for connections across the Internet.

2.6 Identify classful IP (Internet Protocol) ranges and their subnet masks (For example: Class A, B and C).

2.7 Identify the purpose of subnetting.

2.8 Identify the differences between private and public network addressing schemes.

Quick Jump To:

- Objective 2.1
- Objective 2.2
- Objective 2.3
- Objective 2.4
- Objective 2.5
- Objective 2.6
- Objective 2.7
- Objective 2.8
- Objective 2.9
- Objective 2.10
- Objective 2.11
- Objective 2.12
- Objective 2.13
- Objective 2.14
- Objective 2.15
- Objective 2.16
- Objective 2.17
- Objective 2.18

2.9 Identify and differentiate between the following IP (Internet Protocol) addressing methods:

a. Static
b. Dynamic
c. Self-assigned (APIPA (Automatic Private Internet Protocol Addressing))

2.10 Define the purpose, function and use of the following protocols used in the TCP/IP (Transmission Control Protocol/Internet Protocol) suite:

a. TCP (Transmission Control Protocol)
b. UDP (User Datagram Protocol)
c. FTP (File Transfer Protocol)
d. SFTP (Secure File Transfer Protocol)
e. TFTP (Trivial File Transfer Protocol)
f. SMTP (Simple Mail Transfer Protocol)
g. HTTP (Hypertext Transfer Protocol)
h. HTTPS (Hypertext Transfer Protocol Secure)
i. POP3 (Post Office Protocol version 3)
j. IMAP4 (Internet Message Access Protocol version 4)
k. Telnet
l. SSH (Secure Shell)
m. ICMP (Internet Control Message Protocol)
n. ARP/RARP (Address Resolution Protocol/Reverse Address Resolution Protocol)
o. NTP (Network Time Protocol)
p. NNTP (Network News Transport Protocol)
q. SCP (Secure Copy Protocol)
r. LDAP (Lightweight Directory Access Protocol)
s. IGMP (Internet Group Multicast Protocol)
t. LPR (Line Printer Remote)

2.11 Define the function of TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports.

2.12 Identify the well-known ports associated with the following commonly used services and protocols:

a. 20 FTP (File Transfer Protocol)
b. 21 FTP (File Transfer Protocol)
c. 22 SSH (Secure Shell)
d. 23 Telnet
e. 25 SMTP (Simple Mail Transfer Protocol)
f. 53 DNS (Domain Name Service)
g. 69 TFTP (Trivial File Transfer Protocol)
h. 80 HTTP (Hypertext Transfer Protocol)
i. 110 POP3 (Post Office Protocol version 3)
j. 119 NNTP (Network News Transport Protocol)
k. 123 NTP (Network Time Protocol)
l. 143 IMAP4 (Internet Message Access Protocol version 4)
m. 443 HTTPS (Hypertext Transfer Protocol Secure)

2.13 Identify the purpose of network services and protocols (For example: DNS (Domain Name Service), NAT (Network Address Translation), ICS (Internet Connection Sharing), WINS (Windows Internet Name Service), SNMP (Simple Network Management Protocol), NFS (Network File System), Zeroconf (Zero configuration), SMB (Server Message Block), AFP (Apple File Protocol) and LPD (Line Printer Daemon)).

a. DNS
b. NAT
c. ICS
d. WINS
e. SNMP
f. NFS
g. Zeroconf
h. SMB
i. AFP
j. LPD

2.14 Identify the basic characteristics (For example: speed, capacity and media) of the following WAN (Wide Area Networks) technologies:

a. Packet switching
b. Circuit switching
c. ISDN (Integrated Services Digital Network)
d. FDDI (Fiber Distributed Data Interface)
e. T1 (T Carrier level 1)/E1/J1
f. T3 (T Carrier level 3)/E3/J3
g. OCx (Optical Carrier)
h. X.25

2.15 Identify the basic characteristics of the following internet access technologies:

a. xDSL (Digital Subscriber Line)
b. Broadband Cable (Cable modem)
c. POTS/PSTN (Plain Old Telephone Service/Public Switched Telephone Network)
d. Satellite
e. Wireless

2.16 Define the function of the following remote access protocols and services:

a. RAS (Remote Access Service)
b. PPP (Point-to-Point Protocol)
c. SLIP (Serial Line Internet Protocol)
d. PPPoE (Point-to-Point Protocol over Ethernet)
e. PPTP (Point-to-Point Tunneling Protocol)
f. VPN (Virtual Private Network)
g. RDP (Remote Desktop Protocol)

2.17 Identify the following security protocols and describe their purpose and function:

a. IPSec (Internet Protocol Security)
b. L2TP (Layer 2 Tunneling Protocol)
c. SSL (Secure Sockets Layer)
d. WEP (Wired Equivalent Privacy)
e. WPA (Wi-Fi Protected Access)
f. 802.1x

2.18 Identify authentication protocols (For example: CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol), RADIUS (Remote Authentication Dial-In User Service), Kerberos and EAP (Extensible Authentication Protocol)).

a. CHAP
b. MS-CHAP
c. PAP
d. RADIUS
e. Kerberos
f. EAP

2.1 Identify a MAC (Media Access Control) address and its parts

In this objective you will be expected to know a all the parts that make up a MAC address which is that unique identifier that is burned into a NIC card , as well as a great many other network devices. Understanding this will be very beneficial to you as a network engineer, you use MAC and IP addresses very frequently and understanding it helps you to work with it when you need to.

The easiest way to find your MAC address is to go to a command prompt and type ipconfig /all

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : Shimonski-Rob
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter LOOPBACK:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Microsoft Loopback Adapter
        Physical Address. . . . . . . . . : 00-01-4E-1E-2G-34
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Autoconfiguration IP Address. . . : 169.254.25.129
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

The allocation of MAC addresses, which stands for *Medium Access Control* addresses, is administered by the IEEE in the USA. It is a sublayer of the Data Link layer of the OSI model, and they are used as the source and destination addresses for data packets on a LAN. Keep in mind that every network device in the world has a unique MAC address. Once you see the output, the Physical Address will be shown as seen in the illustration, and this is the systems MAC address.

A MAC address is written as 12 hexadecimal characters (0-9, A-F), with the first 6 characters of the MAC address are unique to the manufacturer of the device. The grouping of those 12 characters into pairs separated by colons (00:20:40:70:F4:84) or hyphens (00-20-40-70-F4-84) is purely conventional, and is not related to function.

NOTE: Windows 9x and ME use winipcfg, Linux uses ifconfig, Windows NT, 2000, 2003, and XP use ipconfig. Win9x/ME: click Start, click Run, enter the command winipcfg. Use the pull-down menu to select the network interface you want and alter as you need.
Windows (any version except Win95): open a command window, type the command ipconfig /all. Look for the output section related to the network interface for the cable modem, and look for the Physical Address

2.2 Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions.

In this objective you will be expected to know the OSI model layers and what they represent.

OSI (Open Systems Interconnection) is a standard description or *reference model* for how messages should be transmitted between any two points in a network. Its purpose is to guide product implementers so that their products will consistently work with other products. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion. If there is common ground, then it is easier to get points across or troubleshoot a problem. It is not uncommon to hear someone say, "Use the OSI model to troubleshoot the problem." If your IP address is configured incorrectly, that is a Network layer issue, if your router has a bad route in its table, which is also a layer 3, it is a network layer issue. Having a cable break is a layer 1 issue. A fiber broken and stopping data flow is a layer 1 problem. A Physical layer problem.

Remember, the main idea in OSI is that the process of communication between two end points in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions. OSI divides networking into seven layers as seen in the illustration.

Layer 7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Layer 7
This is the **application** layer, where quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.

Layer 6
This is the **presentation** (or syntax) layer. At this layer, converting incoming and outgoing data from one presentation format to another occurs. For example, from a text stream into a popup window with the newly arrived text.

Layer 5
This is the **session** layer. At this layer, coordinating, and terminating conversations, exchanging, and dialog between the applications at each end occur. It deals with session and connection coordination.

Layer 4
This is the **transport** layer. At this layer, there is end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer.

Layer 3
This is the **network** layer. At this layer, routing of the data takes place, which is the sending of the data in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level. The network layer does routing and forwarding. IP addressing and dynamic or static routing also take place al this layer.

Layer 2
This is the **data-link** layer. At this layer, MAC address, framing, and switching take place.

Layer 1
This is the **physical** layer. This layer conveys the bit stream through the network at the electrical and mechanical level.

2.3 Identify the OSI (Open Systems Interconnect) layers at which the following network components operate:

In this objective you will be expected to know what device operates at what layer of the OSI model.

Hubs	Physical
Switches	Data Link
Bridges	Data Link
Routers	Network
Network Interface Card	Data Link
Wireless Access Point	Data Link

2.4 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability and naming conventions:

IPX/SPX	(Internetwork Packet Exchange/Sequence Packet Exchange) **Routing:** Static routing and dynamically via IPX Routing Information Protocol (IPX RIP) and NetWare Link-State Protocol (NLSP). **Addressing schemes:** The two parts of an IPX address are network and node. IPX addresses consist of each nodes 12 digit Hex address (MAC address) and its network address. **Interoperability:** IPX/SPX is not interoperable with TCP/IP. Novell operating systems are interoperable with just about any other operating system. Novell strives to champion interoperability. **Naming conventions:** Naming in IPX/SPX revolves around NDS (or eDirectory), which is Novell's flagship directory product. NDS is based on LDAP.

NetBEUI	(Network Basic Input/Output System Extended User Interface) **Routing:** No routing. Not routable. There are ways to get it encapsulated to be routed, but in general, it as a protocol, does not have its own power to route. **Addressing schemes:** Naming in NetBEUI is based on broadcasting and there is no addressing scheme that can be used. NetBEUI is a very simple protocol without a lot of overhead; it just does not have the scalability of a protocol like TCP/IP. **Interoperability:** NetBEUI is interoperable in the form of NetBIOS. NetBIOS, which can also be seen as SMB, CIFS and useable via Unix based systems utilizing NFS is actually very interoperable. Nobody really uses NetBEUI anymore, even small home networks these days utilize TCP/IP so that they can quickly access the Internet, most have gained the savvy of using an IP address, now protocols like NetBEUI, which were essentially meant to be for plug and play networks, are outdated. It is still important to know since most of the protocol (NetBIOS) is still very much in use today with Microsoft technologies in particular, so it is imperative that you start to learn the fundamentals of it for the Network+ exam. **Naming conventions:** Naming in NetBEUI is based on broadcasting. An example can be: Names are broadcast to each other, in a small peer to peer network; you can see this via Network Neighborhood.
AppleTalk	AppleTalk over IP (Internet Protocol) **Routing:** AppleTalk, a protocol suite developed by Apple Computer, was developed in conjunction with the Macintosh computer. AppleTalk's purpose was to allow multiple users to share resources, such as files and printers. Cisco Systems AppleTalk Routing is done at layer 3. Routing Table Maintenance Protocol (RTMP) is the layer 3 routing protocol that can be used. **Addressing schemes:** 24 bit addresses, 16 used for the network ID. **Interoperability:** AppleTalk can be support by other systems like Microsoft Windows, but additional software may need to be added. **Naming conventions:**
TCP/IP	(Transmission Control Protocol/Internet Protocol) **Routing:** Statically and Dynamically via many routing protocol options, a few in particular are OSPF, BGP, RIP and IS-IS. **Addressing schemes:** uses an IP address, such as 10.1.1.1 **Interoperability:** TCP/IP is universal and therefore, pretty much interoperable with anything. The only noticeable things that it is not interoperable with would be technologies where a gateway would be needed, like SNA (Systems Network Architecture), which is normally operated via an IBM mainframe. **Naming conventions:** DNS (Domain Name System) is the lifeline of the Internet; this is how TCP/IP hosts can communicate via name.

2.5 Identify the components and structure of IP (Internet Protocol) addresses (IPv4, IPv6) and the required setting for connections across the Internet.

Humans minds do not work too well with binary numbers used this way, because they are long and complicated, hard to read and remember, and the use of only two digits makes them hard to differentiate. What is easier to remember?

11100011010100101001100110110001 or 10.1.1.1

Decimal based IP addresses are used so we do not work within binary except when absolutely necessary.

IPv4 (IP version 4) IP addresses are structured as follows. An IP address is just a 32-bit binary number: made up of 32 alternating ones or zeroes. At the lowest levels computers always work in binary and this also applies to networking hardware and software. When referring to the IP address, we use dotted-decimal notation.

IP addresses contain two components which is the network identifier and the host identifier. In regards to the Network Identifier (Network ID), a certain number of bits, starting from the left-most bit, is used to identify the network where the host or other network interface is located. This is also sometimes called the network prefix or even just the prefix. In regards to the Host Identifier (Host ID), the remainder of the bits are used to identify the host on the network.

By convention, IP devices are often called hosts for simplicity, as I do throughout this Guide. Even though each host usually has a single IP address, remember that IP addresses are strictly associated with network-layer network interfaces, not physical devices, and a device may therefore have more than one IP address.

As defined in RFC 1884 and later revised in RFC 2373, IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces, not nodes. Three general types of addresses exist IPv6 (IP version 6) which is Unicast, Anycast and Multicast. IP addresses are structured as follows:

- Expanded addressing moves us from 32-bit address to a 128-bit addressing method
- Provides newer Unicast and broadcasting methods
- Hexadecimal fused into the IP address format
- Use ":" instead of "." as delimiters

To write 128-bit addresses so that they are more readable to human eyes and not a complete chore to apply, IPv6 allows for using a hexadecimal format. IPv6 is written as 32-hex digits, with colons (**:**) separating the values of the eight 16-bit pieces of the address.

- Example:
  - **7060:0000:0000:0000:0006:0600:100D:315B**

- Leading 0s in each 16-bit value can be omitted, so this address can be expressed as follows:
  - **7060:0:0:0:6:600:100D:315B**

- IPv6 addresses may contain consecutive 16-bit values of 0, one such string of 0s per address can be omitted and replaced by a "**::**". As a result, this address can be shortened even more:
  - **7060::6:600:100D:315B**

2.6 Identify classful IP (Internet Protocol) ranges and their subnet masks (For example: Class A, B and C).

Class	Range
A	1-126 (127 reserved for loopback) **255**.0.0.0
B	128-191 **255**.**255**.0.0
C	192-223 **255**.**255**.**255**.0

2.7 Identify the purpose of subnetting.

In this objective you will be expected to know the purpose of Subnetting. Subnetting is used to conserve address space. A subnet is a part of a network that shares a common address component such as 10.1.1.0. If you had a node on this network, you may be 10.1.1.10, a node on the 10.1.1.0 network. So how do you really know where the network portion of 10.1.1.0 starts and where it begins? Is this a default Class A address because it is in the class A range? A Subnet mask is needed to denote where the host address starts and where the Network address starts. With an address of 10.1.1.10, if the subnet mask is not defined, it would default to 255.0.0.0. In this case, we can say that the subnet mask for the 10.1.1.0 is 255.255.255.0. This would mean that it be 24 bits for the mask denoting the network address, that leaves 8 bits for the host.

The Subnet Mask is important to understand. Doing an ipconfig (or ifconfig /winipcfg) will show you the subnet mask:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter LOOPBACK:
      Autoconfiguration IP Address. . . : 169.254.25.129
      Subnet Mask . . . . . . . . . . . : 255.255.0.0
```

2.8 Identify the differences between private and public network addressing schemes.

In this objective you will be expected to know the difference between public and private addressing. Private IP addressing is blocks of IP addresses reserved for use ONLY internal to the companies that do not want to advertise on the Internet. The private blocks can then be NAT'd to another public range to get on the Internet. This can conserve address space because you can have about 5-10 public IPs to access the Internet with, but have 150 clients that need to view it. Proxy servers serve well here in this scenario. One IP address can be used and the server proxy for the requester behind the proxy server. This is just an example.

These private blocks are reserved as private address space, specified in the RFC 1918. This means everybody can set up an internal network using addresses in these blocks, but packets originating from those addresses should never appear on the internet and most likely will never be routed if you attempt to do so.

These blocks are viewable on the following websites:

http://www.arin.net/

http://www.iana.org/

For quick reference, here they are:

Class	***Private* Range**
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Class	***Public* Range**
A	1-126 (127 **privately** reserved for loopback) **255**.0.0.0
B	128-191 **255.255**.0.0
C	192-223 **255.255.255**.0

2.9 Identify and differentiate between the following IP (Internet Protocol) addressing methods:

In this objective you will be expected to know the difference between assigning an IP address, having one assigned to you dynamically via DHCP or dynamically self assigned via APIPA.

Static

Statically assigned IP addresses are assigned to hosts manually. This is not the best way to do it as you have to keep a manual database of what is given out and so on. This can lead to anarchy once the database grows out of hand or does not get updated often.

Dynamic

Dynamically assigned IP addresses are normally assigned via a DHCP (Dynamic Host Configuration Protocol) server that holds a range of IP addresses assignable to hosts who request them. Once requested, that IP address is marked as in use and that node is given that address to use on a leased period. The database is kept right on the server which makes keeping the database manageable.

Self-assigned (APIPA (Automatic Private Internet Protocol Addressing))

Self assigned IP addresses are found on Windows-based computers (ME, 2000, XP) that are configured to use DHCP can automatically assign itself an Internet Protocol (IP) address if a DHCP server is not available. The Internet Assigned Numbers Authority (IANA) has reserved 169.254.0.0-169.254.255.255 for Automatic Private IP Addressing. As a result, APIPA provides an address that is guaranteed not to conflict with routable addresses.

The Subnet Mask is important to understand. Doing an ipconfig (or ifconfig /winipcfg) will show you the APIPA setting:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter LOOPBACK:
      Autoconfiguration IP Address. . . : 169.254.25.129
      Subnet Mask . . . . . . . . . . . : 255.255.0.0
```

2.10 Define the purpose, function and use of the following protocols used in the TCP/IP (Transmission Control Protocol/Internet Protocol) suite:

In this objective you will be expected to know the basics and fundamental functionality of the following TCP/IP protocols:

TCP (Transmission Control Protocol)	TCP is a transport layer protocol that operates host to host. A connection is established, it is maintained and then TCP ensures the following: Reliable data transfer, sequencing, connection oriented, has a large header because of all this extra overhead, TCP is slower than UDP.
UDP (User Datagram Protocol)	UDP is also a transport layer protocol that operates host to host. A connection is established, it is maintained and then UDP ensures nothing. Since it is only about 20 bytes, you wont have reliable data transfer, sequencing, and it is connectionless.
FTP (File Transfer Protocol)	FTP is used to transfer files. The protocol is optimized to do so. With commands like get, mget, put and mput, options to change files into binary format, or others, FTP is made to transfer files.
SFTP (Secure File Transfer Protocol)	This is the encrypted form of FTP. FTP is an unsecure protocol because it does not contain the overhead to protect itself. That mens if you send credentials to an FTP server to log in, the authentication attempt can be grabbed off the wire and used against you because the credentials are sent in cleartext and easily read. SFTP protects against data theft, manipulation or any other attack that exploits the inherent weaknesses of FTP.
TFTP (Trivial File Transfer Protocol)	FTP has a lot of overhead to transfer files, but what if you wanted a protocol that quickly transferred files without the need for the overhead? TFTP is one such protocol.
SMTP (Simple Mail Transfer Protocol)	SMTP is the lifeblood of email across the world. SMTP is the email protocol that ensures that email data is transferred from server to server and from clients to servers.
POP3 (Post Office Protocol version 3)	POP3 is a scaled down protocol that allows you to use a thin email client and access your email quickly, it has less overhead than SMTP. Commonly used with ISP accounts and remote user accounts in production networks.

IMAP4 (Internet Message Access Protocol version 4)	IMAP4 is a scaled up version of POP3 with more functionality then POP3. The links section of the study guide contains explicit differences between IMAP4 and POP3, it is not needed for the exam, but worth the quick read to understand the functionality of the protocol.
HTTP (Hypertext Transfer Protocol)	HTTP is the key protocol used on the World Wide Web today. HTTP is the protocol used to deliver HTML pages to you in a web browser and the protocol used to deliver web pages to your web clients.
HTTPS (Hypertext Transfer Protocol Secure)	HTTPS is the secure version of this protocol because just like FTP, HTTP suffers from inherent weaknesses.
Telnet	Telnet is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This gives you remote management ability to be able to configure Unix servers, Routers, switches or anything else that allows remote management via Telnet.
SSH (Secure Shell)	Just like HTTP and FTP, Telnet is also unsecure. SSH, or Secure Shell is encrypted Telnet.
ICMP (Internet Control Message Protocol)	ICMP is short for Internet Control Message Protocol, which is an extension to the Internet Protocol (IP) defined by RFC 792. When working on a network, it is important to be able to test the functionality of that network. How would you know if data could be transmitted without knowing you have a complete path from the source to the destination? That being said, how could you test that path? ICMP allows you to test the path (among other things). Ping and Traceroute are two tools that can be used to test a path and they both use ICMP. ICMP packets will be able to help send information about errors, control, and other informational messages.
ARP (Address Resolution Protocol)	Arp is a network layer protocol used to convert an IP address into a physical address (called a MAC address as we covered in this study guide). A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

RARP (Reverse Address Resolution Protocol)	As there is ARP, there is also Reverse ARP (RARP) which can be used by a node on the network to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.
NTP (Network Time Protocol)	NTP is a very important protocol used to transfer time-related information back and forth between users of NTP. Time is important when you have a bunch of Windows 2003 Domain Controllers, or a NetWare 6 eDirectory that needs to keep in synchronization so that corruption is not a result. This is but one of many reasons why NTP is so important to know about.
NNTP (Network News Transport Protocol)	NNTP is used to post, distribute, and retrieve USENET messages on the WWW. The official specification is found in RFC 977.
SCP (Secure Copy Protocol)	SCP is a protocol that will allow you to transfer files between hosts securely using SSH. The protocol is an encrypted version of the old Unix rcp command.
LDAP (Lightweight Directory Access Protocol)	LDAP is a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP.
IGMP (Internet Group Multicast Protocol)	IGMP is defined in RFC 1112 as the standard for IP multicasting. IGMP will establish host memberships in particular multicast groups on a single network.
LPR (Line Printer Remote)	LPR is a printer protocol that uses TCP/IP to establish connections between printers and workstations on a network. The technology was developed originally for UNIX and has since become the de facto cross-platform printing protocol.

NOTE: You should really spend some time with a good TCP/IP book and learn all the fundamentals of what each protocol does to ensure that you know what each of these protocols fundamentally do. It is impossible to cover everything in the TCP/IP protocol suite in a few pages, there are 1000 page books on the subject. The Network+ test wont get that in depth, but as a network technician, engineer or analyst, it is imperative that you understand TCP/IP on a more intimate level.

2.11 Define the function of TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports.

In this objective you will be expected to know how TCP and UDP ports function. Transport Control Protocol (TCP), User Datagram Protocol (UDP) ports, and Protocol Numbers are important to TCP/IP networking, how networking takes place, especially when it comes to Internet access and firewall usage.

Ports and protocol numbers provide access to host computers. However, they also create a security hazard by allowing uninvited access. Therefore, knowing which port to allow or disable increases a network's security. You can allow or disallow certain traffic to pass a firewall (or ACL – access control list) based on a port number so if you did not want Telnet through a firewall, you can block that port which would be TCP 23. If the wrong ports or protocol numbers are disabled on a firewall, router, or proxy server as a security measure, essential services might become unavailable. As well, understand that port numbers are duplicated from TCP to UDP. You will have TCP and UDP ports 23, but because Telnet is a program that requires more overhead than TFTP, it will require the usage of TCP, so it is TCP 23, whereas, TFTP would be UDP 69. You will only need to memorize the ports for the exam, but you should understand how the ports are laid out nonetheless.

2.12 Identify the well-known ports associated with the following commonly used services and protocols:

In this objective you will be expected to know which protocols map to which specific well known port assignment number. A full assignment list can be found at iana.org

Protocol	Port
FTP (File Transfer Protocol)	20
FTP (File Transfer Protocol)	21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name Service)	53
TFTP (Trivial File Transfer Protocol)	69
HTTP (Hypertext Transfer Protocol)	80
POP3 (Post Office Protocol version 3)	110
NNTP (Network News Transport Protocol)	119
NTP (Network Time Protocol)	123
IMAP4 (Internet Message Access Protocol version 4)	143
HTTPS (Hypertext Transfer Protocol Secure)	443

To view a database of all ports, click here

2.13 Identify the purpose of network services and protocols (For example: DNS (Domain Name System), NAT (Network Address Translation), ICS (Internet Connection Sharing), WINS (Windows Internet Name Service), SNMP (Simple Network Management Protocol), NFS (Network File System), Zeroconf (Zero configuration), SMB (Server Message Block), AFP (Apple File Protocol) and LPD (Line Printer Daemon)).

DNS (Domain Name System)	DNS is the TCP/IP based service that translates domain names into IP addresses. The domain name www.rsnetworks.net might translate to 12.1.1.1.
NAT (Network Address Translation)	NAT is used to translate one set of IP addresses for internal traffic into a second set of addresses for external traffic. This is the most fundamental usage of it today. Firewalls perform NAT services to connect you to the Internet. NAT serves two main purposes which is to hide internal IP addressing and allow for more usage of public IP address space.
ICS (Internet Connection Sharing)	ICS is a method used for connecting multiple computers in a LAN to the Internet through a single connection and a single IP address. ICS typically uses NAT technologies to achieve this and works with most connection technologies, including DSL, cable, ISDN, dial-up and satellite.
WINS (Windows Internet Name Service)	WINS is a system that determines the IP address associated with a particular network computer based on its computer name or NetBIOS name. This is called NetBIOS name resolution.
SNMP (Simple Network Management Protocol)	SNMP is a set of protocols for managing networks. SNMP works by sending messages, called protocol data units (PDUs), SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. Management system that can be deployed to help you manage your network or system use SNMP.
NFS (Network File System)	NFS is a client/server application designed by Sun Microsystems that allows all network users to access shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of TCP/IP.
Zeroconf (Zero configuration)	Zero configuration IP networking is a method of networking devices via an Ethernet cable without requiring configuration and administration. Zeroconf is able to allocate addresses without a DHCP server, translate between domain names and IP addresses without a DNS server, and find services, such as a printer, without a directory service. This is meant to be used in small networks.

SMB (Server Message Block)	SMB is a message format used Windows (and other operating system) to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. SMB is now in its better form known as CIFS, which stands for the Common Internet File System
AFP (Apple File Protocol)	AFP is the client/server file sharing protocol used in an AppleTalk network. A non-Apple network can only access data from an AppleShare file server by first translating into the AFP language.
LPD (Line Printer Daemon)	Used in conjunction with LPR, The LPD software typically is stored in the printer or print server and the LPR software must be installed in the client device. The LPR client sends the print request to the IP address of the LPD printer/server, which in turn queues the file and prints it when the printer becomes available.

2.14 Identify the basic characteristics (For example: speed, capacity and media) of the following WAN (Wide Area Networks) technologies:

In this objective you will be expected to know the specifics of the following WAN protocols: ISDN, T1s, E1s and X.25. You will also need to understand the basic characteristics of specific WAN technologies such as how packet switch and circuit switching differ.

Packet and Circuit switching

Most WAN protocols in use today are packet switched. What does this mean? It means that for technologies such as X.25, and Frame Relay the packets are sent across links that are always available. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties and the circuit is brought up when needed. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it is sent. Packet switching is more efficient and robust for data that can withstand some delays in transmission. Delays in transmission will not overly harm applications like email which are asynchronous in their transmission method.

ISDN (Integrated Services Digital Network)

ISDN is the abbreviation of integrated services digital network. ISDN is a Wide Area Network (WAN) based telecommunications technology. We just talked about the CSU/DSU; we had installed a T1 line. Well, lets say we only used a couple of channels (2) and ran pure Digital on it with one extra channel in line to give us control over the session for good reliability, this technology would essentially be the foundations of ISDN.

ISDN, an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires is commonly seen in the corporate office of companies around the world. Mostly used for Wide Area Network links from one company to another, ISDN is unique in that it is call initiated and call terminated so you only pay for what you use. ISDN which uses telephone number like entities called SPIDS, which means Service Provider ID, to dial from peer to peer to bring up the line when interesting traffic such as some streaming video needs to be sent across it. Once the call is deemed over due to inactively, the call is ended and so is the billing for that usage.

ISDN supports data transfer rates of 64 Kbps (64,000 bits per second). There are two types of ISDN: **Basic Rate Interface (BRI)**, which consists of two 64-Kbps B-channels and one **D-channel** for transmitting control information, and **Primary Rate Interface (PRI)** which consists of 23 B-channels and one D-channel (U.S.) or 30 B-channels and one D-channel (Europe). The B channel is used for control. You can bundle multiple ISDN BRIs or PRIs to expand on your bandwidth usage.

FDDI (Fiber Distributed Data Interface)

FDDI is the abbreviation of *Fiber Distributed Data Interface*, a set of ANSI protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and they support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for wide-area networks

T1 (T Carrier level 1)/E1/J1, T3 (T Carrier level 3)/E3/J3

You need to memorize the following telecommunications standards:

A T1 is a dedicated phone connection supporting data rates of 1.544Mbits per second. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbits per second. Each 64Kbit/second channel can be configured to carry voice or data traffic. Most telephone companies allow you to buy just some of these individual channels, known as fractional T-1 access.
An E1 is the European equivalent. An E1 is similar to the North American T-1, E1 is the European format for digital transmission. E1 carries signals at 2 Mbps (32 channels at 64Kbps, with 2 channels reserved for signaling and controlling), versus the T1, which carries signals at 1.544 Mbps (24 channels at 64Kbps).
A T3 is a dedicated phone connection supporting data rates of about 43 Mbps. A T-3 line actually consists of 672 individual channels, each of which supports 64 Kbps. T-3 lines are used mainly by Internet Service Providers (ISPs) connecting to the Internet backbone.
An E3 is the European equivalent. Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps.
J1 and J3 (as well as others) are the Japanese versions of the T Carrier system of North America. The chart below shows the most commonly seen: J1: 24 channels, 1.544 Mbps J2: 96 channels, 6.312 Mbps J3: 480 channels, 32.064 Mbps J4: 1440 channels, 97.728 Mbps J5: 5760 channels, 400.352 Mbps

OCx (Optical Carrier)

Synchronous Optical Network (SONET) includes a set of signal rate multiples for transmitting digital signals on optical fiber.

The base rate (OC-1) is 51.84 Mbps. You need to know the basics of Optical Carrier speeds for the Network+ exam.

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

X.25

X.25 was a popular standard for packet-switching networks but new installations are few and far between these days. The fact that there are sites that still utilize this technology out there is why you must still be familiar with its standards. The X.25 standard was approved by the CCITT (now the ITU) in 1976. It sites on layers 1, 2, and 3 of the OSI Model.

2.15 Identify the basic characteristics of the following internet access technologies:

xDSL (Digital Subscriber Line)	Refers collectively to all types of digital subscriber lines, the two main categories being ADSL and SDSL. Two other types of xDSL technologies are High-data-rate DSL (HDSL) and Very high DSL (VDSL). DSL technologies use sophisticated modulation schemes to pack data onto copper wires.
Broadband Cable (Cable modem)	A modem designed to operate over cable TV lines. Because the coaxial cable used by cable TV provides much greater bandwidth than telephone lines, a cable modem can be used to achieve extremely fast access to the World Wide Web.
POTS/PSTN (Plain Old Telephone Service/Public Switched Telephone Network)	Short for *Public Switched Telephone Network*, which refers to the international telephone system based on copper wires carrying analog voice data. Telephone service carried by the PSTN is often called plain old telephone service (POTS). Short for plain old telephone service, which refers to the standard telephone service that most homes use.
Wireless	Wireless ISPs (WISPs) are known to provide intent access from anywhere where the WISP has coverage. Many locations that have very little access to a good last mile source utilize this technology to connect up to the Internet. Homes also use this very often to get Internet access.
Satellite	Satellite dishes are also starting to gain popularity. Satellite dishes that give access to the Internet via a service provider offer Internet access without having to run the providers line into your home or business.

2.16 Define the function of the following remote access protocols and services:

RAS (Remote Access Service)	The *Remote Access Service* is a feature built into Windows (and other NOSs) that enables users to log into an LAN using a modem, or WAN link. RAS works with several major network protocols, including TCP/IP.
PPP (Point-to-Point Protocol)	Short for *Point-to-Point Protocol*, a protocol used to encapsulate data for transmission. PPP is more stable than the older SLIP protocol and provides error checking features. Working in the data link layer of the OSI model, PPP sends the computer's TCP/IP packets to a server that puts them onto the Internet. PPP will operate with
SLIP (Serial Line Internet Protocol)	Short for *Serial Line Internet Protocol*, a protocol used to encapsulate data for transmission. Developed long ago, SLIP is rarely used now that PPP is used. SLIP only works with IP, whereas PPP uses other protocols within its own suite to handle IPX/SPX for example.
PPPoE (Point-to-Point Protocol over Ethernet)	Acronym for *Point-to-Point Protocol over Ethernet*. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DLS or cable modem.
PPTP (Point-to-Point Tunneling Protocol)	Short for *Point-to-Point Tunneling Protocol*, this is a new technology for creating Virtual Private Networks (VPNs), developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies.
VPN (Virtual Private Network)	VPNs are used to connect sites or users over insecure public connections (such as the Internet) with encryption which creates a virtual *tunnel.* This tunnel is used to transmit data securely, hence, a *virtual and private* network.
RDP (Remote Desktop Protocol)	The *Remote Desktop Protocol* (RDP) is a presentation layer protocol that allows a Windows-based system to communicate with another Windows based system remotely. RDP allows you to connect to a client computer and display as well as to input data.

2.17 Identify the following security protocols and describe their purpose and function:

IPSec (IP Security)	Short for *IP Security*, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs). IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched.
L2TP (Layer 2 Tunneling Protocol)	L2TP is an extension to the PPP protocol that enables the operation of Virtual Private Networks (VPNs). L2TP merges the best features of two other tunneling protocols which is PPTP from Microsoft and L2F from Cisco.
SSL (Secure Sockets Layer)	SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection.
WEP (Wired Equivalent Privacy)	WEP is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN, hence why they call it "Wired Equivalent".
WPA (Wi-Fi Protected Access)	Short for *Wi-Fi Protected Access*, a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP.
802.1x	The IEEE 802.1x standard is simply a standard for passing EAP over a wired or wireless LAN. With 802.1x, you package EAP messages in Ethernet frames and do not use PPP.

2.18 Identify authentication protocols (For example: CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol), RADIUS (Remote Authentication Dial-In User Service), Kerberos and EAP (Extensible Authentication Protocol)).

CHAP	Short for *Challenge Handshake Authentication Protocol*, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated. By transmitting only the hash, the secret cannot be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks. Contrast with PAP.

MS-CHAP	MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Support of this authentication method on Cisco routers will enable users of the Microsoft Windows 2000 operating system to establish remote PPP sessions without needing to first configure an authentication method on the client. MSCHAP V2 authentication introduces an additional feature not available with MSCHAP V1 or standard CHAP authentication, the change password feature. This feature allows the client to change the account password if the RADIUS server reports that the password has expired.
PAP	Short for *Password Authentication Protocol*, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP. The main weakness of PAP is that both the username and password are transmitted in the clear -- that is, in an unencrypted form. Contrast with CHAP.
RADIUS	Short for *Remote Authentication Dial-In User Service*, 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. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.
Kerberos	An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.
EAP	Short for *Extensible Authentication Protocol*, an extension to PPP, EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

Chapter 3

Domain 3.0 - Network Implementation

Quick Jump To:

- Objective 3.1
- Objective 3.2
- Objective 3.3
- Objective 3.4
- Objective 3.5
- Objective 3.6
- Objective 3.7
- Objective 3.8
- Objective 3.9
- Objective 3.10
- Objective 3.11
- Objective 3.12

Network Implementation is covered in this section of the study guide. In this section of the study guide we will cover such technologies to include but not limited to, server based operating systems, backups, fault tolerance and encryption. This section of the study guide covers 25% of the overall exam.

Exam Objectives Covered:

3.1 Identify the basic capabilities (For example: client support, interoperability, authentication, file and print services, application support and security) of the following server operating systems to access network resources:

a. UNIX/Linux/Mac OS X Server
b. Netware
c. Windows
d. Appleshare IP (Internet Protocol)

3.2 Identify the basic capabilities needed for client workstations to connect to and use network resources (For example: media, network protocols and peer and server services).

3.3 Identify the appropriate tool for a given wiring task (For example: wire crimper, media tester/certifier, punch down tool or tone generator).

3.4 Given a remote connectivity scenario comprised of a protocol, an authentication scheme, and physical connectivity, configures the connection. Includes connection to the following servers:

a. UNIX/Linux/Mac OS X Server
b. Netware
c. Windows
d. Appleshare IP (Internet Protocol)

3.5 Identify the purpose, benefits and characteristics of using a firewall.

3.6 Identify the purpose, benefits and characteristics of using a proxy service.

3.7 Given a connectivity scenario determine the impact on network functionality of a particular security implementation (For example: port blocking/filtering, authentication and encryption).

3.8 Identify the main characteristics of VLANs (Virtual Local Area Networks).

3.9 Identify the main characteristics and purpose of extranets and intranets.

3.10 Identify the purpose, benefits and characteristics of using antivirus software.

3.11 Identify the purpose and characteristics of fault tolerance:

a. Power
b. Link redundancy
c. Storage
d. Services

3.12 Identify the purpose and characteristics of disaster recovery:

a. Backup/restore
b. Offsite storage
c. Hot and cold spares
d. Hot, warm and cold sites

3.1 Identify the basic capabilities (For example: client support, interoperability, authentication, file and print services, application support and security) of the following server operating systems to access network resources:

Server OS Type	Services
UNIX/Linux/Mac OS X Server	Can provide Client Support, Interoperability with other systems and protocols, Authentication, File and Print Services, application Support and Security. Most Unix systems always had this functionality. MAC OS X just recently became Unix based, so it has the same features as listed above.
NetWare	Can provide Client Support, Interoperability with other systems and protocols, Authentication, File and Print Services, application Support and Security. NetWare (now up to Version 6) has always been the leading Network Operating System vendor with the best Directory system every created. (Known as NDS and now as eDirectory). The directory system is responsible for most of the features outlined above.
Windows	Can provide Client Support, Interoperability with other systems and protocols, Authentication, File and Print Services, application Support and Security.

3.2 Identify the basic capabilities needed for client workstations to connect to and use network resources (For example: media, network protocols and peer and server services).

To connect to a network you need the following:

- Two or more nodes are needed to create a network. Those nodes need to have NICs to interface to the network with. Wireless, Wired, whatever, but they need a NIC. This also means that obviously will have a MAC address if they have a NIC, it should also mean that those MAC addresses are unique as well.

- Media is needed between those nodes. Cable or Wireless can be used. You can use any topology between them, any form of media, but there must be a connection and it must be configured correctly.

- A Network protocol must be used to communicate. Either TCP/IP, IPX/SPX, whatever, a protocol must be used and the nodes that want to communicate need to have the same ones configured. Let's say TCP/IP is used, that means that all nodes will need a unique IP address to identify them on the network. Using ARP, the IP and MAC addresses are brought together to form the basics of networking.

- A network resource should be available. Honestly, if you are not sharing a printer, Internet access or a set of folders, then why go through all the problems needed to create a network? A network's sole existence revolves around the sharing of resources.

3.3 Identify the appropriate tool for a given wiring task (For example: wire crimper, media tester/certifier, punch down tool or tone generator).

In this objective you will be expected to know how to perform a basic wiring task with commonly used tools.

Wire crimper

A wire crimper is used when creating cables for a wiring job. If you need to create a cable (a Cat5 UTP for instance), then you would need to cut the cable to length, untwist the wires at the end without removing too much of the twist at the base where you then insert the exposed copper cable ends into a blank RJ-45 terminator and then you have to crimp the RJ-45 connector so that copper insulators are kept locked into the RJ-45 connector. A cable crimper is used to do this and searching online can show you many tools used to perform this task.

Media tester/certifier

A Media tester is used to certify a run. What this means is if you run a home run or some other length of cable, you will need to make sure of a few things. Attenuation, Crosstalk, Cable Breaks, no signal, etc can all be issues that you experience when running cable. How can you be sure that you ran it properly? With a Media tester which can be used for copper and fiber cabling runs. A Media tester/certifier is used to do this and searching online can show you many tools used to perform this task.

Punch down tool

A punch down tool is used to push exposed copper cabling into a punch down block, which is usually a 66 or 110 block used to terminate phone lines. In data closets, punch down tools help to punch copper Cat5 into patch panels. A Punch down tool is used to do this and searching online can show you many tools used to perform this task.

Tone generator

A tone generator can be used. Do not use a tone generator on a live network without first asking, it may cause damage. Its sole purpose is to find breaks in a cable. A Tone generator is used to do this and searching online can show you many tools used to perform this task.

3.4 Given a remote connectivity scenario comprised of a protocol, an authentication scheme, and physical connectivity, configure the connection. Includes connection to the following servers:

Virtual Private Networks for Windows Server 2003

Novell NetWare 6.x Documentation Set

Building Linux VPNs (and Sample Chapter) Search online for your specific distro of Linux or Unix to find what you need.

3.5 Identify the purpose, benefits and characteristics of using a firewall.

A firewall is used to protect one network from another. It is used to separate and control network segments and the traffic that traverses them. A firewall was explained earlier in this study guide, but for a rehash, make sure you understand exactly what a firewall does so that you can differentiate it from other Infrastructure devices and know what it normally protects, like Internet access or your companies (or home's) perimeter which is normally either the Internet or link to a company that is not part of your internal network scheme that may need to be NAT'd, secured or whatever else.

3.6 Identify the purpose, benefits and characteristics of using a proxy service.

A Proxy Server is used to protect one network from another, but operates a little differently - than a Firewall. The main reason a firewall exists is to secure whatever it is configured to secure. A Proxy has a different main reason for existence and that is for improved Performance. Proxy servers can dramatically improve performance for groups of users because it saves the results of all requests on websites for a certain amount of time making it easier on the network when data must be pulled from the requested websites back to the corporate office. If you have 900 people and half of them access www.cnn.com for news in the morning, it is common to use a proxy server so that the first time the home page is requested, it is cached on the server. Then, as the next person goes to view it, it does not go past the Proxy server on the local LAN; it now gets the page from the local server. This dramatically increases speed. Also, the Proxy server has refresh rates you can set so that as updates are made to the real websites out on the Internet, the Proxy server can stay up to date with what it has in its Cache.

3.7 Given a connectivity scenario determine the impact on network functionality of a particular security implementation (For example: port blocking/filtering, authentication and encryption).

In this objective you may have to determine from a laid out scenario on the exam, what a problem is. Here are good examples of why you need to understand what could affect connectivity:

Port Blocking and Filtering

Port blocking and filtering will impact the usage of services that are being blocked. For instance, if you block port 135 because of a Virus attack via a firewall rule or access list, you may see problems utilizing some Windows Services because of that block. This is common. Understand that if you block a port, it is common that you will not be able to use that port – which in reality equates to a service. A good example is blocking ICMP traffic because of possible redirect attacks and then not being able to ping a router because ICMP is blocked. You fixed one issue; you disabled functionality because of it.

Authentication

Authentication will add latency to your connectivity. For instance, if you telnet to a router and that router prompts you for a username and password. Unbeknownst to you, that router may have to first check with a RADIUS server, or an external database. This could add time on to connectivity.

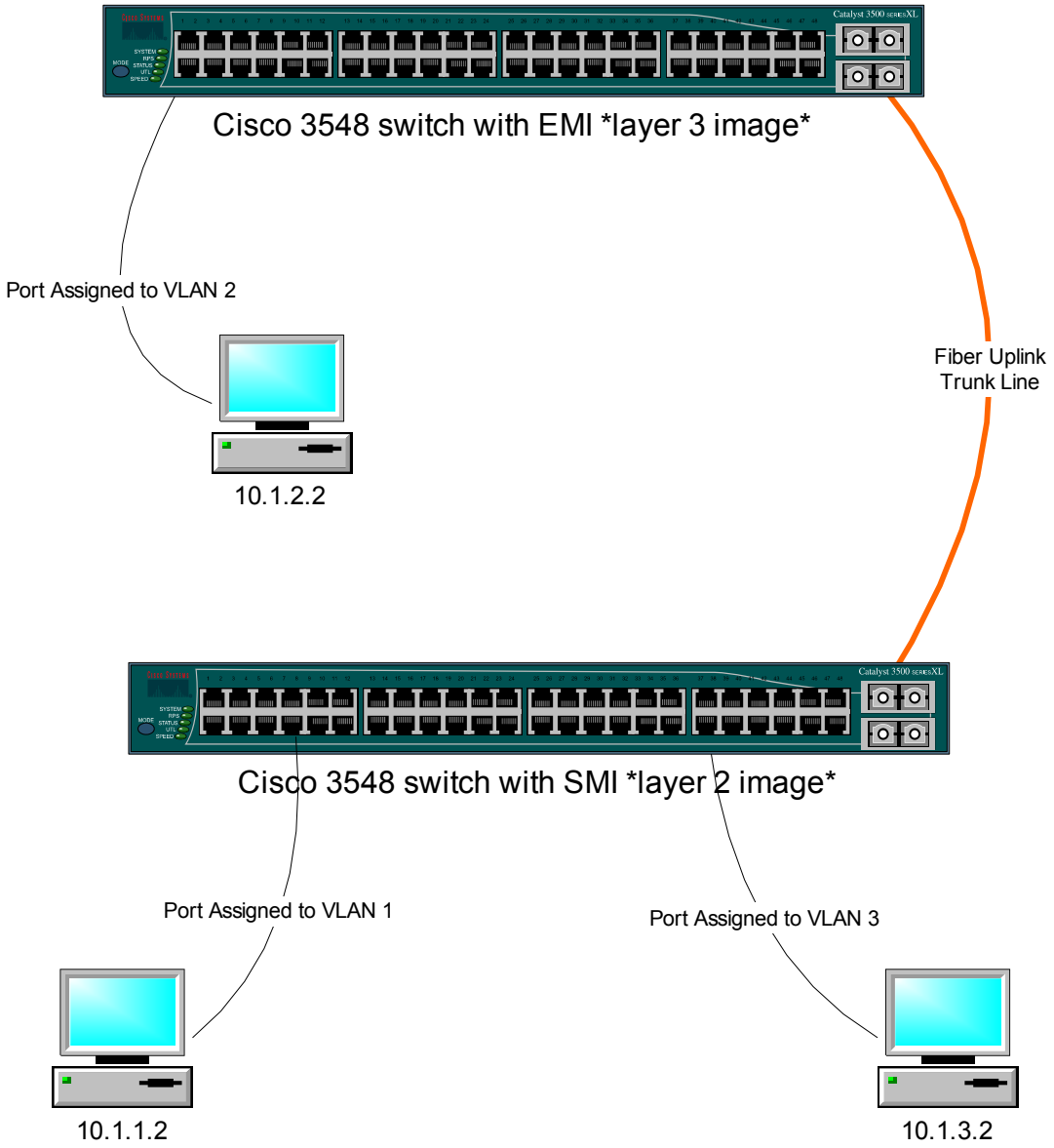
Encryption

Encryption adds overhead to a connection. A good example would be to purchase a DSL line to the Internet and then run an encrypted VPN tunnel over it to the corporate office or other place. Since the data is traversing a public Internet line, for safety reasons, it would be important to secure that data. When you do, you add a process in which adds to the latency of establishing the connections, as well, you are adding size to the data with the encapsulation and extras overhead.

3.8 Identify the main characteristics of VLANs (Virtual Local Area Networks).

VLANs are virtual networks made up of groupings of ports that may be in many different switches. You will not need to know how to configure a VLAN for the exam, but you must know exactly what they are.

VLANs behave as if they are connected to the same switch even though they may actually be physically located on different segments of a LAN on different switches. VLANs are normally configured by port so that you can have a VLAN span multiple switches in your network. A good example of this is seen in the next illustration. VLANs are configured through software rather than hardware, which make them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration, only a software change in the switch, etc.



3.9 Identify the main characteristics and purpose of extranets and intranets.

An extranet is a private network that uses (most commonly) TCP/IP and the public Internet to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. This can be business partners, Business to Business (B2B) connections and so on.

An intranet is a private network that is contained **within** your enterprise. It includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees.

3.10 Identify the purpose, benefits and characteristics of using antivirus software.

In this objective you will be expected to know why AntiVirus software is important. Antivirus software is one of the single most important pieces of software on your system.

The Internet makes it possible for a new virus to spread around the globe in only minutes. This happens on an almost daily basis. Your data can be at risk, your system can be put out of use. For these reasons alone, it almost seems impossible to comprehend that anyone would not put this software on their systems if they visit websites, or send email as simple examples. From this alone, it would almost imply that this software would be some of the most highly sought after for your personal or companies systems. While many new systems come with antivirus software pre-installed, it may not be the best choice for your needs and it most certainly is out of date by the time it is delivered to your home.

If you have an older system, you may want to forgo some of the extra bells and whistles and choose a basic antivirus software package that consumes fewer system resources. Your system can be affected because running AV software in memory and on your system in general may slow it down due to it needing to run and be scanning and checking constantly.

3.11 Identify the purpose and characteristics of fault tolerance:

Fault Tolerance is the ability of any system to be able to respond to failure by being able to recover from it somehow. There are different levels of recovery for a great many different areas where things can fail, this being said, you should have a Fault Management solution in your company.

Power

Power fault tolerance comes in the form of redundant power supplies (2 or more power supplies per device) so if one fails, the other takes over. As well, what it the power in a building went down? Backup generators (Gas run), UPS (Uninterruptible Power Supply) and other forms of redundant power sources can be used.

Link Redundancy

When you depend on a network to deliver services such as email, files and so on, what if that link went down? Having secondary lines in place or a different path through the network would be able to help you recover from issues such as this.

Storage

Storage can also have fault tolerance through a number of ways. Two of the most common would be file server which are clustered. Another way are SANs. Storage Area Networks are share devices for storage that normally reside on their own subnetwork. They are designed in such a way that they are available to all network servers.

Services

Many fault-tolerant computer systems mirror all operations -- that is, every operation is performed on two or more duplicate systems, so if one fails the other can take over. This is called a Cluster. A Cluster will allow you to run a service like email on 2 or more nodes acting as one, which essentially gives you redundancy for the service is one node fails, the other takes over and keeps the email running.

3.12 Identify the purpose and characteristics of disaster recovery:

In this objective you will be expected to know the fundamental concepts of Disaster Recovery (DR). Disaster Recovery is the process of how an organization is going to deal with potential disasters that occur.

Backup and Restore

You must know to backup and restore most operating systems and other equipment so that if failure strikes, you can recover your data. An example would be if you had all your email on one system hard drive and it failed. Even if you put in a new disk, you would have to restore the data you originally backed up to the drive for use. This would restore user mailboxes and critical data.

Offsite Storage

Offsite storage is the storage of important data OFF SIGHT from the location in where the data already sits. This gives you two copies of the data immediately and in cases where a drive fails and you have restore is, if the building the server was in burned down, then at least you have a copy of that data at another location.

Hot and Cold Spares

Hot and cold spares are nothing more than another system either running in parallel or ready to boot up and operate if the system in use fails. A very simple example would be if your monitor burned out, you may have as cold spare in the closet that you KNOW works and you can implement. A Hot spare is something that you have running and can use immediately. A network related example would be if you had a Cisco Switch chassis for a 6509 up and running with no port modules in it, if your other switch chassis failed, you could hot swap all port modules into the new chassis already running and get back up and running quickly.

Hot, Warm and Cold Sites

These are full blown DR sites. You can have a production mainframe sitting in a building somewhere 100 miles away ready to take over all operations for your company if the main system fails. A good example would be with the same mainframe, a hot site would be a mainframe up and running and when the original one fails, then that mainframe immediate goes into production. A warm site and cold site are slightly different. They are both DR sites, but with the example of the hot site, the failure and failover was immediate. With warm sites, you may have to load data or establish a connection. A cold site may need everything, it is just a location where you have get up and running if needed. Each is a DR site, but have different levels of how quickly you can recover associated with them. The Colder you get, the cheaper you get, the Hotter you get, the more expensive it is. Find what is in your budget and implement it.

NOTE: Disaster recovery and fault tolerance make up a small part of the overall exam, but the concepts are very complex, the technology very extensive in many cases and the costs are high. The payback of course is peace of mind, but new management and administration burdens also come into play. For a good book on learning all about High Availability concepts to include Clustering and Load Balancing Windows Server 2003, check out Windows 2000 & Windows Server 2003 Clustering & Load Balancing by Robert J. Shimonski published by McGraw-Hill Osborne Media. ISBN: 0072226226

Domain 4.0 - Network Support

Chapter 4

Quick Jump To:

- Objective 4.1
- Objective 4.2
- Objective 4.3
- Objective 4.4
- Objective 4.5
- Objective 4.6
- Objective 4.7
- Objective 4.8
- Objective 4.9

In the last section of our study guide, we cover Network Support. Network Support covers how to use a troubleshooting strategy as well as what tools to use to troubleshoot with. In this section of the study guide we will cover such technologies to include but not limited to, TCP/IP based troubleshooting tools and using a troubleshooting strategy to isolate issues. This section of the study guide covers 35% of the overall exam.

Exam Objectives Covered:

4.1 Given a troubleshooting scenario select the appropriate network utility from the following:

a. Tracert/traceroute
b. ping
c. arp
d. netstat
e. nbtstat
f. ipconfig/ifconfig
g. winipcfg
h. nslookup/dig

4.2 Given output from a network diagnostic utility (For example: those utilities listed in objective 4.1), identify the utility and interpret the output.

4.3 Given a network scenario, interpret visual indicators (For example: link LEDs (Light Emitting Diode) and collision LEDs (Light Emitting Diode)) to determine the nature of a stated problem.

4.4 Given a troubleshooting scenario involving a client accessing remote network services, identify the cause of the problem (For example: file services, print services, authentication failure, protocol configuration, physical connectivity and SOHO (Small Office/Home Office) router).

4.5 Given a troubleshooting scenario between a client and the following server environments, identify the cause of a stated problem:

a. UNIX/Linux/Mac OS X Server
b. Netware
c. Windows
d. Appleshare IP (Internet Protocol)

4.6 Given a scenario, determine the impact of modifying, adding or removing network services (For example: DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name Service) and WINS (Windows Internet Name Server)) for network resources and users.

4.7 Given a troubleshooting scenario involving a network with a particular physical topology (For example: bus, star, mesh or ring) and including a network diagram, identify the network area affected and the cause of the stated failure.

4.8 Given a network troubleshooting scenario involving an infrastructure (For example: wired or wireless) problem, identify the cause of a stated problem (For example: bad media, interference, network hardware or environment).

4.9 Given a network problem scenario select an appropriate course of action based on a logical troubleshooting strategy. This strategy can include the following steps:

a. Identify the symptoms and potential causes
b. Identify the affected area
c. Establish what has changed
d. Select the most probable cause
e. Implement an action plan and solution including potential effects
f. Test the result
g. Identify the results and effects of the solution
h. Document the solution and process

4.1 Given a troubleshooting scenario select the appropriate network utility from the following:

In this objective you will be expected to know how to use these troubleshooting tools while troubleshooting network problems. Most problems come in the form of connectivity, but others are harder to root out, like a Domain Name System issue for example. Either way, you must memorize all these command and know how to use this inside and out not only to pass the Network+ exam, but to do your job as a network technician. Also, most of these commands can be run on Windows PCs. Tracert is for Windows, where traceroute is for Unix. Nslookup is for Windows and dig is for Unix. The tools are very similar in what they do, but have different syntax you must learn.

To stay current with the time, we will look at Microsoft Windows XP and what it provides a set of built-in utilities for administering and troubleshooting TCP/IP networks. Windows XP contains many of the standard network troubleshooting tools found on most other computers as well as some additional, more advanced ones like pathping. This is just Ping and Tracert incorporated into one utility for the most part. Each of these utilities runs from the Windows command prompt.

From the Start menu, choose **Run** and type **cmd** to open a command window, and then type in the name of the utility to run.

Tracert/traceroute	Tracert is a test tool that will allow you to track the path from one end of the network to another. It will display the name or IP address of each intermediate router or other network gateway device the message passes through to reach its destination. Tracert is especially useful when diagnosing connectivity problems on the Internet because if you have high latency issues, you can see how many *hops* your data is taking and how long it takes to get through each hop. Hops are normally known as router hops, or each router data has to traverse from point A to point B. Tracert (the Windows version) uses ICMP. Traceroute is the Unix version.
ping	Ping is the single most powerful troubleshooting tool for networked computers. The ping tool can help verify that TCP/IP is installed correctly on a computer and that a computer is reachable from one point of the network to another. The ping tool's main offering is that it helps test connectivity via ICMP
arp	The arp command manages the Address Resolution Protocol cache. The ARP cache maintains a list of computer names and their corresponding IP addresses. This is the fundamental way nodes communicate via MAC addresses and arp shows what each node may know about the network.
netstat	The netstat command is designed to help you quickly determine whether your TCP/IP is working correctly. If TCP/IP is having problems, then netstat can help you to determine where the problem is. It will display a list of the current TCP/IP connections. The information presented on this screen includes the protocol (usually TCP), the local address (the MAC address), the foreign address (the IP address), and the connection state.
nbtstat	NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses. TCP/IP provides many options for NetBIOS name resolution, including local cache lookup, WINS server query, broadcast, DNS server query, and LMHOSTS and HOSTS lookup.

ipconfig	The ipconfig tool shows a computer's TCP/IP configuration. It displays the IP address, the network (subnet) mask and the Internet/network gateway address (if one is set for that network). You can use this tool to verify that a TCP/IP configuration has been set up correctly. Ipconfig /all shows the entire configuration. Make sure you are aware of other command line switches you can use by typing ipconfig /? (Found with NT, 2000, 2003, XP)
ifconfig	Linux version of ipconfig
winipcfg	The winipcfg tool shows a computer's TCP/IP configuration. It displays the IP address, the network (subnet) mask and the Internet/network gateway address (if one is set for that network). You can use this tool to verify that a TCP/IP configuration has been set up correctly. It is found with older Windows 9x systems primarily.
nslookup	The nslookup command will Query DNS name servers. You can run command such as setting DNS servers manually, or checking with a server on what IP address a specific DNS name may resolve to.
dig	The dig command will also Query name servers on Linux and Unix systems.

NOTE: The following links can pretty much give you all you need to know about solving connectivity issues on a network and all the syntax you need to know for the network+ exam.

http://support.microsoft.com/kb/314067

http://support.microsoft.com/?kbid=323388

4.2 Given output from a network diagnostic utility (For example: those utilities listed in objective 4.1), identify the utility and interpret the output:

In this objective you will be expected to know how to use the tools in the last objective. Here is a good example of either a ping to a node was successful or not:

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

C:\ >ping 10.1.1.1

Pinging 10.8.102.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=1ms TTL=255
Reply from 10.1.1.1: bytes=32 time=1ms TTL=255
Reply from 10.1.1.1: bytes=32 time=1ms TTL=255
Reply from 10.1.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\ >ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\ >

The important thing to note here is that this is a very simple example of what the objective is looking for. Listing everything that could happen would expand this study guide to about 100+ more pages so make sure that this is an area where you focus some extra time on not only for the exam, but as I mentioned earlier, this is key to surviving in the IT world these days, knowing how to use these tools will help you tremendously and I recommend that you look online or get a book and invest some quality time with this toolset.

NOTE: If possible, I would recommend getting a free copy of Linux and installing it. If you can learn it on Linux as well, you will be surprised as what you can use on that system as well. There are many advanced toolsets on Linux that you can use for help further your network troubleshooting toolset like nmap, tethereal and tcpdump just for starters.

4.3 Given a network scenario, interpret visual indicators (For example: link LEDs (Light Emitting Diode) and collision LEDs (Light Emitting Diode)) to determine the nature of a stated problem:

In this objective you will be expected to know how to look at NIC cards and Switch ports and based on their LEDs, figure out if you have network issue or not. It is almost impossible to know what every vendor has in use – some may have Half Duplex and Full Duplex link lights to show you which one the NIC is running at, you have LEDs that show you what stage of Spanning Tree a switch port may be in. It is really endless what an LED may mean. For production networks, look online to find the vendors website for the product you are using and look up the LEDs online if they are not clearly marked. For purposes of Network+ you should be aware that if you do have a connectivity problem or some form of issue, looking at the back of a server or PC and examining the link light LEDs on the back of the card may provide you information. The most common is the link light, which will show you if at minimum, you even have physical connectivity to the network. Other lights can show duplex and transfer of data.

4.4 Given a troubleshooting scenario involving a client accessing remote network services, identify the cause of the problem (For example: file services, print services, authentication failure, protocol configuration, physical connectivity and SOHO (Small Office/Home Office) router):

In this objective you will be expected to know to look at a scenario involving clients accessing services remotely and any issues that they may have. Most home users are working out of home offices (SOHOs) these days and the numbers are growing. That being said, it is important to know how to quickly figure out and isolate issues as they occur no matter what resource they are trying to use on the corporate network.

First, make sure that the client is physically connected to the network. Knowing the OSI model at this stage can be very helpful for troubleshooting an issue such as this. If you do have network connectivity, make sure you have attempted to connect to the corporate resource via a VPN or remote access service solution. Make sure that if you attempt to do this fails, make sure you have an Internet (or other) connection outside to get to the corporate resources. Checking TCP/IP or any other protocols would make sense here. If all this is ok, then you would want to see if you are entering the right credentials into the client VPN or other solution, so that you can get authenticated, which will allow you access into the corporate network, so you can access resources.

The list goes on, but this is technically what train of thought you are expected to have when doing network support.

4.5 Given a troubleshooting scenario between a client and the following server environments, identify the cause of a stated problem:

In this objective you will be expected to know how to troubleshoot client to server issues. Use the tools found within Mac OSX, Windows, Linux/Unix, and NetWare to make this happen. Just follow common sense practices when troubleshooting end to end. Start with the client and ask the simplest of questions.

Are you the only one experiencing this connectivity issue? Are there any other PC users around you who cannot get to this resource as well? Try to narrow it down, start from there. Then you can use tools like the OSI model to isolate where to look. Is it a blocked port problem? Is it a cabling issue? You can then use tools, and other resources but the key is to understand the environment, isolate to what the root cause is, and lastly, follow a methodology that helps you get granular control over the problem – then attack it and attack it with common sense. Start with the OSI, is it a cabling issue? Layer 1. Is it an IP addressing issue? Layer 3. Figure it out and systematically conquer it.

NOTE: It is important that you understand what tools come with each system and how you can test end to end connectivity from a client to a server so that you can isolate what the problem may be. It could be a network problem, it could be just about anything so it is important to focus on how to isolate issues.

4.6 Given a scenario, determine the impact of modifying, adding or removing network services (For example: DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name Service) and WINS (Windows Internet Name Server)) for network resources and users:

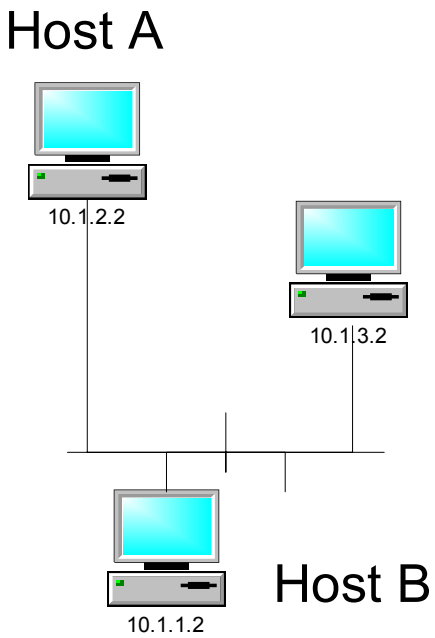
In this objective you will be expected to know what the IMPACT is if you modify, add or remove network services such as DHCP, DNS and WINS.

If you add a DHCP server to the network, you have a lot to consider. First, if you already have one, then you may be adding a *Rogue* DHCP server into the mix. A DHCP server and client operate via a DORA (Discover Offer Request Ack) and the client does not discriminate as to what gives it an address, so if you add a DHCP server to a network segment, you can start to dole out addresses to waiting clients. New DHCP servers (especially with Windows 200x) also offer protective services against this. You also need to understand that routers DO NOT pass broadcasts and that is how clients find DHCP servers so you need to know that a RFC 1542 compliant router is in use, which is one (when configured with lets say, and IP helper address), will forward those broadcasts on to the nearest DHCP server.

DNS and WINS servers can be added to the network, but again, without proper planning, they could also create issues for you. As well, systems like DNS are hierarchical so adding a server means that unless you are creating a new Root, you need to add the DNS server into the existing system. Be aware of what this means for you when it comes to supporting and troubleshooting this effort, hence why nslookup, dig and nbtstat are very important tools to look over and know.

4.7 Given a troubleshooting scenario involving a network with a particular physical topology (For example: bus, star, mesh or ring) and including a network diagram, identify the network area affected and the cause of the stated failure:

In this objective you will be expected to know how to identify a network issue via a diagram. Look at this following illustration. Think about what is wrong. Why is it that Host A cannot ping Host B?



The reason is very simple. Every host is on a different subnet. It is this kind of question you may see on the Network+ exam.

4.8 Given a network troubleshooting scenario involving an infrastructure (For example: wired or wireless) problem, identify the cause of a stated problem (For example: bad media, interference, network hardware or environment):

In this objective you will be expected to know how to figure out what a problem is on a wired or wireless network based on bad media, interference and so on.

Wired network troubleshooting starts with connectivity and verification of that connectivity. Start with the lowest layer of the OSI (which is the Physical layer) and work your way up to the Data Link and so on. Find out what components could have been damaged, disconnected, not powered on, not functional, not responsive, and so on.

Wireless network troubleshooting follows the same exact methodology as the wired network troubleshooting, but with Wireless, you have to consider different issues such as interference from obstacles, attacks such as Jamming, and so on.

4.9 Given a network problem scenario select an appropriate course of action based on a logical troubleshooting strategy.

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

Make sure you know this troubleshooting flow chart like the back of your hand. This flow chart is priceless even beyond the Network+ exam. This chart gives you the exact methodology needed to help find root cause of an issue, which is going to save you time in isolating an issue.