

# TechExams.Net

## Network+ TechNotes (Free version)

**This study guide pertains to the latest exam objectives for the N10-002 Network+ exam.**

**Author: Johan Hiemstra  
CNA, MCSE, CCNA, CCDA**

**Discuss these TechNotes at our forums.**

**Make sure you are ready by using  
our free practice exams.**

**Save over 20% on a Network+ voucher from Pearson VUE!**

**Comments, questions and suggestions:  
[johan@techexams.net](mailto:johan@techexams.net)**

**Need more practice?  
Get the Special Edition of the  
Network+ TechNotes including  
275 practice questions [here](#).**

**TechExams.Net is not sponsored by,  
endorsed by or affiliated with CompTIA.  
All trademarks are trademarks of their respective owners.**

**All images and text are copyright protected,  
violations of these rights will be prosecuted  
to the full extend of the law.**

**MCSE Cisco CompTIA A+ i-Net+ .NET CIW**

**Try Our IT Courses FREE!**

**Click Here!**

**Courses Include:**

- MCSE
- Cisco
- CompTIA A+
- i-Net+
- .NET
- MCAD
- CIW
- Network+
- Linux
- Lotus
- Oracle
- And More!

**FREE Access to Over 400 IT Reference Books!**

**Click Here!**

**Try the NEW MCSE 2003 Course NOW!**

**Click Here!**

**Register to WIN a \$2,400 Dell PC!**

**Click Here!**

**For a FREE Training Catalog Call Toll Free**

**1-877-TRAINING**

1 - 8 7 7 - 8 7 2 - 4 6 4 6

UK Freephone

0800 279 2009



**MCSE Cisco CompTIA A+ i-Net+ .NET CIW**

**INDEX**

**Basic Networking . . . . . 1**

**Media and Topologies . . . . . 2**

**Network Components . . . . . 11**

**WAN Technologies . . . . . 18**

**OSI Model . . . . . 21**

**TCP/IP Suite . . . . . 25**

**TCP/IP Utilities . . . . . 30**

**Network Services . . . . . 38**

**Remote Access and Security Protocols . . . . . 42**

**NETBEUI and NETBIOS . . . . . 45**

**Netware OS and Protocols . . . . . 46**

**AppleTalk . . . . . 49**

**UNIX/LINUX . . . . . 53**

**Fault Tolerance and Disaster Recovery . . . . . 55**

**Internet Connections . . . . . 58**

**Network Support . . . . . 62**

**Exam Objectives . . . . . 64**

## NETWORKING

*Networking* is connecting two or more devices to allow communication between them with the purpose of sharing information and resources. Examples of these devices are computers, printers, routers, hubs, modems, and PDAs. The information and resources being shared can be anything from MS Office documents and e-mail to printers and fax devices. *Internetworking* is connecting multiple networks with the purpose of creating one large network. The Internet is the most common example of an internetwork.

### Client/server vs Peer-to-peer

Most of today's networks use the *client/server* model. In this model at least one computer acts as a server. Servers hold resources that are accessed over the network by clients. Examples of resources are shared files, e-mail messages and even applications. Another common server is the *print server* that allows access to network printers.

In a *peer-to-peer* network model every computer can act as a client and a server at the same time. An example is a network with 4 Windows XP Professional computers in a workgroup using file and print sharing.

### LAN/WAN

The terms LAN and WAN mainly refer to the geographical area of the network. LAN is short for Local Area Network and is a high-speed network typically within a building. WAN is short for Wide Area Network and refers to low-speed networks that cover a large distance, for example a network that spans several cities or the entire globe even. The Internet can be considered the largest WAN, but actually consists of many different WANs, which, in turn, include LANs. The connection between LANs in an internetwork is also referred to as a WAN connection, although a network diagram of a WAN often includes the LANs *in* it.

### Private vs Public Networks

Two other terms used to categorize networks are *private networks* and *public networks*. A private network is typically within the premises of a corporation and can be accessed only by users working for, or related to, that corporation. A public network Internet can be accessed by multiple individuals and/or corporations, the best example of a public network is again, the Internet.

### Media

The physical connection used to transport electrical signals (bits; 1s & 0s) between the network devices is called the *media*. Examples of network media are copper cabling, fiber optic cabling and infra-red. The most common types of media are outlined later in this TechNote.

## Protocols

To be able to communicate with each other, network devices need a common language. The language network devices use is called a *protocol*. There are many different types of protocols available, and most protocols are actually a suite of several protocols, each with a different function.

For example, one protocol allows data transfer between hosts and another can be used to retrieve email from a mail server. Today's most common protocol, TCP/IP, and several older, less common protocols, are described later in this TechNote.

## Addressing

If you want to contact somebody by snail-mail or by telephone you need some sort of address. In a telephone network you need to enter a telephone number to reach your intended communication partner. Similar, devices in a network need an address. There are two types of addresses, the first type is configured in software by a network administrator and uses protocols to define the addressing scheme and format, this type is known as network or layer 3 addressing . The other type of address that devices in a network use, is most commonly referred to as MAC address; this address is burned into the chip of the physical network interface.

## NETWORK TOPOLOGIES

A *logical* topology depicts the route a the signal takes on the network.

A *physical* topology depicts how network devices are connected physically, the cabling.

The 4 diagrams below represent the four topologies:



*Bus* - Devices are connected to a central cable, in this type of network both cable ends must be terminated.



*Star* - Devices are connected through a central hub. The hub forms a single-point-of-failure.



*Ring* - Every device is connected to two other devices, forming a ring.



*Mesh* - In a full mesh every device in the network is connected to every other device. In reality a partial mesh is often used, such as in backbone environments.

## NETWORK TECHNOLOGIES

### 802.2 (LLC)

The Logical Link Control layer is the upper sub layer of the Data Link layer (Layer 2) in the OSI model. LLC masks the underlying network technology by hiding their differences hence providing a single interface to the network layer. The "interface" acts as an intermediate between the different network protocols (IPX, TCP/IP, etc.) and the different network types (Ethernet, Token Ring, etc.).

### 802.3 (Ethernet)

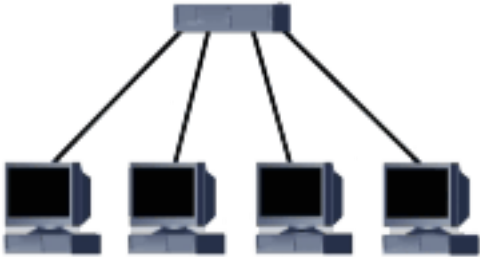
Ethernet is developed by DIX (Digital, Intel and Xerox) in the 1970s. In 1980 the IEEE 802.3 standard was released. Two years later version 2 was introduced which is the basis for today's Ethernet networks. The access method (how the wire is accessed) is Carrier Sense Multiple Access/Collision Detection (CSMA/CD). In a CSMA/CD network stations listen to check if the network is busy, if the network is free the station transmits data. When two stations listen, and both determine the network is not busy, and start sending the data simultaneously a *collision* occurs. When the collision is detected both stations will retransmit the data after a random wait time created by a backoff algorithm.

An Ethernet network is a broadcast system, this means that when a station transmits data every other station receives the data. The frames contain an address in the frame header, only the station with that address will pick up the frame and pass it on to upper-layer protocols to be processed.

## 802.3 Ethernet Standards

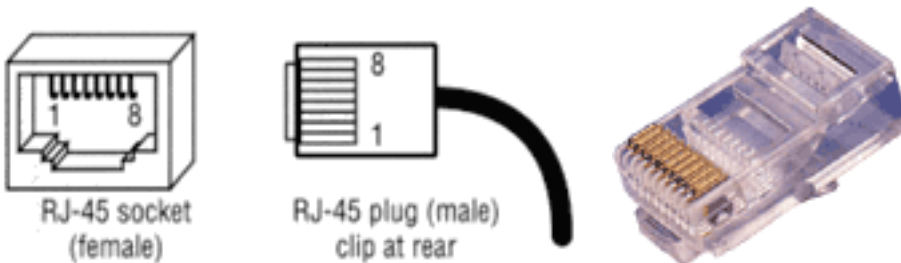
### 10BaseT

The 10BaseT specification uses Cat 3, 4 and 5 UTP cabling in a star/hierarchical topology. Devices on the network are connected through a central hub.



10BaseT specifications:

- Maximum segment length is 100 meters
- Maximum number of attachments per segment is 2
- Maximum data transfer speed is 10Mb/s
- The encoding type used to code the signal is *Manchester*.
- Cat 3, 4 and 5 Unshielded Twisted Pair (UTP) cabling with RJ-45 connectors:



A *wire crimper*, depicted in the image below, is used to attach the RJ-45 connector to the cable.



Another tool commonly used to attach UTP cabling to a jacket, in a patch closet for example, is the *punch down tool*, shown in the following image:



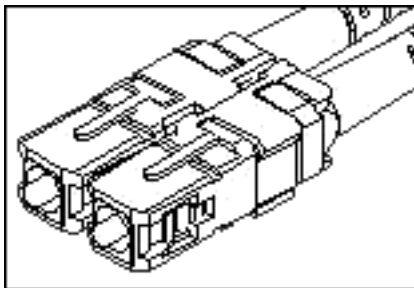
### 100BaseTX (Fast Ethernet, 802.3u)

Is similar to 10BaseT, except it requires Category 5 UTP or Category 1 STP (Shielded Twisted Pair) cabling. Only uses 4 of the 8 wires like just like 10BaseT. The maximum data transfer rate is 100 Mb/s and the encoding type is 4B/5B coding.

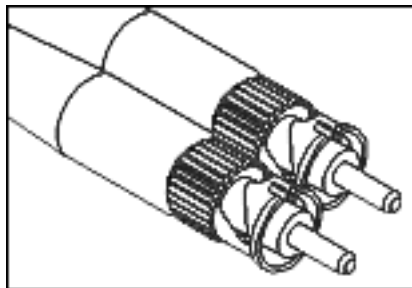
### 100BaseFX (802.3u)

Similar to 100BaseTX but designed to operate over 2 strands of single-mode or multi-mode fiber cabling. One cable is used to send the other is used for collision detection and receiving. The maximum length of a 100BaseFX link is 400 meters in half-duplex mode, 2000 meters in full-duplex mode.

Uses ST, SC or MIC connectors:



SC connectors



ST connectors



SC to ST connectors



MIC connector

## Gigabit Ethernet

There are two standards that specify Gigabit Ethernet systems described below. The encoding type is 8B/10B with simple NRZ (Non Return to Zero) resulting in 10 bits being sent per byte (instead of 8), by running pulses of 1250 MHz the maximum data transfer rate is 1000 Mb/s (1 Gb/s) even with the 20% overhead.

### 802.3ab

Specifies 1000BaseT Gigabit Ethernet over Cat 5e UTP cabling.

- Utilizes all four pairs of cable wires for transmission.
- Maximum segment length is 100 meters.

### 802.3z

Specifies Gigabit Ethernet over fiber and coaxial cabling.

- 1000BaseLX, uses multi-mode fiber with a maximum length of 550 meters or single-mode fiber with a maximum length of 5 km
- 1000BaseSX, uses multi-mode fiber with a maximum length of 500 meters
- 1000BaseCX, uses coaxial cabling with a maximum length of 25 meters (mostly used between servers)

## 10Base2

Commonly referred to as Thinnet, uses a bus topology represented in the following diagram:



Both cable ends are terminated using a 50 ohm terminator.

10Base2 specifications:

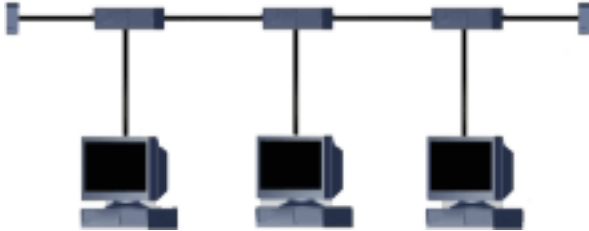
- Maximum segment length is 185 meters
- Maximum number of nodes per segment is 30
- Maximum data transfer speed is 10Mb/s
- 0.2 inch, 50 ohm RG-58 coaxial cable (Thinnet)
- Minimum length between segments 0.5 meter
- Maximum length of collision domain is 925 meters (5 segments, 4 repeaters, max. 3 segments populated)
- Stations are attached using BNC T-connectors represented in the following picture:



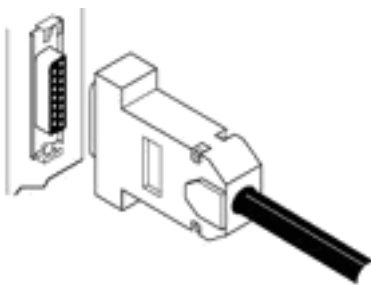
BNC (British Naval Connector) T-connector.

## 10Base5

Commonly referred to as Thicknet, commonly uses a bus topology represented in the following diagram:



Stations are attached using MAUs, a transceiver that is attached to the cable using vampire taps that pierce the cable. A cable with AUI connectors is used to connect the transceiver to the network interface on for example a computer, hub or repeater. Both cable ends are terminated using a 50 ohm terminator.



AUI connectors



MAU transceiver

### 10Base5 specifications:

- Maximum segment length is 500 meters
- Maximum number of nodes per segment is 100
- Maximum data transfer speed is 10Mb/s
- 0.4 inch, 50 ohm coaxial RG-8 cabling (Thicknet)
- Maximum length from a MAU to AUI connector on pc is 50 meter
- Minimum length between MAUs is 2.5 meter
- Maximum length of collision domain is 2500 meters (5 segments, 4 repeaters, max. 3 segments populated)

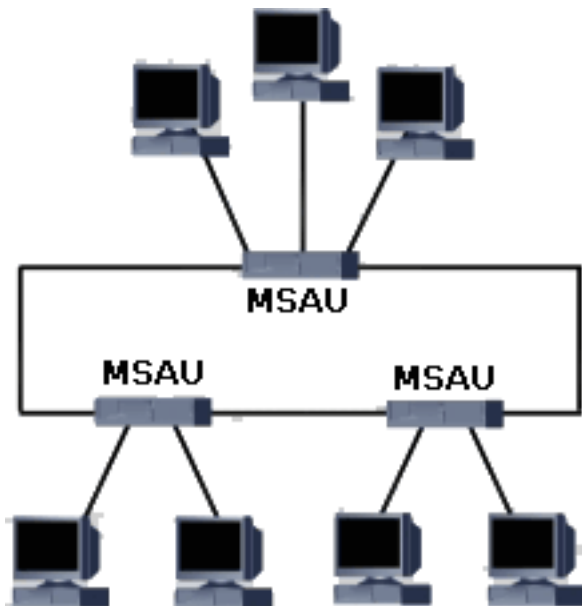
## OTHER NETWORK TECHNOLOGIES

### 802.5 (Token Ring)

Token Ring was originally developed by IBM in the 1970s, later the IEEE 802.5 specification was developed based on IBM's Token Ring. Despite what the exam objective implies, Token Ring and the IEEE 802.5 specification are not the same, but the differences are minor. For example, the IEEE 802.5 specification does not specify a physical topology and media, while Token Ring does. But the term Token Ring usually refers to both specifications.

A token is passed around the network from station to station, when a station does not need to transmit data it passes the token to the next station in the logical ring. A station that receives the token and needs to transmit data seizes the token and sends a data frame, the receiving station marks the data frame as read and passes it forward along the ring to the source station. During this time no other station can transmit data which rules out collisions. The source station releases the token (passing it to the next station) when it receives the data frame and verified it was read.

While the logical topology is a ring, the physical topology is star/hierarchical as illustrated in the diagram below. Stations connect to MultiStation Access Units (look a bit like hubs) using UTP cabling which in turn are connected in a physical ring. If one station in the ring fails it generally doesn't mean the ring is broken, the MSAU will bypass the individual port and exclude it from the ring.



**Token Ring specifications:**

- Data transfer rate is 4 or 16 Mb/s
- Maximum attachments per segment is 250
- Uses Twisted Pair cabling (Cat 3 for 4 MB/s, Cat 5 for 16 Mb/s)
- Access method is token passing
- Logical topology ring, physical topology is star
- Encoding type is Differential Manchester
- Connector type is RJ-45

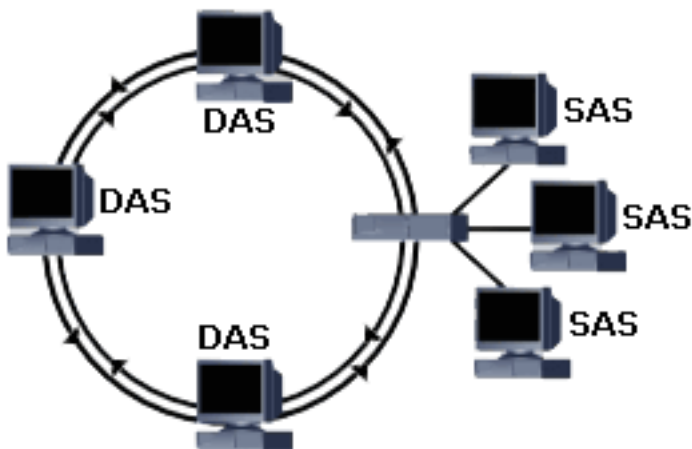
The original IBM Token Ring specification uses IBM Class 1 STP cabling with IBM proprietary connectors. This connector is called the IBM-type Data Connector (IDC) or Universal Data Connector (UDC), and is male nor female.

**FDDI**

Another token-passing network technology is Fiber Distributed Data Interface, created by ANSI (American National Standards Institute) in the mid 1980s. FDDI networks are often used as backbones for wide-area networks providing data transfer rates up to 100 Mb/s using fiber media. The use of fiber also makes it immune to electrical interference, allows it to transmit data over greater distances.

FDDI provides fault tolerance by using a dual counter-rotating ring configuration, an active primary ring and a secondary ring used for backup. Some stations are connected to both rings (Dual-Attached Stations) directly and others are connected to a single ring using concentrators (Single-Attached Stations).

There is also an implementation of FDDI that runs on traditional Copper wiring (UTP) which is known as CDDI but is beyond the scope of the Network+ exam.

**FDDI Specifications**

- Data transfer rates at 100 Mb/s
- Access method is token passing
- Encoding type is 4B/5B with NRZI (nonreturn to zero inverted)
- FDDI is defined at the MAC sub layer and the Physical layer of the OSI model
- Uses fiber optic cabling with SC, ST or MIC connectors

### 802.11b (wireless)

The 802.11b standard specifies wireless Ethernet LAN technology. The topology used in wireless networks is known as *cellular*. It is a wireless structure where stations send signals to each other via wireless media hubs. The access method for 802.11b is CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), this means that a node broadcasts a warning it is about to use the network, before it actually transmits data.

- Clients connect via *wireless access points* with data transfer rates up to 11 MB/s.
- Maximum coverage area/distance instead of maximum length.
- Operates in the 2.45 GHz range

Another WLAN standard that has recently emerged, 802.11a, offers a maximum transmission speed of 54 Mbps.

### MORE TOOLS

#### *Media tester/certifier*

There are several types of cable testers, of which some only monitor the electrical signal and others are capable of recognizing errors such as collisions, traffic congestion, error frames, and protocol errors even. A certifier typically measures frequencies to determine the maximum MHz for a cable.

#### *Tone generator*

This device is used to find outer ends of a cable. Place the tone generator on one end of the cable you want to find the other end of, and use a tracer (or probe) on the other end, or usually, what you think is the other end.

#### *Optical tester*

This device can be used to find a break or kink in fiber optic cabling.

#### *Time Domain Reflectometer (TDR)*

This device sends pulses through a cable to detect a break or other inconsistencies.

#### *Loopback adapter*

As a physical device, a loopback adapter is a kind of terminator you can connect directly to a NIC, allowing you to configure it with an IP address to simulate as if a network were attached.

#### *Digital Volt meter*

A very common electrical measurement tool that can be used to track down breaks in the cable, as well as shortage with other cabling or metal.

#### *Protocol Analyzers (Sniffers)*

Typically a tool implemented in software, that analyzes data packets itself to determine network problems related to software, clients/servers, network addressing and much more.

## Network Components

### Collision Domain

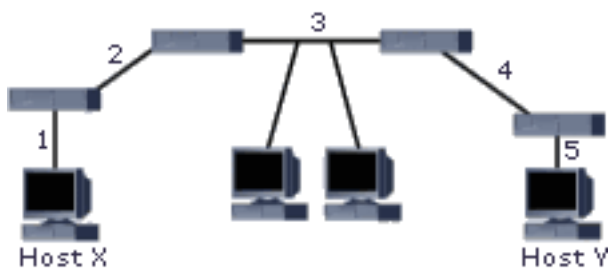
As you may have read in our [Media and Topologies TechNote](#) collisions occur on Ethernet networks when two nodes on the 'network' start transmitting data at exactly the same time and the two frames collide. In today's large-fast-growing-bandwidth-eating network environments this will soon become a problem, stations will have to wait longer before they can transmit data and more collisions will occur. But there are multiple solutions to this problem; those two nodes would actually have to be in the same *collision domain (segment)* for this problem to occur, and networks can be separated in to multiple collisions domains using the appropriate device. Where the boundaries of a collision domain lies will be made clear using a network diagram for each of the following relevant network components.

### Broadcast Domain

All devices in this domain will receive broadcast frames originating from any other device within the domain. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Broadcast frames are frames explicitly directed to all nodes on the LAN.

### Repeaters

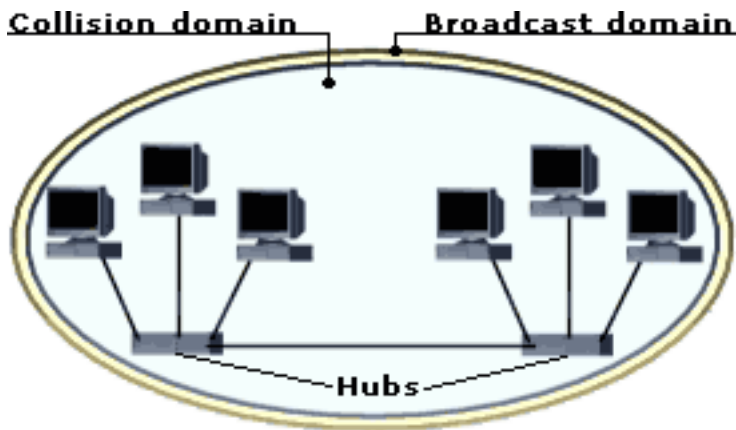
A repeaters is a simple device that is used to expand LANs over larger distances by connecting segments. They do not control broadcast or collision domains, they are not aware of upper-layer protocols and frame formats, they merely regenerate/amplify the signal. Repeater operate at the Physical layer of the OSI model. An important rule when using repeaters to expand a network is the *5-4-3 rule*, which defines that the maximum distance between two hosts on the same network can be 5 segments, 4 repeaters, and only 3 of the segments can be populated, as illustrated in the following logical network diagram:



## Hubs

Hubs, also known as concentrators or multiport repeaters, are used in star/hierarchical networks to connect multiple stations/cable segments. There are two main types of hubs: *passive* and *active*. An active hub takes the incoming frames, amplifies the signal, and forwards it to all other ports, a passive hub simply splits the signal and forwards it. Another type of hubs can be managed allowing individual port configuration and traffic monitoring, these are known as intelligent- or managed hubs.

Hubs operate on the physical layer of the OSI model and they are *protocol transparent*, that means they are not aware of the upper-layer protocols and such as IP, IPX nor MAC addressing. Hence they do not control broadcast or collision domains, but they extend them as illustrated below:



The following is a picture of a Fast Ethernet hub.

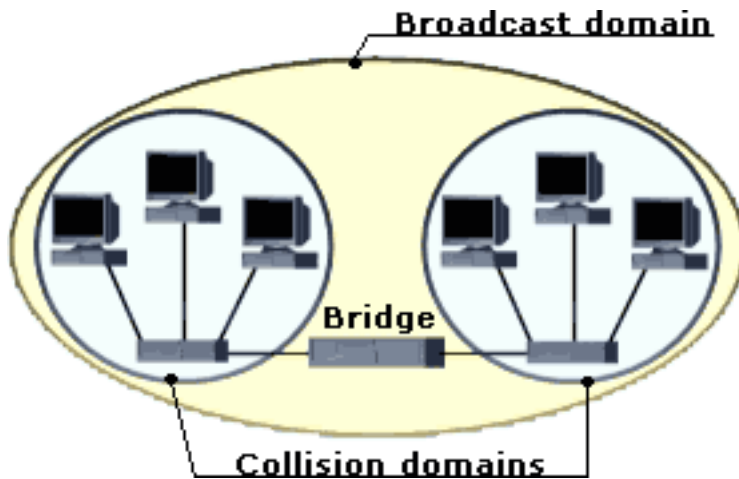


## BRIDGES

Bridges are more intelligent than hubs; they operate on the Data Link layer of the OSI model. They are used to increase network performance by *segmenting* networks in separate collision domains. Bridges are also protocol transparent, they are not aware of the upper-layer protocols. They keep a table with MAC addresses of all nodes, and on which segment they are located.

A bridge takes an incoming frame, reads its destination MAC address and consults the database to decide what should be done with the frame; if the location of the destination MAC address is listed in the database, the frame is forwarded to the corresponding port. If the destination port is the same as the port where the frame arrived it will be discarded. If the location is not known the frame will be *flooded* through all outgoing ports/segments.

As illustrated below, bridges control collision domains, they do not control broadcast domains:



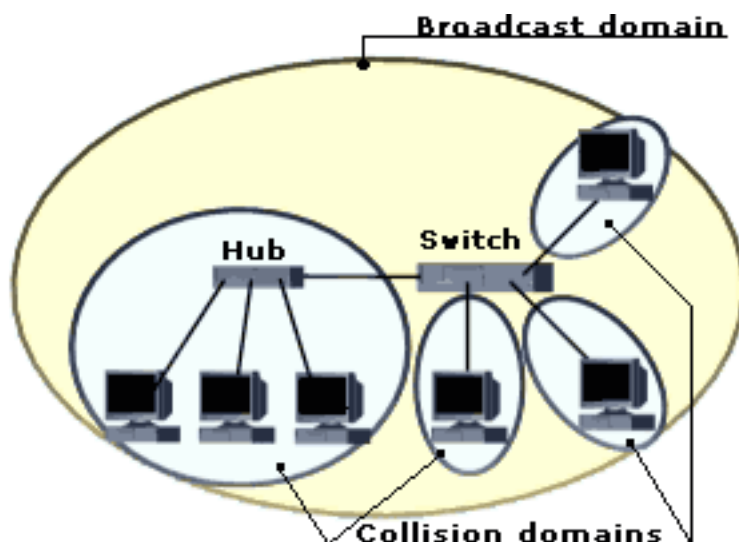
## SWITCHES

To improve network performance even more switches were developed, switches are very similar to bridges; they also keep a table with MAC addresses per port to make switching decisions, operate in the OSI model and are protocol transparent.

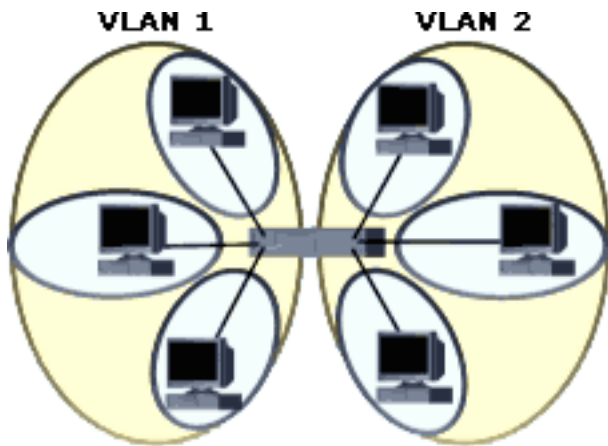
Some of the main differences are:

- a switch has more ports than a bridge (a switch looks more like a hub) and provide a collision domain per port.
- bridges switch in software whereas switches switch in hardware (integrated circuits)
- switches offer more variance in speed, an individual port can be assigned 10 Mb/s or 100 Mb/s or even more.

As illustrated below, switches control collision domains, they do not control broadcast domains\*:



\* Switches do not control broadcast domains unless Virtual Local Area Networks (VLANs) are being used, and most modern switches do support VLANs. The following diagram represents a router configured with two VLANs. Like in the previous diagram each port forms an collision domain, but as you can see in this diagram the network is separated in two broadcast domains using VLANs. If the network protocol used in this network would be TCP/IP the VLANs would each have its own (sub-)network address, for example VLAN 1 could be Class C 192.168.110.x and VLAN 2 192.168.220.x.



Switches are able to use software to create Virtual LANs; a logical grouping of network devices where the members can be on different physical segments. A VLAN can be based on Port IDs, MAC addresses, protocols or applications. For example in the network diagram above port 1 to 12 on the switch could be assigned to VLAN 1, and port 13 to 24 to VLAN 2, resulting in two different broadcast domains, or station 1, 2 and 3 could be using IPX/SPX while station 4, 5 and 6 could be using TCP/IP.

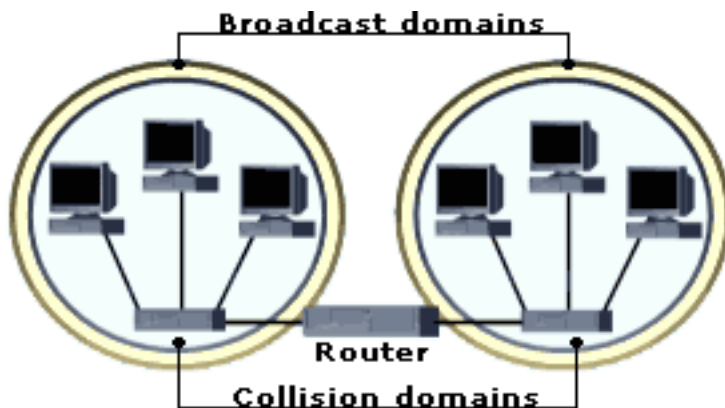
Switches are able to use software to create Virtual LANs; a logical grouping of network devices where the members can be on different physical segments. A VLAN can be based on Port IDs, MAC addresses, protocols or applications. For example in the network diagram above port 1 to 12 on the switch could be assigned to VLAN 1, and port 13 to 24 to VLAN 2, resulting in two different broadcast domains, or station 1, 2 and 3 could be using IPX/SPX while station 4, 5 and 6 could be using TCP/IP.

An example of a large network with VLANs could be an office building with a switch on each of the three floors and a main switch connecting them all together. An administrator would be able to keep a list of MAC addresses and assign stations from different floors to a single VLAN and for example create a VLAN (broadcast domain) for each department in the company. Switches share their MAC address table information with other switches so the path to a destination can be found quickly.

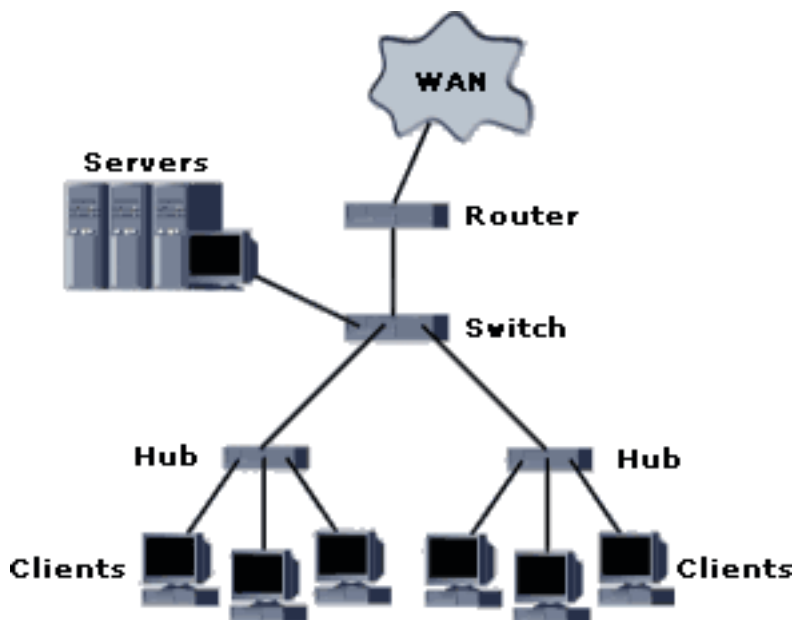
## ROUTERS

Routers are used to interconnect multiple (sub-)networks and route information between these networks by choosing an optimal path ("route") to the destination. They operate on the Network layer (Layer 3) of the OSI model and in contradiction to hubs, bridges and switches, routers are protocol-aware. Examples of these protocols are: IP, IPX, and AppleTalk. Routers make forwarding decisions based on a table with network addresses and their corresponding ports, this table is known as the *route table*. Common use of routers is to connect two different type of networks (for example Ethernet and Token ring) or to interconnect LANs into a WAN. The concept of routing will be covered in more detail in another TechNote, covering the most popular routed protocol: TCP/IP.

As illustrated below, routers control collision domains AND broadcast domains:



The network components described above are often used in combination. The following network diagram shows a simple network using three of them:



## GATEWAYS

A gateway (as a network component) is a device that connects networks with dissimilar network protocols or architectures and translates between the networks. Gateways are very intelligent devices, generally they operate on the Transport layer and on those above it (Session, Presentation, Application). A gateway could be used to allow IPX/SPX clients to use a gateway with a TCP/IP uplink to an internet connection. TCP/IP would be converted to IPX/SPX. Another common use of a gateway is to connect an Ethernet network to an IBM SNA mainframe environment.

## CSU/DSU

CSU/DSU stands for Channel Service Unit/Data Service Unit. A CSU/DSU is a hardware device about the size of an external modem that converts digital data frames from the communications technology used on a local area network (LAN) into frames appropriate to a wide-area network (WAN) and vice versa. A CSU/DSU is mainly used on both ends of a T-1 or T-3 connection. A T1 or T3 is a fast digital leased line, often used for high-speed internet connections. (will be covered in more detail in our WAN Technologies TechNote.)

## NICs

A Network Interface Card (NIC), typically an expansion card in a computer, is used to connect to the physical network media. The NIC's interface itself is defined at the Physical layer (Layer 1) of the OSI model, the *physical address* (also known as Burned-In Address and commonly: MAC address) of the adapter as well as the drivers to control the NIC are located at the Data Link layer's MAC sub-layer. The reason the *physical address* is defined at the Data Link layer is that the Physical layer only handles bits. Some mainboards and most portable computers are equipped with a built-in (*onboard*) NIC. NICs are available for different types of network media, the most common today being Ethernet NICs with a RJ-45 socket for UTP/STP cabling. To install a network interface card you need a free ISA or PCI expansion slot and an appropriate driver that the computer's operating system will use to communicate with the NIC. Some older ISA NICs can be manually configured to use a particular IRQ. This is done by setting jumpers or dip switches. Some other NICs allow the IRQ to be configured through the use of configuration software.



An image of a Fast Ethernet network interface card.

Many of today's NICs are equipped with status indicators in the form of leds. These leds can be used to troubleshoot network problems. Typically one green led indicates the NIC is physically connected to the network and flashes when activity occurs, i.e., the port is transmitting or receiving data, this is also known as a *heartbeat*. When the NIC supports multiple speeds, for example 10 and 100 Mbps, there can be a green led for each speed, of which one is lit indicating the current speed, possibly auto-negotiated with a hub or switch. Some NICs, as well as other network devices such as hubs, include an orange or red led which flashes when collisions occur. If the collision LED flashes repeatedly or continuously, the NIC may be configured incorrectly or may be malfunctioning, or there may be other devices utilizing the network heavily.

As described earlier, network interfaces are physically configured with an address known as the MAC address (MAC is short for Media Access Layer), layer 2 address, Burned In Address (BIA), or physical address. Here's an example of a MAC address: 00-10-E3-42-A8-BC. The first 6 hexadecimal digits specify the vendor/manufacturer of the NIC, the other 6 define the host. MAC addresses are supposedly unique across the planet.

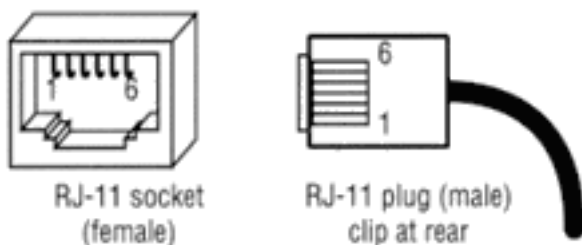
## MODEMS

Modems are used to for low-speed long-distance connections over telephone lines. Modems convert parallel digital data to serial analog data and vice versa.

There are two main types of modems:

- **Internal** Expansion cards (e.g. ISA, PCI) or 'On-board' (integrated in mainboard)
- **External** Modems that connect to the serial RS-232 or USB port and often have their own power supply.

A telephone line is connected to the modem using a RJ-11 connector displayed below:



## WAN Technologies

### Circuit switching vs. Packet switching

The most common example of a *circuit switching* network is the telephone system; the sender and the receiver establish a dedicated physical path for the entire duration of the call. All packets send follow the same route. PSTN (the Public Switched Telephone Network) and ISDN both use the circuit switching technology.

In a *packet switching* network data is segmented in packets that each take a route independently based on the addressing information their header. In theory the route can be different for each packet, but also one and the same. The packet is sent from hop to hop whereby each 'router' determines the (best) next part of the route. The Internet is largely made up of packet switching networks.

### ISDN

Integrated Services Digital Network, a circuit-switching network used for voice, data and video transfer over existing copper telephone lines. ISDN is a bit similar to the normal telephone system but it is faster and needs less time to setup a call.

There are several types of digital channels, the two main being the 64 Kilobits per second B-channel for data, and the D-channel for control information.

Two B-channels + one D-channel make up ISDN BRI (Basic-Rate Interface), some Remote Access servers support a feature called *multilink* allowing both B-channels to be combined in a single virtual link of 128 Kbps. Often 1 B-channel is used for data (an internet connection for example) and 1 B-channel is used for voice (connected to a digital telephone for example). ISDN PRI (Primary-Rate Interface) is made up of 23 B-channels and 1 D-channel (The European version supports 30 B-channels).

A common implementation of these two types of ISDN is a remote access solution with ISDN PRI at the corporate network supporting 23 dial-in connections for employees with ISDN BRI at home.

### ATM

ATM is short for Asynchronous Transfer Mode, a packet-switching network that is commonly used for high-speed backbones in large network environments such as the Internet, for voice, data and video transfer.

Data is transmitted in small 53-byte fixed length *cells*. Partly because of this fixed length ATM is able to reach data rates up to 622 Mbps. Also, an ATM switch uses integrated hardware circuits that switch cells between incoming and outgoing ports which significantly increase data throughput compared to software based switching. Every cell with the same source and destination address travels over the same route when possible.

ATM support some innovative features such as *Bandwidth on demand* and *QoS (Quality of Service)*, the latter allows data to be prioritized based on the content. For example real-time video transfer could have a higher priority then file transfer to allow the user to watch the video without interruptions.

ATM support some innovative features such as *Bandwidth on demand* and *QoS (Quality of Service)*, the latter allows data to be prioritized based on the content. For example real-time video transfer could have a higher priority then file transfer to allow the user to watch the video without interruptions.

ATM uses its own reference model, which corresponds roughly to both the Data Link and the Physical Layer.

ATM supports different types of media such as:

- Sonet OC-3, OC-12
- T3/E3
- 155 Mbps UTP
- 100 Mbps FDDI

### Frame Relay

Frame Relay, one of today's most common examples of a packet-switching network, is a high-performance WAN protocol that operates at the physical and data link layers of the OSI model. An advantage of using Frame Relay is that the physical network medium and the available bandwidth is dynamically shared between end nodes. Common use of Frame Relay is to interconnect LANs in a WAN and or providing centralized internet connectivity to remote offices. It is very cost-effective because generally you only pay for the bandwidth usage. A Frame Relay network is often represented as a cloud like in the following network diagram:



The cloud typically represents the carriers network (owned by the phone company for example if is a public network, but private Frame Relay networks keep getting more common.) which can be shared by several companies. To ensure there is bandwidth available the carrier and the customer agree on a *Committed Information Rate (CIR)*, this is where you pay for, if more bandwidth is available you'll be able to use it but the CIR is the minimum guaranteed bandwidth available. Common line speeds in the US are fractional T1 to T1 (1.544 Mbps).

The boxes in the diagram above represent the routers (which can also be terminals, PCs, bridges etc.) are located on the premises of a customer. The connections between two locations are called Virtual Circuits; there are two types of VCs in frame relay:

- Permanent Virtual Circuits: manually configured permanent connection.
- Switched Virtual Circuits: dynamically by software configured connection, created when needed.

Frame Relay supports a wide variety of physical interfaces. Media includes ISDN and T1.

## **HIGH-SPEED WAN MEDIA**

### **SONET/OCx**

Sonet is short for Synchronous Optical NETWORK, a hierarchy of standardized digital data rates for optical transmission interfaces proposed by Bellcore.

These data rates divided in OC-levels, the following table lists the speeds for "a couple of" OC levels:

OC-1 = 51.85 Mbps  
OC-3 = 155.52 Mbps  
OC-9 = 466.56 Mbps  
OC-12 = 622.08 Mbps  
OC-18 = 933.12 Mbps  
OC-24 = 1.244 Gbps  
OC-36 = 1.866 Gbps  
OC-48 = 2.488 Gbps  
OC-192=9.952 Gbps

(Note: You only need to remember the speed of OC-1, for example: OC-18 is simply 18 times the speed of OC-1)

### **T1/E1 & T3/E3**

T1 is a digital leased line made up of 24 channels (called DS0, 1 DS0 is 64K), providing rates up to 1.544 Mbps, often used to connect corporate networks and ISPs to the Internet. The European version E1 is made up of 30 channels providing rates up to 2.048 Mbps.

T1 uses the DS1 signaling standard and that's why they are sometimes also referred to as DS1 lines.

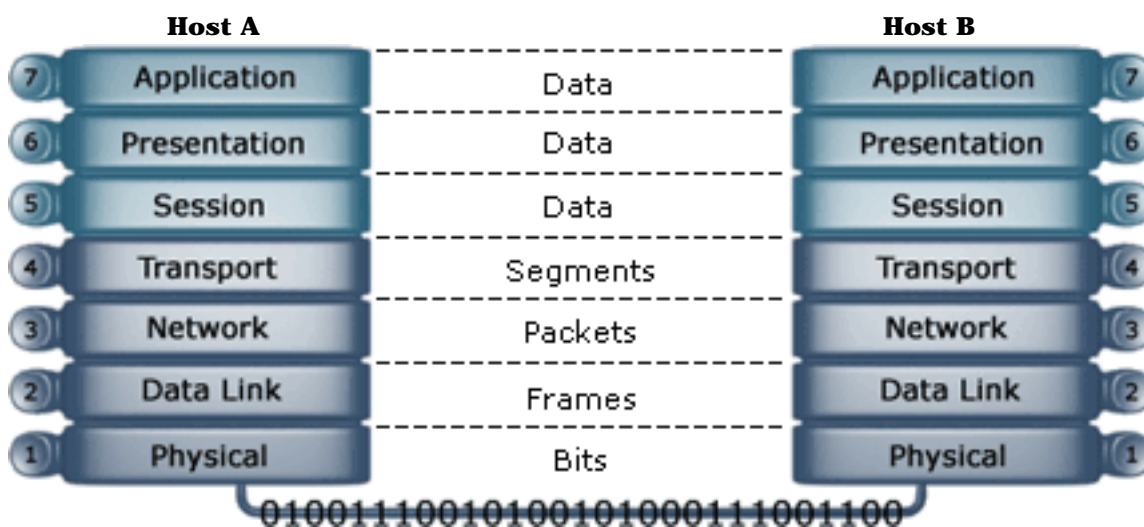
A T3 is an even faster digital leased line providing rates up to 44.736 Mbps (672 DS0s), often used for high-speed internet backbones. The European version E3 provides rates up to 34.064 Mbps (480 DS0s). T3/E3 uses the DS3 signalling standard.

CSU/DSU stands for Channel Service Unit/Data Service Unit, a modem-like device that converts digital data frames from the communications technology used on a local area network into frames appropriate to a wide-area network and vice versa. This device is usually on each site of the T1/T3 connection (sometimes as an integrated device in a router.)

## 7-layer OSI MODEL

The OSI (Open System Interconnection) model is developed by ISO in 1984 to provide a reference model for the complex aspects related to network communication. It divides the different functions and services provided by network hardware and software in 7 layers. This facilitates modular engineering, simplifies teaching and learning network technologies, helps to isolate problems and allows vendors to focus on just the layer(s) in which their hardware or software is implemented and be able to create products that are compatible, standardized and interoperable.

The diagram below shows the 7 layers of the OSI Model, to remember them in the correct order a common mnemonic is often used: **All People Seem To Need Data Processing**.



The Application, Presentation and Session layer are known as the *Upper Layer* and are implemented in software. The Transport and Network layer are mainly concerned with protocols for delivery and routing of packets to a destination and are implemented in software as well. The Data Link is implemented in hard- and software and the Physical layer is implemented in hardware only, hence its name. These last two layers define LAN and WAN specifications.

A more detailed description of each layer follows below, but here's what basically happens when data passes from Host A to Host B:

1. the Application, Presentation and Session layer take user input and converts it into data,
2. the Transport layer adds a segment header converting the data into segments,
3. the Network layer adds a network header and converts the segments into packets / datagrams,
4. the Data Link layer adds a frame header converting the packets/datagrams into frames,
5. the MAC sublayer layer converts the frames into a bits which the Physical layer can put on the wire.

The steps are known as the 5 steps of *data encapsulation*. When the bits stream arrives at the destination, the Physical layer takes it off the wire and converts it into frames, each layer will remove their corresponding header while the data flows up the OSI model until it is converted back to data and presented to the user, this is known as *decapsulation*.

## APPLICATION

The Application layer provides network services directly to the user's application such as a web browser, email software and Windows Explorer. This layer is said to be "closest to the user". Protocols that operate on this layer include: TELNET, HTTP, FTP, TFTP, SMTP, NTP.

## PRESENTATION

This layer 'represents' the data in a particular format to the Application layer. It defines encryption, compression, conversion and other coding functions. Specifications defined at this layer include: GIF, JPEG, MPEG, MIME, and ASCII.

## SESSION

Establishes, maintains and terminates end-to-end connections (sessions) between two applications on two network nodes. It controls the dialogue between the source and destination node, which node can send when and how long. Also provides error reporting for the Application, Presentation and Session layer. Protocols/API's that operate on this layer include: RPC, NETBIOS.

## TRANSPORT

This layer converts the data received from the upper layers into segments. The Transport layer is responsible for end-to-end (also called source-to-destination) delivery of entire messages. Provides end-to-end connectivity, it allows data to be transferred reliably and sequencing to guarantee that it will be delivered in the same order that it was sent. Provides services such as error checking and flow control (software). Protocols that operate on this layer: TCP, UDP, NETBEUI, SPX.

These protocols are either *connectionless* or *connection-oriented*:

**Connection-oriented** means that a connection (a virtual link) must be established before data can be exchanged. This can guarantee that data will arrive, and in the same order it was sent. It guarantees delivery by sending acknowledgements back to the source when messages are received. TCP is an example of an connection-oriented transport protocol.

A common example of connection-oriented communication is a telephone call: you call, the 'destination' picks up the phone and acknowledges and you start talking (sending data). When a message or a piece of it doesn't arrive, you say: "What!?" and the sender will retransmit the data.

**Connectionless** is the opposite of connection-oriented; the sender does not establish a connection before it sends data, it just sends without guaranteeing delivery. UDP is an example of an connectionless transport protocol.

## NETWORK

This layer converts the segments from the Transport layer into packets (or datagrams) and is responsible for path determination, *routing*, and the delivery of these individual packets across multiple networks without guaranteed delivery. The network layer treats these packets independently, without recognizing any relationship between those packets, it relies on upper layers for reliable delivery and sequencing.

Also this layer is responsible for *logical addressing* (also known as network addressing or Layer 3 addressing) for example IP addresses

Protocols defined at this layer: IP, IPX, ICMP, RIP, OSPF, BGP.

Devices that operate on this layer: Routers, Layer 3 Switches.

## DATA LINK

The Data Links provides transparent network services to the Network layer so the Network layer can be ignorant about the physical network topology and provides access to the physical networking media. Responsible for reassembling bits taken of the wire by the Physical layer to frames, makes sure they are in the correct order and requests retransmission of frames in case an error occurs. Provides error checking by adding a CRC to the frame, and flow control.

Devices that operate on this layer: Switches and Bridges

## IEEE 802 Data Link sub layers

Around the same time the OSI model was developed, the IEEE developed the 802-standards such as 802.5 Token Ring and 802.11 for wireless networks. Both organizations exchanged information during the development which resulted in two compatible standards. The IEEE 802 standards define physical network components such as cabling and network interfaces, and correspond to the Data Link and/or Physical layer of the OSI model. The IEEE refined the standards and divided the Data Link layer into two sublayers: the LLC and the MAC sub layer.

### - LLC sublayer

LLC is short for Logical Link Control. The Logical Link Control is the upper sublayer of the Data Link layer. LLC masks the underlying network technology by hiding their differences hence providing a single interface to the network layer. The LLC sublayer uses Source Service Access Points (SSAPs) and Destination Service Access Points (DSAPs) to help the lower layers communicate to the Network layer protocols acting as an intermediate between the different network protocols (IPX, TCP/IP, etc.) and the different network types (Ethernet, Token Ring, etc.) This layer is also responsible for frames sequencing and acknowledgements.

The LLC sublayer is defined in the IEEE standard 802.2.

**- MAC sublayer**

The Media Access Control layer takes care of physical addressing and allows upper layers access to the physical media, handles frame addressing, error checking. This layer controls and communicates directly with the physical network media through the network interface card. It converts the frames into bits to pass them on to the Physical layer who puts them on the wire (and vice versa)

IEEE LAN standards such as 802.3, 802.4, 802.5 and 802.10 define standards for the MAC sublayer as well as the Physical layer.

**PHYSICAL**

This layer communicates directly with the physical media, it is responsible for activating, maintaining and deactivating the physical link. It handles a raw bits stream and places it on the wire to be picked up by the Physical layer at the receiving node. It defines electrical and optical signaling, voltage levels, data transmission rates and distances as well as mechanical specifications such as cable lengths and connectors, the amount of pins and their function. Devices that operate on this layer: HUBs/concentrators, repeaters, NICs, and LAN and WAN interfaces such as RS-232, OC-3 and BRI.

## TCP/IP Suite

TCP/IP is today's most popular network protocol and is *the* protocol in the internet. It is a *routable* protocol that provides connection between *heterogeneous* systems, these are the main reasons the protocol is so widely adapted; for example it allows communication between UNIX, Windows, Netware and Mac OS computers spread over multiple interconnected networks.

The "TCP/IP protocol" is actually the "TCP/IP suite" composed of many different protocols each with its own functions. The two main protocols are in its name: the Transmission Control Protocol and the Internet Protocol, both outlined below as well as some of the many other protocols in the TCP/IP suite.

## IP

The Internet Protocol is defined at the Network layer and provides connectionless delivery of packets across networks. IP is also responsible for routing and Network layer addressing.

## IP Addressing

IP addressing is assigning a 32-bit logical numeric address to a network device. Every IP address on the network must be unique. An IP address is represented in a dotted decimal format, for example:

159.101.6.8

as you can see the address is divided in 4 parts, these parts are called *octets*.

## Decimal to Binary

Each octet represents 8 bits. The IP address mentioned above can also be displayed in dotted binary format:

10011111.01100101.00000110.00001000

Converting the decimal address to a binary format (and vice versa) is a fairly easy process. The highest decimal number you can represent in 8 bits is 255:

$$\begin{array}{cccccccc}
 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 128 + & 64 + & 32 + & 16 + & 8 + & 4 + & 2 + & 1 \\
 (2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0)
 \end{array}
 = 255$$

Examples:

00000010 = 2

00000011 = 3

10000001 = 129

10111111 = 191

11000000 = 192

The current used addressing schema in version 4 of IP is divided in 5 Classes:

<b>Classes</b>	<b>First Octet</b>
Class A	1--126
Class B	128--191
Class C	192--223
Class D	224--239
Class E	240--254

### Private Address ranges

IANA reserved 4 address ranges to be used in private networks, these addresses won't appear on the Internet avoiding IP address conflicts:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255
- 169.254.0.1 through 169.254.255.254 (reserved for Automatic Private IP Addressing)

The range 127.0.0.0 to 127.255.255.255 is reserved for IP loopback addresses, which is mainly used for testing purposes and to check if the TCP/IP stack has correctly loaded.

### Subnet Masks

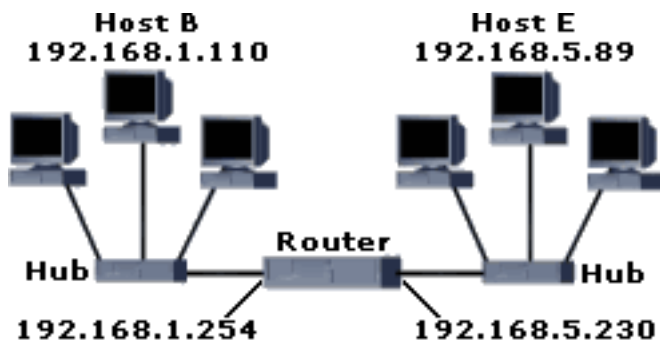
In order for a protocol to be routable a network address must have two parts: a *host* and a *network* portion. TCP/IP uses subnet masks to determine which part is the host portion and which is the network portion. For example in a Class B IP address 172.16.12.234 with the default Class B 16 bits subnet mask of 255.255.0.0 the network portion is 172.16 and the host part is 12.234.

Default subnet masks:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

### Default gateway

The purpose of a default gateway is easily defined ("All data not meant for the local subnet is sent to this router") but best explained using an example of an IP packet traveling along an internetwork.



For example, in the previous network diagram the default gateway for Host B would be the router interface with 192.168.1.254 and the default gateway for Host E would be 192.168.5.230. If Host B wants to contact Host E it will notice the *host* part of the IP address of Host E differs from its own address, so it will forward the packet to the router interface with IP 192.168.1.254, the router will decide the route to the network 192.168.5.x, which in this case is directly connected to another interface of the same router, this interface with IP 192.168.5.230 will connect to Host E and deliver the packet. So again: if a default gateway is set and a computer wants to send a packet to a host on another (sub-)network it would be send to the default gateway.

## IPv6

The info above refers to IP version 4. Another version, IPv6, was developed to allow larger networks with more hosts, because we might be running out of IPv4 addresses within a couple of years. IPv6 uses a 128-bit address format allowing a theoretical  $2^{128}$  unique addresses (= 340282366920938463463374607431768211456 forgive me if I made a typo ; ) ).

An IPv6 address is written in a maximum of 8 groups of 16 bits each written as four hex digits separated by colons, for example: FEDC:BA12:ABCD:3210:FEDC:BA98:7654:1234

## OTHER TCP/IP PROTOCOLS

### *Sockets*

Before describing the main TCP/IP protocols first an important feature of TCP/IP: sockets. A socket is the combination of an IP address and a port number. Different applications (defined at the Application layer of the OSI model) use different port numbers allowing multiple applications to share the same connection, for example connect to an SMTP mail server on port 25 to send email and at the same time connect to a web server on port 80 to browse a web site.

Each application uses either TCP or UDP for transport, although some can use both.

### TCP

The Transmission Control Protocol is a Transport layer protocol that provides reliable *connection-oriented* full-duplex transport. Connection-oriented means that a connection must be established before hosts can exchange data. A common explanation of connection-oriented communication is a telephone call: you call, the 'destination' picks up the phone and acknowledges and you start talking (sending data). TCP guarantees delivery by sending acknowledgements back to the source when messages are received.

**UDP**

The User Datagram Protocol is a connectionless Transport layer protocol that provides *best-effort* delivery.

Unlike TCP, there is no guarantee that UDP datagrams ever reach their intended destination, UDP is said to be unreliable. It is like sending a postcard, you just send it out and hope it will reach its destination.

**FTP**

The File Transfer Protocol is an Application layer protocol and provides connection-oriented file transfer functions. Connects to TCP port 21 for control and uses TCP port 20 to transfer data.

**TFTP**

The Trivial File Transfer Protocol is an Application layer protocol that provides connectionless file transfer functions. Connects to UDP port 69.

**SMTP**

The Simple Mail Transfer Protocol is an Application layer protocol used to transfer e-mail. Connects to TCP port 25.

**POP3/IMAP4**

While SMTP is used to send email, both the Post Office Protocol and the IMAP are used to retrieve e-mail, the main difference between these two protocols is that POP3 can be used to access the "Inbox" folder only, the more complex IMAP4 can be used to access every server-based messaging folder (sent items, deleted items etc) hence eliminates the need for a local repository.

Defined at the Application layer. POP3 connects to TCP port 110, IMAP4 connects to TCP port 143.

**HTTP**

The HyperText Transfer Protocol is an Application layer protocol used for transferring World Wide Web documents but is extensible to transfer other files as well. Connects to TCP Port 80 by default.

**HTTPS**

HTTPS can be used in exactly the same way as the HTTP protocol. The differences are that HTTPS uses a default port number of 443 and that HTTPS uses SSL (Secure Socket Layer) to send data in encrypted form. Instead of connecting to `http://www.techexams.net`, `https://www.techexams.net` would be used.

**TELNET**

An Application layer protocol that provides terminal emulation on TCP port 23 (for example by using the tool with the same name as the protocol: telnet)

**NTP**

The Network Time Protocol is an Application layer protocol used to provide accurate time synchronization in LANs and WANs by synchronizing the time of a computer to reference time source, such as an NTP server, or a radio or satellite receiver or modem. NTP is capable of synchronizing distributed clocks to the millisecond.

Uses UDP port 123.

**ICMP**

The Internet Control Message Protocol is a Network layer protocol that travels in IP packets and is used for sending information and control messages back to the source. One of the most common applications that uses ICMP is the *ping* utility.

Ping is a utility used to determine whether a particular TCP/IP host is reachable; it sends out an *echo request* to an IP address, if the destination is alive and reachable it will send an *echo reply* back to the source, if not then the last router on the path send a Destination Unreachable message to the source host. Echo request and echo reply are two of a set of *message types* ICMP uses to provide/request feedback.

**ARP**

Before two stations in a network are able to communicate with each other, they must know each others physical (MAC) addresses, the Address Resolution Protocol is used to discover an IP address (layer 3) to a MAC address (layer 2). An *ARP request* is broadcasted on the local network to discover the MAC address of the destination host, the station with the correct MAC address responds with an *ARP reply* containing its IP and MAC address.

**RIP**

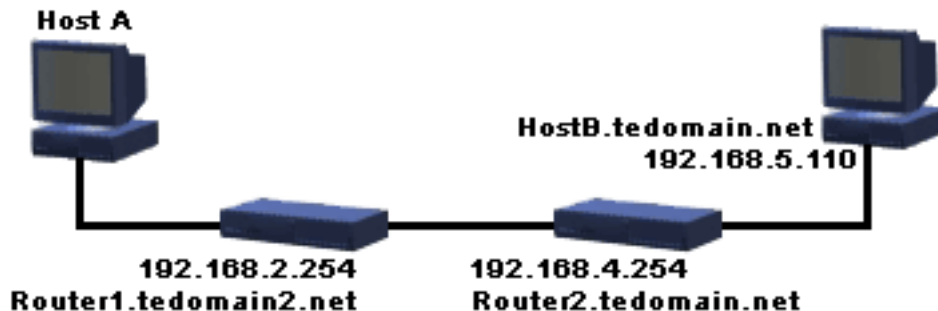
The Routing Information Protocol (RIP) is used to exchange routing information between routers. Each router builds a routing table that contains entries of possible routes in the network and their attributes. When a link to a network goes down, the route to that network, and perhaps other networks that are connected to, become invalid. To inform routers in an internetwork about this change in the network, a routing protocol is used. RIP is typically used in smaller environments. Another example of a more scalable routing protocol is Open Shortest Path First.

## TCP/IP UTILITIES

Note: not all parameter and switches are described in this TechNote, just those of importance for the Network+ exam. If you want more information about a particular utility type use the command with a /? switch. Try these commands on your own PC when you're preparing for the Network+ exam.

### TRACERT

Can be used to trace the path that an IP packet takes to its destination. Tracert uses ICMP Echo packets and their TTL to determine the route and hopcount. In the following network for example:



when a connection between host A and B fails, you can use tracert to find out where the packet stopped.

The following shows the output of running **tracert -d 192.168.5.110** on host A (the -d switch is used to turn off host name resolving which speeds up the tracing):

```

C:\>tracert 192.168.5.110 -d

Tracing route to 192.168.5.110 over a maximum
of 30 hops:

 1      1 ms      3 ms      3 ms    192.168.2.254
 2     40 ms     25 ms     20 ms    192.168.4.254
 3     42 ms     40 ms     27 ms    192.168.5.110

Trace complete.
  
```

Without the -d switch the result would be like this:

```

C:\>tracert 192.168.5.110

Tracing route to 192.168.5.110 over a maximum of 30 hops:

 1      1 ms      3 ms      3 ms    router1.tedomain2.net [192.168.2.254]
 2     40 ms     25 ms     20 ms    router2.tedomain.net [192.168.4.254]
 3     42 ms     40 ms     27 ms    hostb.tedomain.net [192.168.5.110]

Trace complete.
  
```

The target can be either a name or an IP address.

## PING

The ping utility is a diagnostic tool that you can use to test TCP/IP configurations and connections. Use the ping utility to determine whether a particular TCP/IP host is reachable and/or available.

Syntax:

### **PING *target***

where *target* can be either a name or an IP address.

The following shows the output of running the command **ping www.techexams.net**

```
C:\>ping www.techexams.net

Pinging www.techexams.net [216.12.219.37] with 32 bytes
of data:

Reply from 216.12.219.37: bytes=32 time=169ms TTL=238
Reply from 216.12.219.37: bytes=32 time=170ms TTL=238
Reply from 216.12.219.37: bytes=32 time=172ms TTL=238
Reply from 216.12.219.37: bytes=32 time=177ms TTL=238

Ping statistics for 216.12.219.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 169ms, Maximum = 177ms, Average = 172ms
```

Some common situations where PING can be used:

- To verify that TCP/IP has been initialized and is correctly installed and bound to your network adapter card use the ping command with the loopback address (ping 127.0.0.1).
- To verify that the default gateway is available and that the computer can communicate with a remote host through a router by pinging a host on a remote network.
- To verify that DNS host name resolution is available by pinging an existing host name.
- To verify that WINS name resolution is available by pinging an existing NETBIOS name.

## ARP

The ARP protocol is used to resolve an (layer 3) IP address to a (layer 2) Ethernet MAC address.

The ARP utility provides the functionality to modify or display the arp cache table.

Below is an example of output when arp is used with the -a switch to display the displays the IP address to MAC entries currently in the arp cache:

**arp -a**

```
C:\>arp -a

Interface: 192.168.2.2 --- 0x2
 Internet Address      Physical Address      Type
 192.168.2.254        08-00-46-2d-2a-0e    dynamic
 192.168.2.10         00-90-69-42-c6-09    static
```

This command is issued on Host A (referring to the network diagram above). The first (dynamic) entry has been discovered using ARP broadcasts. When Host A (IP address 192.168.2.2) connected to the default gateway (router1) an ARP request with the IP address 192.168.2.254 in it was broadcasted on the network; the node that had the IP address returned its hardware address.

The second static entry has been entered using arp with the -s switch:

```
arp -s 192.168.2.10 00-90-69-42-c6-09
```

An entry can be deleted by issuing the command **arp -d ip address**

## NETSTAT

Displays TCP/IP protocol statistics and information about TCP and UDP connections to and from your computer. Use **netstat -a** to display all the connections and listening ports:

```
C:\>netstat -a

Active Connections

 Proto Local Address           Foreign Address         State
 TCP   cc118442-a:epmap        cc118442-a:0           LISTENING
 TCP   cc118442-a:microsoft-ds cc118442-a:0           LISTENING
 TCP   cc118442-a:1025         cc118442-a:0           LISTENING
 TCP   cc118442-a:1028         cc118442-a:0           LISTENING
 TCP   cc118442-a:2869         cc118442-a:0           LISTENING
 TCP   cc118442-a:3400         cc118442-a:0           LISTENING
 TCP   cc118442-a:3405         cc118442-a:0           LISTENING
 TCP   cc118442-a:3407         cc118442-a:0           LISTENING
 TCP   cc118442-a:3787         cc118442-a:0           LISTENING
 TCP   cc118442-a:5000         cc118442-a:0           LISTENING
 TCP   cc118442-a:3003         cc118442-a:0           LISTENING
 TCP   cc118442-a:3004         cc118442-a:0           LISTENING
 TCP   cc118442-a:3005         cc118442-a:0           LISTENING
 TCP   cc118442-a:netbios-ssn  cc118442-a:0           LISTENING
 TCP   cc118442-a:netbios-ssn  cc118442-a:0           LISTENING
 UDP   cc118442-a:epmap        *:*
 UDP   cc118442-a:microsoft-ds *:*
 UDP   cc118442-a:ntp          *:*
```

Netstat can also be used to display ethernet statistics such as the number of bytes sent and received, as well as any dropped network packets by using the -e switch:

**netstat -e**

```
C:\>netstat -e
Interface Statistics

                Received                Sent
Bytes           9583224                1657344
Unicast packets   11568                11484
Non-unicast packets 66121                302
Discards         0                      0
Errors           0                      181
Unknown protocols 0
```

Note: **netstat -r** will give the same output as the **route print** command.

**NBTSTAT**

Used for troubleshooting network NetBIOS names over TCP/IP resolution problems. It displays protocol statistics and current TCP/IP connections that are using (NBT) NetBIOS over TCP/IP as well as the NetBIOS name table and cache.

To display the NetBIOS name table of the local computer use nbtstat with the -n switch. The status of *Registered* indicates that the name is registered either by broadcast or with a WINS server. If two hosts on the local network would use the same NetBIOS name, the status would be *Conflict*.

**nbtstat -n**

```
C:\>nbtstat -n
RealTEk:
Node IpAddress: [212.204.175.76] Scope Id: []

                NetBIOS Local Name Table

-----
Name                Type                Status
-----
HOSTA                <00>                UNIQUE              Registered
WORKGROUP            <00>                GROUP               Registered
HOSTA                <03>                UNIQUE              Registered
HOSTA                <20>                UNIQUE              Registered
WORKGROUP            <1E>                GROUP               Registered
WORKGROUP            <1D>                UNIQUE              Registered
HOSTB                <00>                UNIQUE              Registered
HOSTB                <03>                UNIQUE              Registered
HOSTB                <20>                UNIQUE              Registered
..__MSBROWSE___.    <01>                GROUP               Registered
```

To display the NetBIOS name table of a remote computer use one of the following syntaxes:

**nbtstat -a remotename**

or

**nbtstat -A IPaddress**

To display the contents of the local computer NetBIOS name cache, type:

**nbtstat -c**

Use **nbtstat -r** to display to verify NETBIOS names are correctly resolved by WINS:

```
C:\>nbtstat -r

NetBIOS Names Resolution and Registration Statistics
-----

Resolved By Broadcast          = 1
Resolved By Name Server       = 40

Registered By Broadcast       = 14
Registered By Name Server     = 11
```

## IPCONFIG

(Windows NT, 2000, XP)

Displays TCP/IP configuration information and renew and release DHCP assigned address configuration.

When the **ipconfig** command is issued without any options the output will be similar to the one below:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter RealTEk:

    Connection-specific DNS Suffix  . : tedomain.net
    IP Address. . . . .               : 192.168.2.2
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.2.254
```

**ipconfig /all** display full configuration information, for example:

```
C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : hosta
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter RealTEk:

Connection-specific DNS Suffix: tedomain.net
Description . . . . . : Realtek RTL8029(AS) PCI Ethernet Adapter
Physical Address. . . . . : 00-50-BF-61-6C-71
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . : Yes
IP Address. . . . . : 192.168.2.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.254
DHCP Server . . . . . : 192.168.2.194
DNS Servers . . . . . : 192.168.2.194
                        192.168.2.195

Lease Obtained. . . . . : Wednesday, January 15, 2003 10:08:41 PM
Lease Expires . . . . . : Wednesday, January 22, 2003 1:36:52 PM
```

Use **ipconfig /release** release the IP address configuration.

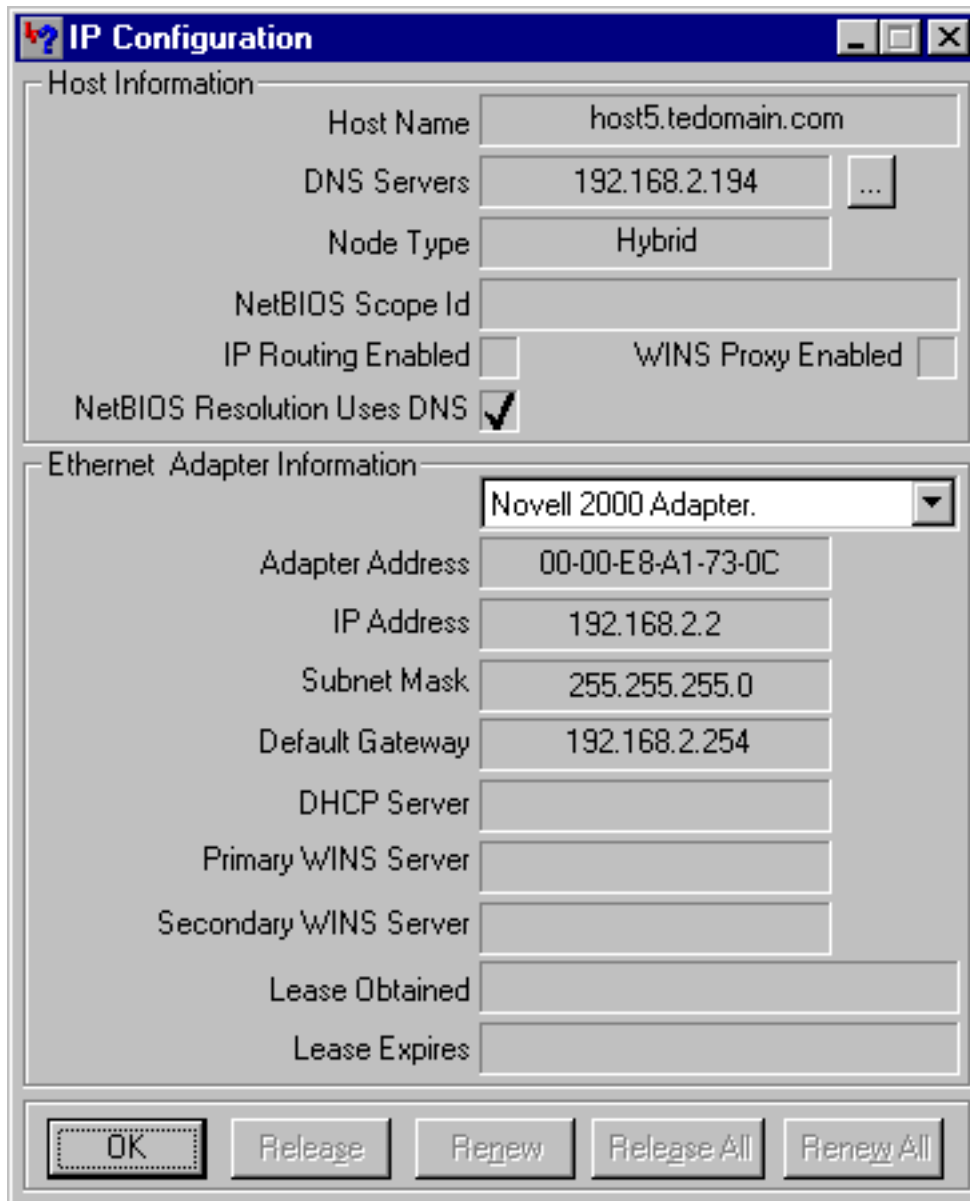
Use **ipconfig /renew** Renew the IP address configuration.

The ipconfig command component has more option than those decribed above, especially in Windows 2000/XP but are beyond the scope of the exam.

**WINIPCFG**

(Windows 9x, ME)

Displays TCP/IP configuration information and renew and release DHCP assigned address configuration.



The screenshot above shows the configuration of an ethernet adapter with a manually assigned IP address configuration. When the configuration is automatically assigned by a DHCP server the buttons at the bottom would be enabled allowing you to perform the same tasks as with the ipconfig command.

Note that winipcfg is available only on Windows 9x/ME and ipconfig is available on Windows 9x/ME and Windows NT, 2000, XP.

## NSLOOKUP

Displays information that you can use to diagnose Domain Name System (DNS) servers and to send DNS queries to DNS servers. Nslookup can be used in interactive (use the nslookup command without options to enter a text based console where you can use several sub commands to diagnose DNS), and non-interactive mode (providing the parameter directly on the command-line.)

Here's an example of the results of running nslookup www.techexams.net (non-interactive mode)

```
C:\>nslookup www.techexams.net
Server: proxy1.tedomain.net
Address: 212.120.66.194

Non-authoritative answer:
Name: www.techexams.net
Address: 216.12.219.37
```

You can use a different DNS server by adding the hostname or IP address of another DNS server, for example:

**nslookup www.techexams.net ns2.tedomain.net**

## NETWORK SERVICES

### DHCP/bootp

*DHCP* is short for *Dynamic Host Configuration Protocol*. This service is used in TCP/IP networks to provide automatic IP address configuration for network hosts. It is typically installed on a server, but some routers are able to run DHCP as well. DHCP significantly simplifies administration and ensures every host will use a unique IP address as required.

When a client configured to use DHCP boots for the first time, it will use the bootp protocol to request a DHCP server to issue an address. This *lease* process goes as follows:

1. The client sends out a *DHCPDiscover* broadcast message to request IP addressing info from a DHCP server.
2. One or more DHCP servers respond with a *DHCPOffer*, containing an IP address and other IP addressing info such as subnet mask and default gateway. The first *DHCPOffer* received is used.
3. The client responds with a *DHCPRequest*, a broadcast message containing the IP addressing information again to make sure it is still available and can be used.
4. The server responds with a *DHCPAck* (Acknowledge) and the optional configuration, such as DNS and WINS servers, if the address is still available, and the client can start using it. Or, the DHCP server responds with a *DHCPNak* (Negative Acknowledge) when the IP address is not available anymore forcing the client to start the lease process all over again.

When 50% of the lease period has expired the client will try to renew the lease for the same IP address. If this fails, the client will try again at 87.5%. When a DHCP client isn't able to locate a DHCP server, during the initial configuration or after the lease renewal attempt, the client will be configured with an IP address of 0.0.0.0. In case the client uses Automatic Private IP Addressing (APIPA), it will be configured with an IP address from the network 169.254.0.0, with the subnet mask 255.255.0.0.

DHCP Server listen to UDP port 67, and clients to UDP port 68. Routers typically do not forward UDP broadcasts, hence every subnet requires its own DHCP server. To overcome this limitation, the router can be configured to forward UDP port 67 and 68 broadcasts, or a DHCP relay agent can be installed in subnets without DHCP servers. The DHCP relay agent can be either a client or a server, it picks up DHCP broadcasts and forwards it to a DHCP server in another subnet, which responds to the DHCP relay agent, which in turn forwards the information to the DHCP client that has sent the original broadcast. In other words, the DHCP relay agent acts as an intermediate between a DHCP client in one subnet and a DHCP server in another subnet.

Besides and IP address and subnet mask other IP addressing options are also typically issued by a DHCP server. Addressing options include:

- Default gateway
- DNS servers
- WINS servers

Besides for DHCP, the Bootp protocol is also used for *bootstrapping*. Bootstrapping allows a diskless client to boot from the network by loading the operating system from a central server.

## **Name Resolution**

Compared to TCP/IP networks, most telephone systems are rather dumb; in general when you want to call someone you have to dial an x-digit number. In TCP/IP networks you can contact an intended communication partner by using a name instead of having to know an address for every computer you want to contact. For this, there has to be something to resolve the name to an IP address, the two main services taking care of this are DNS and WINS.

## **DNS**

Today's primary naming system in corporate networks and the naming system used on the Internet is the *Domain Naming System (DNS)*. The primary function of DNS is to resolve *host names* to IP addresses and vice versa. A DNS server maintains a hierarchical database/directory, which contains a zone for each domain. Records are created in a zone to map host names of individual resources to IP address. Following are some common example of resource records:

- A** This is the *hostb* part in the FQDN above and maps a host name to an IP address.
- CNAME** This is an alias for a A record, for example the *www* part in *www.tedomain.net* could actually be an alias for *host11.tedomain.net*, and *mail.tedomain.net* and *ftp.tedomain.net* might be the same host as well.
- MX** This name maps to the IP address where email for this domain should be send to, for example *mail.tedomain.net*
- PTR** A pointer record allows an IP address to be resolved to a host name.

A host name is actually a part of a 'larger' name, called a Fully Qualified Domain Name (FQDN). Here's an example of a FQDN:

hostb.tedomain.net

This name consists of three parts read from right to left:

*net* is the top-level domain

*tedomain* is the second-level domain

*hostb* is the host name.

When a client wants to communicate with another host by using its host name *hostc.techexams.net*, it connects to UDP port 53 on the DNS server and requests the IP address. If the zone for the domain *techexams.net* is located on the DNS server it will reply with the IP address. If the zone is located on another DNS server, on the Internet for example, the DNS server can forward the request and act as an intermediate between the client requesting the IP address and the DNS server hosting the record.

The HOSTS file is the local, static equivalent and predecessor of DNS. It is a text file that contains IP address to host name mappings. It originated on UNIX but can be used on Windows OS clients and servers as well.

Following is example content of a HOSTS file:

```
102.54.94.97 server1.tedomain.net # source server
38.25.63.10 server2.tedomain.com # x client host
127.0.0.1 localhost
```

On Windows NT, 2000 and XP systems the file is located in the C:\WINDOWS\system32\drivers\etc folder. On Windows 9x the file can be found in the C:\WINDOWS\ folder.

## WINS

The *Windows Internet Naming System (WINS)* was the primary naming system in Microsoft networks before Windows 2000. WINS maps *NETBIOS* names to IP addresses. Read the [NETBEUI/NETBIOS TechNotes](#) for more information about NETBIOS names.

When a station without access to a WINS server uses a NETBIOS name to contact another station, the station will send a broadcast to discover the name of its intended communication partner, and the station with the correct name will respond with its IP address. To reduce broadcasts on the network, clients can be configured to use a WINS server so they will register their names at the WINS server at startup and send queries to discover IP addresses of NETBIOS names directly to the WINS server instead of generating broadcasts.

Besides the fact that WINS is used for NETBIOS names to IP address name resolution, and DNS for host name to IP address name resolution, the main difference between DNS and WINS *used to be* that the WINS database is dynamic and DNS was static. WINS clients register and update their own records (although you can also add static entries to a WINS database). But although the DNS servers on the Internet are still static, DNS in Windows 2000 networks can also be dynamic. WINS is used heavily in Windows NT 4 networks.

The LMHOSTS file is the local, static equivalent and predecessor of WINS. It is a text file that contains IP address to NetBIOS name mappings. It originated on Lan Manager (Microsoft's OS before Windows) but can be used on Windows OS clients and servers as well. Following is a sample entry of a LMHOSTS file:

```
102.54.94.97 teserver1 #PRE #DOM:tedomain
```

On Windows NT, 2000 and XP systems the file is located in the C:\WINDOWS\system32\drivers\etc folder. On Windows 9x the file can be found in the C:\WINDOWS\ folder. Note that the file is called lmhosts.sam by default, you will need to create a new file or rename the sample file (thus remove the .sam extension) before you can use it.

## NAS

*Network Attached Storage (NAS)* is a file server that runs on a specialized device directly connected to the network. It is typically a box that contains several hard disks combined in a RAID set.

NAS is directly attached to an Ethernet network providing access through a 10Mbps, 100Mbps, or 1Gbps connection. Many NAS devices are based on Linux or Unix derivatives and are usually easily installed, and configured and managed using a web browser. It can communicate with the network using TCP/IP, IPX/SPX, NetBEUI or AppleTalk even. The primary advantage of this wide variety of supported protocols, is that Windows, UNIX/Linux, MacOS, and Novell clients, can all use the same storage and can access and share the same files. Following is a list of operating systems and the file access protocols they use to access files on a NAS device:

- Windows systems access files using either Server Messenger Block (SMB) or Common Internet File System (CIFS).
- Unix/Linux systems access files using the Network File System (NFS)
- Novell systems access files using the Netware Core Protocol (NCP)
- Apple systems access files using AppleShare

In addition to these protocols most NAS devices also support file access through HTTP, and often optional, FTP as well.

Do not confuse NAS with *SAN (Storage Area Network)*. The difference is that SAN is not a just a device, but refers to a complete network configuration where servers use central storage connected through fiber optic cabling or SCSI. Instead of being an autonomous device, the file system is dictated by the operating system running on the servers. SAN is commonly used in combination with *clusters*.

## SNMP

The Simple Network Management Protocol (SNMP) is included in the Network Services TechNotes because it is much more than 'just' a protocol. SNMP is an application layer protocol that is primarily used to monitor, and gather information about, network systems and devices. An SNMP *agent* is installed on a *managed device* to send SNMP information to a central *Network Management System (NMS)*. On the NMS the information is stored in a *Management Information Base (MIB)* which can be used to produce graphs, reports, base-lines and other useful overviews of the network.

Following are 3 of the basic commands supported by SNMP:

**Read** In case of gathering information a *read* can be send to an agent to provide information about a managed device.

**Trap** A trap messages is send from the agent to an NMS when a certain event occurs. When a service on a server stops running, for example.

**Write** Besides passively monitoring and gathering information, SNMP can also be used to 'manage' a network by configuring managed devices using a write command.

SNMP agents listen and respond to UDP port 161, trap messages are send to UDP port 162. Besides operating over UDP and IP, SNMP can also be used in IPX and AppleTalk networks.

## REMOTE ACCESS & SECURITY PROTOCOLS

### REMOTE ACCESS SERVICES (RAS)

RAS is originally a service which can be installed on Microsoft's Windows NT to allow remote clients to dial-in and connect to the network, logon to the domain and act as if they were locally connected to the network. Nowadays the acronym RAS is used to define many types of remote dial-in solutions. Typically when a client dials-in DHCP is used to configure the client's IP addressing.

### POINT-TO-POINT PROTOCOL (PPP)

PPP is today's most commonly used RAS protocol and is supported by virtually every operating system as it is part of the TCP/IP suite. Besides point-to-point dial-up connections over POTS and ISDN, PPP is also often used for router-to-router connections in WANs. PPP operates at the Network layer of the OSI model and consists of two types of control protocols:

**LCP** - The *Link Control Protocol* establishes, configures, maintains, and terminates the point-to-point connection.

**NCP** - *Network Control Protocols* exist for various upper-layer Network protocols such as IP, IPX, AppleTalk and NetBEUI, and are used to encapsulate the upper-layer protocols' data and transfer it over the link created by the LCP. Multiple protocols, such as IP and IPX, can use the link at the same time.

PPP supports several security protocols including MS-CHAP, EAP, the older Password Authentication Protocol (PAP) and the common Challenge Handshake Authentication Protocol (CHAP) for authentication purposes. PAP sends user credentials in clear text and CHAP provides a more secure, encrypted, method of authenticating users. After the remote user is authenticated the PPP connection is rather insecure, because the data itself is not encrypted. Several other protocols are available to encrypt the transmitted data and/or the authentication process which are discussed later on.

A very useful extension to PPP is Multilink PPP, this allows multiple physical connections to be combined in one logical connection, this is often use to bundle the 2 B-channels in ISDN BRI.

PPP is the successor of SLIP, an older dial-up protocol, used primarily in Unix environments and still supported by some ISPs, major differences with PPP is that it lacks authentication, compression and multilink capabilities.

## VIRTUAL PRIVATE NETWORKS (VPN)

A VPN is a private connection over a public network such as the Internet. This can be a connection between two LANs located in different states, using the Internet as the transport mechanism as depicted in the diagram below.



Another common implementation of a VPN is between a remote dial-up client and a corporate LAN. The client connects to the corporate LAN via the Internet. When the connection is established a virtual encrypted *tunnel* is created, allowing secure communication. VPNs can save a company a lot of money because they can use the, often existing, Internet connections instead of implementing expensive point-to-point connections, such as ISDN and T1. Two of the common tunneling protocols used to create VPNs are described below.

## POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

PPTP is a tunneling protocol created primarily by Microsoft. It is an extension of the PPP, and encapsulates PPP packets to transfer them through an encrypted tunnel, over IP networks only. The protocol being tunneled through the public IP network can be IP, but also IPX, AppleTalk and other protocols supported by PPP. PPTP clients connect to TCP port 1723.

## LAYER 2 TUNNELING PROTOCOL (L2TP)

Another common but newer tunneling protocol is L2TP, which will probably replace PPTP because it is considered to be more secure and supports tunneling through other types of networks than just IP. L2TP is the result of combining the technology of Cisco's Layer 2 Forwarding (L2F) tunneling protocol with PPTP. L2TP is used to encrypt traffic over various types of point-to-point networks including IP, Frame-Relay, X.25 and ATM. The protocol being tunneled is always IP. To provide a (relatively) real secure connection, L2TP is often used in combination with IPsec. L2TP clients connect to UDP port 1701.

## IPSEC

IPsec is an encryption protocol for IP networks providing another level of end-to-end security at the Network layer. The sending and the receiving computer negotiate a key to use to encrypt the traffic, during the duration of the connection this key is renewed frequently. IPsec is often used in conjunction with tunneling protocols to offer a higher level of security in VPNs.

In addition to VPNs, IPsec is also commonly used in LAN environments for client/server connections, router to router connections in WANs, and for secure RAS connections. A main advantage of IPsec is that it is transparent to the user and can be easily implemented, and today's modern operating systems support it natively, including Windows 2000.

IPsec can operate in two different modes:

- *Transport Mode* encrypts the IP payload only (the data you transfer).
- *Tunneling Mode* encrypts IP payload and the IP message headers.

## **SECURE SOCKET LAYER (SSL)**

SSL is a protocol, developed by Netscape, that provides security at higher levels in the OSI model by using a public key to encrypt the session between a client and a server and to identify the server to the client (and optionally the client to the server). The server is usually a web server; the most common use of SSL is HTTPS, which is similar to the HTTP but uses SSL to encrypt the traffic. A main difference with IPsec is that IPsec can be used to protect any IP connection and SSL can only be used if the application supports it, such as a web browser. SSL uses either TCP or UDP port 443.

## **KERBEROS**

Kerberos is a secure authentication protocol. In a Kerberos environment a centralized authorization server, called the Key Distribution Center (KDC), issues a ticket to a client when it logs on, this ticket is used to authorize the user (or a system) when it tries to access a resource such as a share, printer, intranet application, database, anything that support Kerberos. The advantage of this is that it can be used to provide single sign-on capabilities for users in large heterogeneous network environments, when a user logs on to the network the user will be authenticated automatically for every resource or application he or she will try to access, without having to enter a username and password again and again. Kerberos uses TCP and UDP port 88.

## **ICA**

The Citrix Independent Computing Architecture (ICA) protocol is used for remote connections to advanced terminal servers such as Citrix Metaframe. A client will be able to run all kinds of applications on the terminal server, the ICA protocol is used to transfer the screen output back to the client and mouse and keyboard input from the client to the server. This would allow a computer with a minimal configuration, for example a 486, to run Office 2000 or other applications that would normally not run on the computer due to hardware limitations. It's like connecting dozens of keyboards, mice and monitors to a single computer using a network connection and allowing multiple users to use different applications, in their own private workspace on the server, at the same-time.

## NETBEUI and NETBIOS

NETBios Extended User Interface is a non-routable Transport layer protocol created by Microsoft. Novell and Microsoft wanted to use the Session layer part of the Netbios protocol with other transport protocols such as TCP and SPX and decided to split up NetBios in NetBEUI and NETBIOS.

The reason it is non-routable is in its *flat* addressing scheme, NETBEUI uses *Netbios* names to identify computers on the network, that do not contain a network portion. Netbios names are sometimes referred to as *friendly names*. NetBIOS names are 16 characters in length and cannot contain any of the the following characters: \ / : \* ? " < > |

The first 15 characters represents a unique name identifying a resource, the 16th character (if you would set a name of 8 character it is padded with spaces up to 15 characters long to allow a '16th' character) is a suffix identifying the type of resource or group of resources, for example the redirector, server, or messenger services can be installed on one computer resulting in three times the same name but with different suffixes.

NETBEUI is a broadcast protocol, meaning a computer running NETBEUI discovers the MAC address from the intended communication partner by sending out a broadcast with the NETBIOS name. The main advantage of NETBEUI is that it is small in size and easy-configurable.

## NETWARE OS & PROTOCOLS

### Novell Netware

Netware was developed by Novell in the early 1980s and is based on the Xerox Network System. It is a Network Operation System (NOS) that allows file and printer sharing and mail functionality using a client-server architecture. Netware used to be very popular, and can still be found in many corporate networks today. Before we go to the important part, the Netware protocols, first some common Netware items:

In Netware version 4, Novell introduced the *Netware Directory Services (NDS)*, which allows network resources to be grouped together and organized in a hierarchical way, so they can be easily located and administered. NDS uses the same concept as Microsoft's Active Directory. Before version 4, Netware clients needed to be configured with a *preferred server* to handle the logon authentication request, Netware clients version 4.x and up need to be configured with a *Tree* and *Context*. NetWare operating systems prior to NetWare 4 relied on the *bindery*. The NetWare bindery kept server-specific user and group information in a flat file which every network server maintained independent of the bindery on other servers, hence there was no relationship between objects. The bindery relied heavily on the Service Advertising Protocol to advertise its resources to clients.

A once very popular version of Netware, was 3.12, which became millennium proof with version 3.2.

*Netware Loadable Modules (NLMs)* are software modules that can be added to a Netware server installation to provide additional functionality.

*NWLINK* is Microsoft's implementation of IPX/SPX which allows Windows clients to communicate with Netware servers.

*GroupWise* is a popular groupware server and client that provides email and other groupware services, similar to a combination of MS Exchange Server and Outlook.

### Netware Protocol Suite

Although current versions of Novell Netware use TCP/IP, before Netware version 5, IPX was *the* protocol in Netware networks. It is a small and easy to implement routable protocol developed by Novell and based on the Xerox Network System. The Netware protocol suite is a suite of several protocols for different functions, the most important being IPX and SPX. IPX is similar to the Internet Protocol from the TCP/IP suite, it is a connectionless Layer 3 (Network layer) protocol used to transfer datagrams between hosts and networks. SPX is the Transport protocol used to provide reliable transport for IPX datagrams, similar as TCP does for IP. IPX/SPX networks support a maximum of approximately 300 hosts per segment. Next, we will further outline the Netware protocols in correlation to the 7-layer OSI model. Netware protocols and services are defined at the 5 upper layers, but Novell created their own version of an Ethernet frame format for the Data Link layer (Layer 2) as well. Besides Ethernet, IPX/SPX can run over a variety of network technologies such as Token Ring, FDDI and PPP WAN connections.

This frame format is known as the frame type, which refers to the format of the layer 2 frame, in which the IPX packet is encapsulated when it flows down the OSI model. The frame types of two Netware hosts must match to enable communication without a router. IPX can use several frame formats, of which the two most important are listed in the following table.

Frame Format	Frame Type	Netware Versions
Novell 802.3 raw	802.3	Default frame type for Netware 3.11 and earlier. Supports only IPX/SPX as the upper layer protocol
IEEE 802.3	802.2	Default frame type for Netware 3.12 and 4.x. The main difference with Novell's 802.3 format is the addition of LLC field, which specifies the upper-layer protocol, such as IPX or IP.

At the Network layer, 4 key protocols are defined:

Internet Packet Exchange (IPX)	A connectionless datagram protocol providing best-effort delivery and layer 3 addressing. Similar to the function of IP.
Netware Routing Information Protocol (RIP)	Allows IPX routers to exchange information and build their routing tables. The routing tables contain entries of possible routes in the network and their attributes. Netware RIP routers broadcast their routing table to neighboring routers every 60 seconds.
Netware Link-State Protocol (NLSP)	A more advance routing protocol with the same purpose as RIP, but typically used in larger IPX internetworks.
IPXWAN	Used to negotiate options for an IPX link when a new physical connection is established.

At the Transport layer *the* transport protocol in Netware networks is defined:

Sequenced Packet Exchange (SPX)	A connection-oriented protocol providing reliable transport services for the delivery of IPX datagrams. Similar to the function of TCP.
---------------------------------	---

At the Session layer, the next 3 protocols are defined:

Service Advertising Protocol (SAP)	Used by network resources such as file and print servers to advertise the services they provide and at which IPX address they can be reached. This occurs every 60 seconds. SAP is mainly used in Netware networks before version 4. In Novell Netware version 4 and above network resources are typically located using the NDS.
NetBIOS	Although not really a Netware protocol, Novell adapted this protocols to allow NetBIOS communication between a Netware server and Windows clients.

A key part of Novell Netware networking is the Netware Core Protocol (NCP). This protocol operates on the upper three layers of the OSI-model, and provides services to client redirectors such as the Netware Shell. Services include file and printer access, security and name services.

Some of the most important Application layer services are the Message-Handling Services (MHS), a simple electronic messaging system, and NDS, Novell's directory services.

## IPX Addressing

A complete IPX network address is 80 bits in length and is represented in a hexadecimal format. As with all routable protocols it needs a network and a host portion, the network portion is 32 bits in length and is manually configured. The host portion is 48 bits in length and is derived from the MAC address of the host's network interface.

Examples of full IPX internetwork addresses are:

- 0CC001D8.0050.BF61.6C71
- 0000ABBA.0060.9736.954B
- 00000046.0060.E92A.C2A4

Data send to an address of which the network portion is 0 (zero), is meant for the local network. Hence, this number cannot be used when configuring network addresses. The IPX broadcast address is FFFFFFFFFF.

To identify an unique connection when multiple processes are communicating over IPX addresses can also include a *socket*, which is a 16-bit number appended at the end of the IPX address, for example: 0CC001D8.0050.BF61.6C71.322

Every Netware host that provides server services, such as a Netware server or MS NWLINK client sharing resources, or those that act as a router, needs an *internal network number*. This is a logical IPX address that is not present on the physical network, only inside the server.

## AppleTalk

AppleTalk was developed by Apple Computers in the early 1980s to allow file and printer sharing and mail functionality between Macintosh computers. A Mac that shares resources is called a server, and the computer connecting to it a client. Like TCP/IP, AppleTalk is not just one protocol, but a suite of several protocols for different functions. It is built-in in every Macintosh computer and requires virtually no user interaction, therefore it is very easy to administer in small network environments. As with any other protocol, AppleTalk is best explained in correlation to the 7-layer OSI model.

At the Physical and Data Link layer several specifications are defined to allow AppleTalk to run over several network types with different media-access technologies. EtherTalk allows AppleTalk to run over Ethernet, TokenTalk allows AppleTalk to run over Token Ring, FDDITalk allows AppleTalk to run over FDDI, and LocalTalk is Apple's own media-access technology. LocalTalk uses UTP or STP cabling and has a maximum data transfer rate of 230 KB, you can still find this in today's networks, typically in very small environments for simple file and printer sharing. The image below shows a connector used in LocalTalk networks to connect network nodes. At one side it connects to a computer or printer using a min-din connector or DB-9 serial connector. The other side connects to a phone cable, which in turn, connects to another LocalTalk connector or a terminator. This type of media is known a *PhoneNet*, and is similar to building a 10Base2 bus network topology.



At the Network layer, two main protocols are defined:

Datagram Delivery Protocol (DDP)	A connectionless datagram protocol providing best-effort delivery and layer 3 addressing. Similar to the function of IP.
AppleTalk Address Resolution Protocol (AARP)	Maps (Network) layer 3 addresses to (Data Link) layer 2 MAC addresses. Analogous to the function of the ARP protocol in TCP/IP.

At the Transport layer a big difference with the TCP/IP suite becomes noticeable. In TCP/IP the routing protocols are defined at the Network layer, with AppleTalk this is not the case:

Routing Table Maintenance Protocol (RTMP)	Allows AppleTalk routers to exchange information and build their routing tables. The routing tables contain entries of possible routes in the network and their attributes. RTMP is the equivalent of the Routing Information Protocol (RIP) typically used in TCP/IP networks.
---	---

---

AppleTalk Update-based Routing Protocol (AURP)	Allows AppleTalk networks to be connected over a TCP/IP WAN link. AURP wraps AppleTalk datagrams into UDP datagrams allowing them to be tunneled over IP connections.
AppleTalk Echo Protocol (AEP)	Used to verify if remote hosts are reachable. This is similar to ICMPs Echo messages used by the PING utility in TCP/IP networks.
AppleTalk Transaction Protocol (ATP)	This is the transport protocol in AppleTalk. Provides reliable delivery service for transaction-oriented operations. ATP handles acknowledgements, flow control and sequencing.
Network Binding Protocol (NBP)	Maps AppleTalk names to AppleTalk network layer addresses. This protocol is largely responsible for the large overhead on AppleTalk networks because of the broadcast method it uses. NBP is somewhat similar to DNS and WINS in TCP/IP.

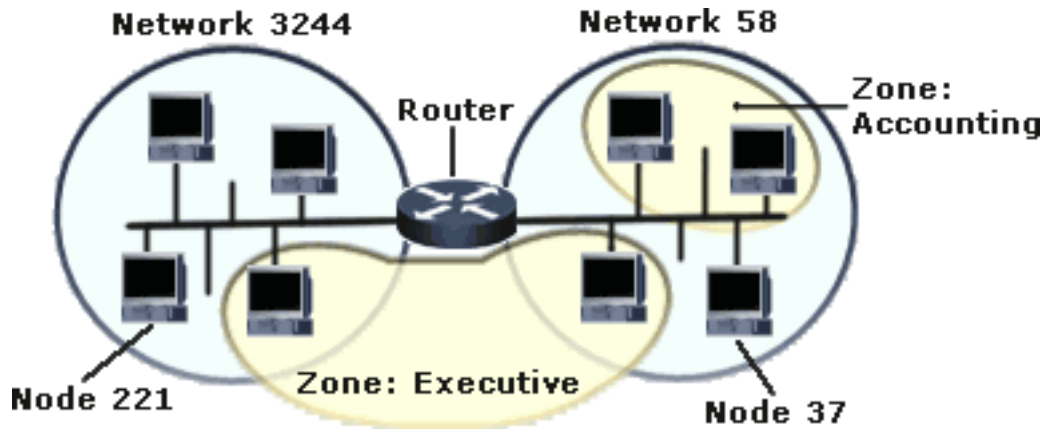
At the Session layer, the next 4 protocols are defined:

Printer Access Protocol (PAP)	A protocol created for client to printer communication, which manages the virtual connection to printers and print servers.
AppleTalk Data Stream Protocol (ADSP)	Provides a data channel between hosts. It is a full-duplex, connection-oriented protocol that provides its own transport layer services (therefore ADSP functions reside partly on OSI's Transport layer)
AppleTalk Session Protocol (ASP)	A Session protocol that manages sessions for higher layer protocols and uses the AppleTalk Transaction Protocol (ATP) for transport services.
Zone Information Protocol (ZIP)	Manages the relationship between network numbers and zone names and allows applications to use zones.

At the Presentation *and* Application layer the AppleTalk Filing Protocol (AFP) is defined. AFP provides an interface between an application and a file server. AFP allows a workstation on an AppleTalk network to access files on an AFP file server, such as an AppleShare file server. When the user opens a session with an AppleShare file server over the network, it appears as if the files were located on a local disk drive.

## AppleTalk Addressing

The following network diagram shows an example of a simple AppleTalk network using EtherTalk:



An AppleTalk network consists of three main components:

Nodes	A uniquely identified host on the network, includes Macintosh computers, printers, Windows PCs and routers.
Networks	Multiple network numbers can be assigned to a single segment, known as an <i>extended cable range</i> .
Zones	Similar to the concept of VLANs, they are used to control broadcast traffic by dividing <i>internetworks</i> into logical groups. When a client request resources such as shares and printers, only those in the same zone of the client, will appear by default.

An AppleTalk address is 24 bits in length and as with all routable protocols needs a network and a host portion. The first 16 bits denote the network portion of the address, and is learned automatically from an AppleTalk router or computer. The other 8 bits denote the *node* portion. When a client is added to the network, it will make up the node portion itself and broadcasts requests to see if the number is already in use. If the number is in use, the client will generate a new number and start over again until an unused node number is found. The complete AppleTalk network address of node 37 is 58.37. The 16 bits network portion allows for 65000 networks and the 8 bits node portion allows for 254 hosts (0 can't be used, 255 is the broadcast address). The current version of AppleTalk is named AppleTalk phase 2, allowing multiple network numbers to be assigned to a single segment, known as an *extended cable range*, and eliminates the limit of 254 nodes per network. Sometimes the address includes the socket number, for example 58.37.254 or 58.37/254. An AppleTalk socket is similar to the concept of ports in TCP/IP.

Using the Network Binding Protocol's services, AppleTalk objects can be named. AppleTalk names consist of a object, type and zone field, where each of these three parts are limited to 32 characters in length. An example of a printer name could be:

Finance1:LaserWriter@Executive, where *Finance1* is the name configured for the object, *LaserWriter* the object type, and *Executive* the zone name.

## MAC OS

The current operating system running on Macintosh computers is MAC OS X and supports TCP/IP. Macintosh computers are often used for graphical and other multimedia related purposes. MAC OS runs only on Macintosh computers, not on general x86 based machines. Mac OS X uses an access permission system based on a UNIX. Every file and folder on a hard disk has an associated set of permissions that determines who can do what. The three types of permissions are Read (r--), Write (-w-), and Execute (--x).

## UNIX/LINUX

### UNIX

UNIX is a multi-tasking, multi-user, server and client, text-based operating system. In a typical UNIX network, dumb terminals are connected to a centralized server. It's like connecting several monitors and keyboards to the same computer. In more modern networks where UNIX systems co-exist with other operating systems such as Windows, clients usually use a terminal emulator (such as TELNET) to access the server, or other specialized software.

Every user executes programs and stores files on the same system, allowing them to share resources in real-time. There are many different UNIX variants (Linux, Solaris, SunOS, HP-UX, Digital UNIX, SCO Open Server, DG-UX, UNIXWARE, AIX, BSDI, NetBSD, NEXTSTEP, A/UX, to name a few.), which run on differing type of hardware, from regular PCs to large mainframes. Unix variants are also used in telecommunication systems and many other devices. It is a operating system "developed by programmers for programmers", making it rather complex to manage, but because it is powerful and stable it is used in many different types of environments such as hospitals, academia and many corporate networks.

TCP/IP is the native protocol in UNIX networks. The HOSTS file and DNS originated on UNIX. Those who have experience with UNIX will notice the *etc* directory as the location of the HOSTS file on Windows NT/2000/XP.

The Network File System (NFS) is also an important part of UNIX networking, it allows a UNIX machine to mount a directory (share) on a remote computer and treat it as part of the local file system. The main drawback of NFS is that it is not secure.

Every file and folder in UNIX has an associated set of permissions that determines who can do what. The three types of permissions are Read (r--), Write (-w-), and Execute (--x).

SAMBA was developed to provide Service Message Block (SMB) communication between Windows and UNIX. SMB is similar to NFS and is used primarily in Windows NT network. SAMBA allows a UNIX server to participate in a Windows NT domain, so UNIX shares and resources show up in the Network Neighborhood of clients. Newer versions of SAMBA can also process logon requests for clients in a Windows NT domain environment, hence act as a domain controller.

Besides centralized applications and storage, UNIX provides advanced printer sharing. The LPD/LPR are the printing protocols used in cross-platform IP networks, and originated on UNIX. With LPD/LPR you can print from a UNIX, MAC, or Windows workstation to a print server. The *line printer daemon* (LPD) is the print server, (i.e. a UNIX server or a printer). And the *line printer remote* (LPR) is the client part.

## **LINUX**

Linux is an *open source* operating system that is similar to UNIX. Open source means that its source code is available to the public, allowing everyone to create extension, utilities, GUIs, software and more. Partly because of this, there are many different distributions of Linux, of which most are free. Linux is very popular at web hosting companies, most of the web servers on the Internet today run a Linux or a Linux-like OS. Besides acting as a HTTP, FTP or mail server, Linux is also often used for firewalls and proxy servers. Every PC with a 386DX CPU or higher can run Linux. In addition to using Linux on servers, Linux can also be used as a workstation. A variety of GUIs are available to make it all a bit more user-friendly.

## **FAULT TOLERANCE AND DISASTER RECOVERY**

### **FAULT TOLERANCE**

Fault tolerance refers to software or hardware options that allow a system to continue operating in case a particular component fails. Following are some of the most common fault tolerant configurations.

#### **Redundant network connections**

A faulty network interface card or cable can prevent an entire server from being able to provide its services to users. To prevent a NIC, and the connection, from being a single-point of failure for the entire server, an extra NIC can be installed. These NICs can be combined to provide *load-balancing* and/or fault tolerance.

#### **Mirrored servers**

A more advanced solution is to mirror complete servers, also known as clustering. A cluster contains 2 or more *nodes* (servers). If a node fails another node will take over its duties. This process is known as *fail-over*. In modern configuration the nodes connect to a shared storage device using fibre optic cabling. Some editions of Windows 2003 support up to 8 *nodes* in a *cluster*.

### **RAID**

RAID stand for Redundant Array of Inexpensive (or Independent) Disks, and is commonly used on servers in corporate environments. It allows multiple hard disks to be combined. The three most common, and important for the Network+ exam, are described next.

*RAID 1* refers to Disk Mirroring/Duplexing. This configuration requires two, in some cases identical, hard disks. When the OS writes data to the hard disk, the same data is also written to the mirrored disk. This may slow down write performance, but increases read performance since data can be read from both disks at the same time. It's called *duplexing* when each disk has its own hard disk controller, providing an extra level of redundancy. When a disk fails the other disk can continue to operate, in some configurations this process occurs entirely automatically. In Window NT and higher, when the main disk fails, you'll need to manually configure the system to use the mirrored disk.

*RAID 5* is more advanced and requires at least 3 hard disks. RAID 5 is also known as a *stripe set with parity*. When data is written to the RAID 5 set, it is distributed over several disks, and parity information about data blocks on one disk are stored on the other disks. In case of a disk failure, the parity information can be used to reconstruct the data which was on the missing disk. Because data is spread out over several disks, RAID 5 offers better read performance than single or mirrored disks. But because every write requires the parity calculation, write performance can be slower, especially when RAID 5 is implemented in software. If two disks in a RAID 5 set fail, you will need to replace the disks and restore the information from backup.

Fault tolerance RAID configurations implemented in hardware usually offer hot-swappable drives. This means you can pull out and replace a drive while the system is running, and it will perform the reconstruction of the data automatically.

Another type is RAID 0, also known as a *stripe set*. It requires at least 2 hard disks, but does not provide fault tolerance, it's merely a method of combining hard disks to allow for larger volumes. When a file is written to a RAID 0 stripe set with 2 disks, the first block is written to the first disk, the second block to the second disk, and the third data block is written on the first disk, and so on. If one of the hard disks in the stripe set fails, the entire stripe set is lost and needs to be rebuild and restored from backup.

## UPS

UPS is short for Uninterruptible Power Supply. It is a hardware device that goes between the power outlet and the system. Systems include servers, monitors, router and switches. When the main power fails, the UPS will take over and function as a battery. This will allow the system to keep running so the system can be taken down properly, user can be warned in advance, or in the best case, an effort to restore the main power can be made.

## DISASTER RECOVERY

Even if you have fault tolerance, it doesn't mean you 'have' disaster recovery. Planning for disaster recovery is an essential task, no matter the level of fault-tolerance. Backing up data to tape regularly is the most common method to prepare for disaster recovery.

Following are some important practices to consider when developing a tape backup strategy:

- Use a carefully planned *tape rotation* scheme. You want to avoid data on tapes from being overwritten too frequently, problems with data may have occurred long before they are discovered. On the other hand, using a new tape for every single day is often too costly. A common rotation scheme is *Grandfather-Father-Son*. For example, a "Son" tape is used for a daily incremental backups on Monday through Thursday, these 4 tapes are reused weekly. A "Father" tape is used for a full backup on Friday, a different tape exists for every Friday in a month, these 5 tapes are reused monthly. A "Grandfather" tape is used to perform a full backup on the last business day of each month in a quarter, these 3 tapes are reused quarterly.
- Store tapes at an off-site location. Imagine a large office complex with several buildings. A company that has offices in two buildings can easily exchange back ups at the end of a work day. If one building goes up in flames, the backup tapes will be safely stored in the other building. Having employees storing backup tapes at home is generally not a good idea.
- Store tapes in a locked fire safe. This doesn't mean they will be safe from *any* fire, the heat can get so intense the tapes will melt anyway, but it is the least you can do.

## Backup Types

To understand the various common backup types, first you'll have to know about the *archive* file attribute. If a file has this attribute it means it has changed since the previous time the archive attribute was turned off. An archive attribute can be turned off by performing certain types of backup, or manually by using the 'attrib' command line utility or Windows Explorer for example. The table below lists the most common backup types:

- Normal/Full* Backs up every selected file, regardless of the archive attribute setting, and clears the archive attribute.
- Copy* Backs up every selected file, regardless of the archive attribute setting. Does not clear the archive attribute.
- Daily* Backs up every selected file that has changed that day, regardless of the archive attribute setting, and clears the archive attribute.
- Incremental* Backs up only those files created or changed since the last normal or incremental backup, and clears the archive attribute. This method is used in combination with a periodic full backup. For example, a Normal/Full backup on Mondays and an incremental backup on the remaining days of the week. In case of a restore, you will need the last normal backup as well as all incremental backups since the last normal backup.
- Differential* Backs up only those files created or changed since the last normal or incremental backup, but does not clear the archive attribute. This method is also used in combination with a periodic full backup. For example, a Normal/Full backup on Mondays and a differential backup on the remaining days of the week. In case of a restore, you will need the last normal backup and the last differential backup.

## Hot-spare

Hot-spare devices are stored fully configured devices that are identical to production devices and can be used to replace the running system in case of a disaster. Examples include routers, switches and complete servers. Hot-spare systems are also referred to as standby systems.

## INTERNET CONNECTIONS

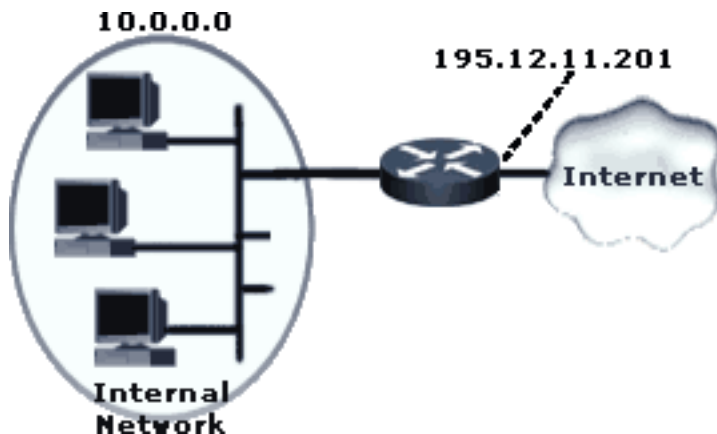
Before we discuss the services and devices that are used to connect LANs and WANs to the Internet, we will first have a look at *why* we need such services. You might need a basic understanding of TCP/IP to fully comprehend this TechNote. For more information about the TCP/IP suite read the [TCP/IP Suite TechNote](#).

As you know, corporate LANs and WANs use *private* address ranges, and the Internet uses *public* address ranges. This means that every IP address on the Internet is unique, but the addresses used in corporate networks are repeatedly used. For example, the private class A network 10.0.0.0 can be used by both company A and company B, while both their networks can be connected to the Internet.

In this context, there are two main types of connections: *routed* and *translated*. In a routed network every IP address must be unique. If in the above example, both company A and B would have a *routed* connection to the Internet, their internal addresses would be advertised on the web, hence resulting in conflicting duplicate IP addresses. To avoid this, companies could register public addresses and use them for their internal hosts. This would be very expensive, and there are simply not enough available public IP addresses to make every corporate LAN/WAN part of the same WAN (the Internet). The solution to this is a *translated* connection.

### Network Address Translation (NAT)

Network Address Translation (NAT, defined in RFC 1631), is typically implemented on routers to translate IP addresses and TCP and UDP port numbers. It operates at the Network layer (Layer 3) of the OSI model. A NAT router is typically also a DHCP server and DNS Proxy. NAT offers some security as well, because only one, or more, public IP addresses are visible to external hosts. The following network diagram shows an example of *dynamic* NAT. When a host from the internal network communicates with a web server on the Internet, the web server will receive packets with a source address of the NAT router's external interface instead of the internal host's address. When the web server sends the requested data back to the NAT router it will forward it to the host that initially made the request.



With *static* NAT, the router is configured with an address table. This table contains static entries that maps public address to local addresses. Static NAT entries are typically used when a web server or mail server resides on the internal LAN, but should be accessible by external users.

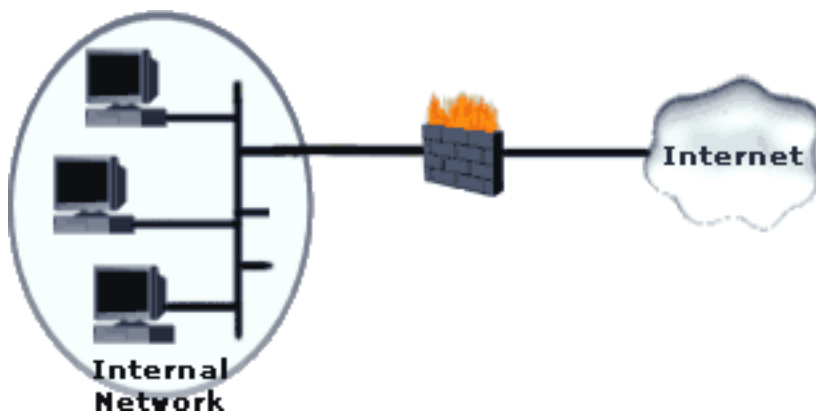
Besides using NAT on routers that are connected to the Internet, NAT is also used in corporate WANs when multiple LANs use the same IP subnet.

In addition to translating IP addresses, NAT can also be used to translate TCP and UDP port numbers, which are essentially part of a complete address, known as *socket*. (A socket is the combination of an IP address and a port number.) For example, you configured a mail server on your internal network to listen to port 125 for incoming SMTP connections instead of the default port 25. A NAT router would translate an incoming SMTP request and forward it to the appropriate port, 125, on the server.

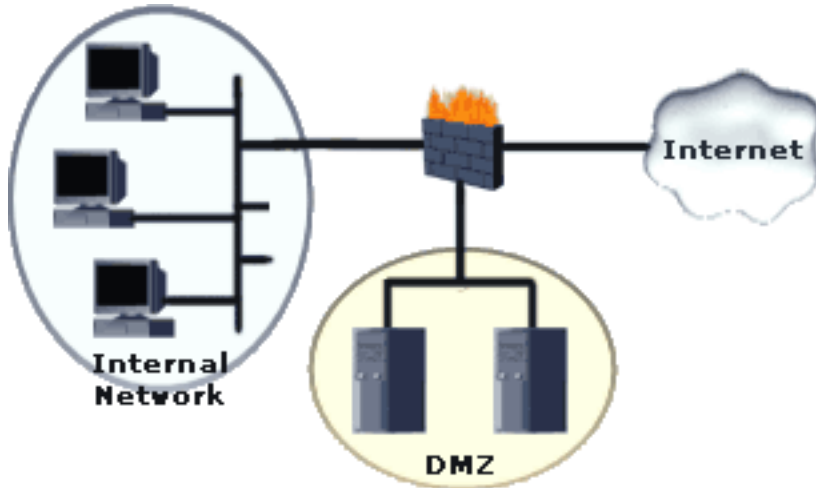
## Firewall

A firewall is a hardware device or software application that protects private networks from unauthorized external intruders. A firewall filters both inbound and outbound traffic and checks if it meets certain criteria. This filtering can occur on different levels of the OSI model. A basic firewall that operates at layer 3 is known as a *packet filter*, the criteria for letting packets pass or discard them are typically the source and destination address. The higher in the OSI model the firewall operates the more advanced criteria can be assigned to traffic, the most advanced being obviously the Application layer. Firewalls that operate at the Application layer typically use port numbers as the main criteria. For example you could allow port 25 for inbound and outbound SMTP traffic but deny port 110 for POP3. Another type of firewall is the *circuit-level* firewall that operates on the Transport layer of the OSI model; this firewall checks if the TCP and UDP messages used to establish a connection, meet certain criteria. Once a connection is established, traffic can pass the firewall without further checking.

The following diagram shows a simple firewall configuration, all outbound and inbound traffic must be authorized by the firewall before it can pass.

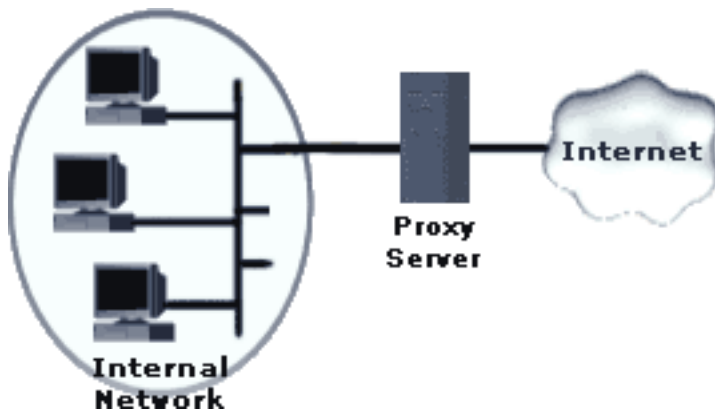


The next diagram shows a firewall configuration with a DMZ (demilitarized zone). The hosts in the DMZ are typically web servers, e-mail servers and the alike and are accessible for both internal and external users, such as those on the Internet.



## Proxy

The word "proxy" can be defined as something or someone that impersonates some other thing or someone else. Or simply: "something that acts on behalf of another". In the context interesting to us a proxy can be many things, the most common being the web proxy server. A proxy server is placed between the internal network and the Internet as depicted in the diagram below:



When a client from the internal network connects to an external resource and requests data, the proxy server pretends to be the client and retrieves the data and passes it on to the client. This offers some sort of protection because only the IP address of the proxy server is known on the external network. The main difference with NAT, is that a proxy is requested to act on behalf of a client. The proxy is making the actual request to the web server. With NAT, the web server is merely fooled by changing the addressing info of packets. Also NAT is transparent, the client doesn't know anything about the translating. To use a proxy server, the applications, such as a web browser, must support it.

There are many different types of proxy servers. Although not necessarily, most of them offer some sort of caching. For example if the proxy server in the diagram above represents a web caching proxy, the proxy server would first check if the data that an internal client requests, is requested by another client at an earlier time. In this case the proxy server would retrieve the data from its own hard disk instead of using the external connection. Obviously this can save a lot of traffic on expensive and relatively slow internet connections. Following are the most common type of proxies:

- *SOCKS Proxy*, SOCKS is a protocol that works with TCP/IP (and therefore with HTTP, FTP, POP3, SMTP, NNTP, etc.), and allows secure and transparent communication between a client and a proxy server.
- *HTTP Proxy*, besides providing an anonymous appearance on the web and acting as an intermediate for clients, it also caches web contents requested by clients.
- *DNS Proxy*, caches DNS lookups initiated by clients. When an internal client needs to know the IP address for a domain name, i.e. www.techexams.net, it will send the request to the DNS Proxy (i.e. a NAT router), which will forward it to DNS server on the Internet or retrieve the info from its cache with previous lookups on disk.
- *WINS Proxy*, works similar as a DNS Proxy except it forward NETBIOS name lookups to a WINS server and is only used in Microsoft networks.

A HTTP Proxy is often used in combination with a SOCKS proxy, the HTTP Proxy handles requests for web pages, and the SOCK proxy all other TCP/IP traffic, such as SMTP, POP3, and Telnet for example. Many companies today use proxy servers and virtually every ISP provides one to its subscribers. There are also many public proxy servers available. These are intended for anonymous surfing rather than for improving speed through caching.

## ICS

Internet Connection Sharing is a great feature included in several versions of Windows. It's designed to allow multiple clients to use the same internet connection. For example, in a small company with five employees that need regular access to the Internet ICS would allow you to implement one cable or xDSL connection for example, and share it between all five employees. Even a plain dial-up connection can be shared and set up when required.

ICS performs NAT and the computer with the shared connection acts as a DHCP server DNS proxy as well. This is at the same time the main disadvantage of ICS since it is not always desirable to have an 'extra' DHCP server in a LAN. Only IP addresses from the private IP Class C network 192.168.0.0 can be assigned to hosts in the internal network. In SOHO networks ICS can be very suitable though.

ICS can be enabled on the Advanced tab of the Properties of the connection to the Internet.

## Network Support

This TechNote will focus on one exam objective only: *4.9 Given a network problem scenario, select an appropriate course of action based on a general troubleshooting strategy. This strategy includes the following steps:*

- *Establish the symptoms*
- *Identify the affected area*
- *Establish what has changed*
- *Select the most probable cause*
- *Implement a solution*
- *Test the result*
- *Recognize the potential effects of the solution*
- *Document the solution*

If you carefully read a *network problem scenario* question in the Network+ exam, one or more of the first 3 steps will be given. For example: "A user calls you and says she can't logon to the network since her workstation has been moved to another office building." This includes pretty much all the information you need to complete step 1, 2, and 3. The following steps would be to select the most probable cause and implement a solution.

The remaining part of the question could be: "Select the most probable cause: a. Incorrect TCP/IP settings b. Defective NIC c. Defective patch cable d. Incorrect password". In this case you'll have to select the most probable cause by combining your technical knowledge with plain logic. There is no reason to assume that answer b, c, or d is correct. Although they could all be the cause of the problem, they are less easy to relate to the move. More probable is that the other office building requires different TCP/IP settings.

Instead, the remaining part of the question could also be: "What would you do to solve the problem? a. Replace the workstation's NIC b. Reinstall the client's OS c. Reconfigure the client's IPX settings d. Replace the patch cable" This means they will assume you know the probable cause already and they skip right ahead to implementing a solution. The cause is mostly obvious and the best solution can be determined again by using your technical knowledge combined with plain logic. There is no reason to assume that answer a, or d is correct, and answer b is obviously incorrect. Or you will pick answer c instantly because you assume the 2 buildings are connected with routers, meaning the IPX network number will be different in the other office.

Some scenario questions might include network diagrams. These are almost always related to the second step, "Identify the affected area", and the fourth step, "Select a probable cause". Knowing the facts and details covered in the other Network+ TechNotes will enable you to solve most of the scenario questions related to the exam objectives of Domain 4.0 Network Support. The rest comes down to knowing the steps described in this TechNote.

Another possibility is that you'll be asked to choose the next step. For example, in the first scenario above, the remaining part of the question could be: "*What is the next step you should take? a. Test the result b. Implement a solution c. Recognize the potential effects of the solution d. Select the most probable cause*". The correct answer would of course be d. The chance that you might encounter a question like this, and the fact that it will make you more efficient in solving such problems, is reason enough to memorize these steps.

You don't need to go thru all of the steps for every problem you will encounter. And the order of the steps is neither fixed. Also, every step can be repeated multiple times. For example, you probably won't document a solution if it the solution was "disable caps lock". In many real world scenarios you also want to recognize the potential effects of the solution before you implement it. And if you implemented a solution and tested the results, the results might be negative and force you to go back and repeat previous steps.

**APPENDIX I - Network+ Exam Objectives****Domain 1.0 - Media and Topologies – 20%**

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

- Star/hierarchical
- bus
- mesh
- ring
- wireless

1.2 Specify the main features of 802.2 (LLC), 802.3 (Ethernet), 802.5 (token ring), 802.11b (wireless) and FDDI networking technologies, including

- Speed
- Access
- Method
- Topology
- Media

1.3 Specify the characteristics (e.g., speed, length, topology, cable type, etc.) of the following 802.3 (Ethernet) standards

- 10BASE-T
- 100BASE-TX
- 10BASE2
- 10BASE5
- 100BASE-FX
- Gigabit Ethernet

1.4 Recognize the following media connectors and/or describe their uses

- RJ-11
- RJ-45
- AUI
- BNC
- ST
- SC

1.5 Choose the appropriate media type and connectors to add a client to an existing network.

1.6 Identify the purpose, features, and functions of the following network components

- Hubs
- Switches
- Bridges
- Routers
- Gateways
- CSU/DSU
- Network Interface Cards/ISDN adapters/system area network cards
- Wireless access points
- Modems

**Domain 2.0 – Protocols and Standards – 25%**

2.1 Given an example identify a MAC address

2.2 Identify the seven layers of the OSI model and their functions

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

- TCP/IP
- IPX/SPX
- NetBEUI
- AppleTalk

2.4 Identify the OSI layers at which the following network components operate

- Hubs
- Switches
- Bridges
- Routers
- Network Interface Cards

2.5 Define the purpose, function and/or use of the following protocols within TCP/IP

- IP
- TCP
- UDP
- FTP
- TFTP
- SMTP
- HTTP
- HTTPS
- POP3/IMAP4
- TELNET
- ICMP
- ARP
- NTP

2.6 Define the function of TCP/UDP ports. Identify well-known ports.

2.7 Identify the purpose of the following network services (e.g. DHCP/bootp, DNS, NAT/ICS, WINS, and SNMP)

2.8 Identify IP addresses (Ipv4, Ipv6) and their default subnet masks.

2.9 Identify the purpose of subnetting and default gateways.

2.10 Identify the differences between public vs. private networks

2.11 Identify the basic characteristics (e.g., speed, capacity, media) of the following WAN technologies

- Packet switching vs. circuit switching
- ISDN
- FDDI
- ATM
- Frame Relay
- Sonet/SDH
- T1/E1
- T3/E3
- OCx

2.12 Define the function of the following remote access protocols and services

- RAS
- PPP
- PPTP
- ICA

2.13 Identify the following security protocols and describe their purpose and function

- IPsec
- L2TP
- SSL
- Kerberos

### **Domain 3.0 Network Implementation – 23%**

3.1 Identify the basic capabilities (i.e. client support, interoperability, authentication, file and print services, application support, and security) of the following server operating systems

- UNIX/Linux
- Netware
- Windows
- Macintosh

3.2 Identify the basic capabilities of client workstations (i.e., client connectivity, local security mechanisms, and authentication)

3.3 Identify the main characteristics of VLANs

3.4 Identify the main characteristics of network attached storage

3.5 Identify the purpose and characteristics of fault tolerance

3.6 Identify the purpose and characteristics of disaster recovery

3.7 Given a remote connectivity scenario (e.g., IP, IPX, dial-up, PPPoE, authentication, physical connectivity etc.), configure the connection.

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

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

3.10 Given a scenario, predict the impact of a particular security implementation on network functionality (e.g. blocking port numbers, encryption, etc.)

3.11 Given a network configuration, select the appropriate NIC and network configuration settings (DHCP, DNS, WINS, protocols, NETBIOS/host name, etc.).

#### **Domain 4.0 Network Support – 32%**

4.1 Given a troubleshooting scenario, select the appropriate TCP/IP utility from among the following

- Tracert
- Ping
- Arp
- Netstat
- Nbtstat
- Ipconfig/Ifconfig
- Winipcfg
- Nslookup

4.2 Given a troubleshooting scenario involving a small office/home office network failure (e.g., xDSL, cable, home satellite, wireless, POTS), identify the cause of the failure.

4.3 Given a troubleshooting scenario involving a remote connectivity problem (e.g., authentication failure, protocol configuration, physical connectivity) identify the cause of the problem.

4.4 Given specific parameters, configure a client to connect to the following servers

- UNIX/Linux
- Netware
- Windows
- Macintosh

4.5 Given a wiring task, select the appropriate tool (e.g., wire crimper, media tester/certifier, punch down tool, tone generator, optical tester, etc.).

4.6 Given a network scenario interpret visual indicators (e.g., link lights, collision lights, etc.) to determine the nature of the problem.

4.7 Given output from a diagnostic utility (e.g. tracert, ping, ipconfig, etc.), identify the utility and interpret the output.

4.8 Given a scenario, predict the impact of modifying, adding, or removing network services (e.g., DHCP, DNS, WINS, etc.) on network resources and users.

4.9 Given a network problem scenario, select an appropriate course of action based on a general troubleshooting strategy. This strategy includes the following steps

1. Establish the symptoms
2. Identify the affected area
3. Establish what has changed
4. Select the most probable cause
5. Implement a solution
6. Test the result
7. Recognize the potential effects of the solution
8. Document the solution

4.10 Given a troubleshooting scenario involving a network with a particular physical topology (i.e., bus, star/hierarchical, mesh, ring, and wireless) and including a network diagram, identify the network area effected and the cause of the problem.

4.11 Given a network troubleshooting scenario involving a client connectivity problem (e.g., incorrect protocol/client software/authentication configuration, or insufficient rights/permission), identify the cause of the problem.

4.12 Given a network troubleshooting scenario involving a wiring/infrastructure problem, identify the cause of the problem (e.g., bad media, interference, network hardware).