

### 1) What is a Link?

A link refers to the connectivity between two devices. It includes the type of cables and protocols used in order for one device to be able to communicate with the other.

### 2) What are the layers of the OSI reference model?

There are 7 OSI layers: Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer and Application Layer.

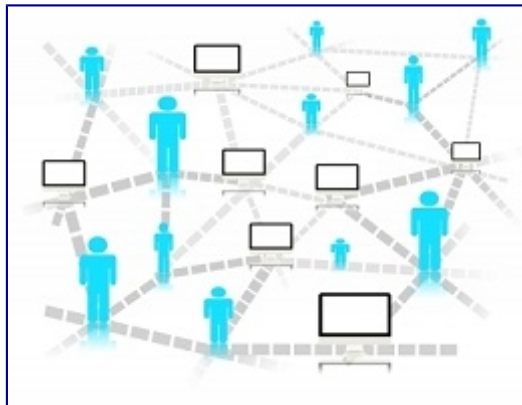
### 3) What is backbone network?

A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles management of bandwidth and various channels.

### 4) What is a LAN?

LAN is short for Local Area Network. It refers to the connection between computers and other network devices that are located within a small physical location.

### 5) What is a node?



A node refers to a point or joint where a connection takes place. It can be computer or device that is part of a network. Two or more nodes are needed in order to form a network connection.

### 6) What are routers?

Routers can connect two or more network segments. These are intelligent network devices that store information in its routing table such as paths, hops and bottlenecks. With this info, they are able to determine the best path for data transfer. Routers operate at the OSI Network Layer.

### 7) What is point to point link?

It refers to a direct connection between two computers on a network. A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers.

### 8) What is anonymous FTP?

Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed access to data in these servers do not need to identify themselves, but instead log in as an anonymous guest.

### 9) What is subnet mask?

A subnet mask is combined with an IP address in order to identify two parts: the extended network address and the host address. Like an IP address, a subnet mask is made up of 32 bits.

**10) What is the maximum length allowed for a UTP cable?**

A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.

**11) What is data encapsulation?**

Data encapsulation is the process of breaking down information into smaller manageable chunks before it is transmitted across the network. It is also in this process that the source and destination addresses are attached into the headers, along with parity checks.

**12) Describe Network Topology**

Network Topology refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect to one another.

**13) What is VPN?**

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

**14) Briefly describe NAT.**

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share single connection to the Internet.

**15) What is the job of the Network Layer under the OSI reference model?**

The Network layer is responsible for data routing, packet switching and control of network congestion. Routers operate under this layer.

**16) How does a network topology affect your decision in setting up a network?**

Network topology dictates what media you must use to interconnect devices. It also serves as basis on what materials, connector and terminations that is applicable for the setup.

**17) What is RIP?**

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

**18) What are different ways of securing a computer network?**

There are several ways to do this. Install reliable and updated anti-virus program on all computers. Make sure firewalls are setup and configured properly. User authentication will also help a lot. All of these combined would make a highly secured network.

**19) What is NIC?**

NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to

connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

## **20) What is WAN?**

WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.

## **21) What is the importance of the OSI Physical Layer?**

The physical layer does the conversion from data bits to electrical signal, and vice versa. This is where network devices and cable types are considered and setup.

## **22) How many layers are there under TCP/IP?**

There are four layers: the Network Layer, Internet Layer, Transport Layer and Application Layer.

## **23) What are proxy servers and how do they protect computer networks?**

Proxy servers primarily prevent external users from identifying the IP addresses of an internal network. Without knowledge of the correct IP address, even the physical location of the network cannot be identified. Proxy servers can make a network virtually invisible to external users.

## **24) What is the function of the OSI Session Layer?**

This layer provides the protocols and means for two devices on the network to communicate with each other by holding a session. This includes setting up the session, managing information exchange during the session, and tear-down process upon termination of the session.

## **25) What is the importance of implementing a Fault Tolerance System? Are there limitations?**

A fault tolerance system ensures continuous data availability. This is done by eliminating a single point of failure. However, this type of system would not be able to protect data in some cases, such as in accidental deletions.

## **26) What does 10Base-T mean?**

The 10 refers to the data transfer rate, in this case is 10Mbps. The word Base refers to base band, as oppose to broad band. T means twisted pair, which is the cable used for that network.

## **27) What is a private IP address?**

Private IP addresses are assigned for use on intranets. These addresses are used for internal networks and are not routable on external public networks. This ensures that no conflicts are present among internal networks while at the same time the same range of private IP addresses are reusable for multiple intranets since they do not “see” each other.

## **28) What is NOS?**

NOS, or Network Operating System, is specialized software whose main task is to provide network connectivity to a computer in order for it to be able to communicate with other computers and connected devices.

## **29) What is DoS?**

DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the

internet or any other network services. Such attacks may come in different forms and are done by a group of perpetrators. One common method of doing this is to overload the system server so it cannot anymore process legitimate traffic and will be forced to reset.

### **30) What is OSI and what role does it play in computer networks?**

OSI (Open Systems Interconnect) serves as a reference model for data communication. It is made up of 7 layers, with each layer defining a particular aspect on how network devices connect and communicate with one another. One layer may deal with the physical media used, while another layer dictates how data is actually transmitted across the network.

### **31) What is the purpose of cables being shielded and having twisted pairs?**

The main purpose of this is to prevent crosstalk. Crosstalks are electromagnetic interferences or noise that can affect data being transmitted across cables.

### **32) What is the advantage of address sharing?**

By using address translation instead of routing, address sharing provides an inherent security benefit. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer that provides address translation and not the private IP addresses on the internal network.

### **33) What are MAC addresses?**

MAC, or Media Access Control, uniquely identifies a device on the network. It is also known as physical address or Ethernet address. A MAC address is made up of 6-byte parts.

### **34) What is the equivalent layer or layers of the TCP/IP Application layer in terms of OSI reference model?**

The TCP/IP Application layer actually has three counterparts on the OSI model: the Session layer, Presentation Layer and Application Layer.

### **35) How can you identify the IP class of a given IP address?**

By looking at the first octet of any given IP address, you can identify whether it's Class A, B or C. If the first octet begins with a 0 bit, that address is Class A. If it begins with bits 10 then that address is a Class B address. If it begins with 110, then it's a Class C network.

### **36) What is the main purpose of OSPF?**

OSPF, or Open Shortest Path First, is a link-state routing protocol that uses routing tables to determine the best possible path for data exchange.

### **37) What are firewalls?**

Firewalls serve to protect an internal network from external attacks. These external threats can be hackers who want to steal data or computer viruses that can wipe out data in an instant. It also prevents other users from external networks from gaining access to the private network.

### **38) Describe star topology**

Star topology consists of a central hub that connects to nodes. This is one of the easiest to setup and

maintain.

### **39) What are gateways?**

Gateways provide connectivity between two or more network segments. It is usually a computer that runs the gateway software and provides translation services. This translation is a key in allowing different systems to communicate on the network.

### **40) What is the disadvantage of a star topology?**

One major disadvantage of star topology is that once the central hub or switch get damaged, the entire network becomes unusable.

### **41) What is SLIP?**

SLIP, or Serial Line Interface Protocol, is actually an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.

### **42) Give some examples of private network addresses.**

10.0.0.0 with a subnet mask of 255.0.0.0

172.16.0.0 with subnet mask of 255.240.0.0

192.168.0.0 with subnet mask of 255.255.0.0

### **43) What is tracert?**

Tracert is a Windows utility program that can be used to trace the route taken by data from the router to the destination network. It also shows the number of hops taken during the entire transmission route.

### **44) What are the functions of a network administrator?**

A network administrator has many responsibilities that can be summarized into 3 key functions: installation of a network, configuration of network settings, and maintenance/troubleshooting of networks.

### **45) Describe at one disadvantage of a peer to peer network.**

When you are accessing the resources that are shared by one of the workstations on the network, that workstation takes a performance hit.

### **46) What is Hybrid Network?**

A hybrid network is a network setup that makes use of both client-server and peer-to-peer architecture.

### **47) What is DHCP?**

DHCP is short for Dynamic Host Configuration Protocol. Its main task is to automatically assign an IP address to devices across the network. It first checks for the next available address not yet taken by any device, then assigns this to a network device.

### **48) What is the main job of the ARP?**

The main task of ARP or Address Resolution Protocol is to map a known IP address to a MAC layer

address.

**49) What is TCP/IP?**

TCP/IP is short for Transmission Control Protocol / Internet Protocol. This is a set of protocol layers that is designed to make data exchange possible on different types of computer networks, also known as heterogeneous network.

**50) How can you manage a network using a router?**

Routers have built in console that lets you configure different settings, like security and data logging. You can assign restrictions to computers, such as what resources it is allowed access, or what particular time of the day they can browse the internet. You can even put restrictions on what websites are not viewable across the entire network.

**51) What protocol can be applied when you want to transfer files between different platforms, such between UNIX systems and Windows servers?**

Use FTP (File Transfer Protocol) for file transfers between such different servers. This is possible because FTP is platform independent.

**52) What is the use of a default gateway?**

Default gateways provide means for the local networks to connect to the external network. The default gateway for connecting to the external network is usually the address of the external router port.

**53) One way of securing a network is through the use of passwords. What can be considered as good passwords?**

Good passwords are made up of not just letters, but by combining letters and numbers. A password that combines uppercase and lowercase letters is favorable than one that uses all upper case or all lower case letters. Passwords must be not words that can easily be guessed by hackers, such as dates, names, favorites, etc. Longer passwords are also better than short ones.

**54) What is the proper termination rate for UTP cables?**

The proper termination for unshielded twisted pair network cable is 100 ohms.

**55) What is netstat?**

Netstat is a command line utility program. It provides useful information about the current TCP/IP settings of a connection.

**56) What is the number of network IDs in a Class C network?**

For a Class C network, the number of usable Network ID bits is 21. The number of possible network IDs is 2 raised to 21 or 2,097,152. The number of host IDs per network ID is 2 raised to 8 minus 2, or 254.

**57) What happens when you use cables longer than the prescribed length?**

Cables that are too long would result in signal loss. This means that data transmission and reception would be affected, because the signal degrades over length.

### **58) What common software problems can lead to network defects?**

Software related problems can be any or a combination of the following:

- client server problems
- application conflicts
- error in configuration
- protocol mismatch
- security issues
- user policy and rights issues

### **59) What is ICMP?**

ICMP is Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP/IP stack. This is also the protocol that manages error messages that are used by network tools such as PING.

### **60) What is Ping?**

Ping is a utility program that allows you to check connectivity between network devices on the network. You can ping a device by using its IP address or device name, such as a computer name.

### **61) What is peer to peer?**

Peer to peer are networks that does not rely on a server. All PCs on this network act as individual workstations.

### **62) What is DNS?**

DNS is Domain Name System. The main function of this network service is to provide host names to TCP/IP address resolution.

### **63) What advantages does fiber optics have over other media?**

One major advantage of fiber optics is that it is less susceptible to electrical interference. It also supports higher bandwidth, meaning more data can be transmitted and received. Signal degrading is also very minimal over long distances.

### **64) What is the difference between a hub and a switch?**

A hub acts as a multiport repeater. However, as more and more devices connect to it, it would not be able to efficiently manage the volume of traffic that passes through it. A switch provides a better alternative that can improve the performance especially when high traffic volume is expected across all ports.

### **65) What are the different network protocols that are supported by Windows RRAS services?**

There are three main network protocols supported: NetBEUI, TCP/IP, and IPX.

### **66) What are the maximum networks and hosts in a class A, B and C network?**

For Class A, there are 126 possible networks and 16,777,214 hosts

For Class B, there are 16,384 possible networks and 65,534 hosts

For Class C, there are 2,097,152 possible networks and 254 hosts

**67) What is the standard color sequence of a straight-through cable?**

orange/white, orange, green/white, blue, blue/white, green, brown/white, brown.

**68) What protocols fall under the Application layer of the TCP/IP stack?**

The following are the protocols under TCP/IP Application layer: FTP, TFTP, Telnet and SMTP.

**69) You need to connect two computers for file sharing. Is it possible to do this without using a hub or router?**

Yes, you can connect two computers together using only one cable. A crossover type cable can be used in this scenario. In this setup, the data transmit pin of one cable is connected to the data receive pin of the other cable, and vice versa.

**70) What is ipconfig?**

Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

**71) What is the difference between a straight-through and crossover cable?**

A straight-through cable is used to connect computers to a switch, hub or router. A crossover cable is used to connect two similar devices together, such as a PC to PC or Hub to hub.

**72) What is client/server?**

Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refers to workstation that access the server.

**73) Describe networking.**

Networking refers to the inter connection between computers and peripherals for data communication. Networking can be done using wired cabling or through wireless link.

**74) When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?**

Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when the NIC card was replaced by another one.

**75) Explain clustering support**

Clustering support refers to the ability of a network operating system to connect multiple servers in a fault-tolerant group. The main purpose of this is in the event that one server fails, all processing will continue on with the next server in the cluster.

**76) In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?**

An anti-virus program must be installed on all servers and workstations to ensure protection. That's because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives.



### **77) Describe Ethernet.**

Ethernet is one of the popular networking technologies used these days. It was developed during the early 1970s and is based on specifications as stated in the IEEE. Ethernet is used in local area networks.

### **78) What are some drawbacks of implementing a ring topology?**

In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular part of the network, the entire network has to be temporarily brought down as well.

### **79) What is the difference between CSMA/CD and CSMA/CA?**

CSMA/CD, or Collision Detect, retransmits data frames whenever a collision occurred. CSMA/CA, or Collision Avoidance, will first broadcast intent to send prior to data transmission.

### **80) What is SMTP?**

SMTP is short for Simple Mail Transfer Protocol. This protocol deals with all Internal mail, and provides the necessary mail delivery services on the TCP/IP protocol stack.

### **81) What is multicast routing?**

Multicast routing is a targeted form of broadcasting that sends message to a selected group of user, instead of sending it to all users on a subnet.

### **82) What is the importance of Encryption on a network?**

Encryption is the process of translating information into a code that is unreadable by the user. It is then translated back or decrypted back to its normal readable format using a secret key or password. Encryption help ensure that information that is intercepted halfway would remain unreadable because the user has to have the correct password or key for it.

### **83) How are IP addresses arranged and displayed?**

IP addresses are displayed as a series of four decimal numbers that are separated by period or dots. Another term for this arrangement is the dotted decimal format. An example is 192.168.101.2

### **84) Explain the importance of authentication.**

Authentication is the process of verifying a user's credentials before he can log into the network. It is normally performed using a username and password. This provides a secure means of limiting the access from unwanted intruders on the network.

### **85) What do mean by tunnel mode?**

This is a mode of data exchange wherein two communicating computers do not use IPSec themselves. Instead, the gateway that is connecting their LANs to the transit network creates a virtual tunnel that uses the IPSec protocol to secure all communication that passes through it.

### **86) What are the different technologies involved in establishing WAN links?**

Analog connections – using conventional telephone lines; Digital connections – using digital-grade telephone lines; switched connections – using multiple sets of links between sender and receiver to

move data.

**87) What is one advantage of mesh topology?**

In the event that one link fails, there will always be another available. Mesh topology is actually one of the most fault-tolerant network topology.

**88) When troubleshooting computer network problems, what common hardware-related problems can occur?**

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs and even hardware startups. Incorrectly hardware configuration is also one of those culprits to look into.

**89) What can be done to fix signal attenuation problems?**

A common way of dealing with such a problem is to use repeaters and hub, because it will help regenerate the signal and therefore prevent signal loss. Checking if cables are properly terminated is also a must.

**90) How does dynamic host configuration protocol aid in network administration?**

Instead of having to visit each client computer to configure a static IP address, the network administrator can apply dynamic host configuration protocol to create a pool of IP addresses known as scopes that can be dynamically assigned to clients.

**91) Explain profile in terms of networking concept?**

Profiles are the configuration settings made for each user. A profile may be created that puts a user in a group, for example.

**92) What is sneakernet?**

Sneakernet is believed to be the earliest form of networking wherein data is physically transported using removable media, such as disk, tapes.

**93) What is the role of IEEE in computer networking?**

IEEE, or the Institute of Electrical and Electronics Engineers, is an organization composed of engineers that issues and manages standards for electrical and electronic devices. This includes networking devices, network interfaces, cablings and connectors.

**94) What protocols fall under the TCP/IP Internet Layer?**

There are 4 protocols that are being managed by this layer. These are ICMP, IGMP, IP and ARP.

**95) When it comes to networking, what are rights?**

Rights refer to the authorized permission to perform specific actions on the network. Each user on the network can be assigned individual rights, depending on what must be allowed for that user.

**96) What is one basic requirement for establishing VLANs?**

A VLAN requires dedicated equipment on each end of the connection that allows messages entering the Internet to be encrypted, as well as for authenticating users.

### 97) What is IPv6?

IPv6 , or Internet Protocol version 6, was developed to replace IPv4. At present, IPv4 is being used to control internet traffic, but is expected to get saturated in the near future. IPv6 was designed to overcome this limitation.

### 98) What is RSA algorithm?

RSA is short for Rivest-Shamir-Adleman algorithm. It is the most commonly used public key encryption algorithm in use today.

### 99) What is mesh topology?

Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device have at least two network connections.

### 100) what is the maximum segment length of a 100Base-FX network?

The maximum allowable length for a network segment using 100Base-FX is 412 meters. The maximum length for the entire network is 5 kilometers.

### Example of Networking commands in Unix

let's see some example of various networking command in Unix and Linux. Some of them are quite basic e.g. ping and telnet and some are more powerful e.g. nslookup and netstat. When you used these commands in combination of find and grep you can get anything you are looking for e.g. hostname, connection end points, connection status etc.

#### hostname

**hostname** with no options displays the machines host name

**hostname -d** displays the domain name the machine belongs to

**hostname -f** displays the fully qualified host and domain name

**hostname -i** displays the IP address for the current machine

#### ping

It sends packets of information to the user-defined source. If the packets are received, the destination device sends packets back. Ping can be used for two purposes

1. To ensure that a network connection can be established.
2. Timing information as to the speed of the connection.

#### ifconfig

View network configuration, it displays the current network adapter configuration. It is handy to determine if you are getting transmit (TX) or receive (RX) errors.

#### netstat

Most useful and very versatile for finding connection to and from the host. You can find out all the multicast groups (network) subscribed by this host by issuing "**netstat -g**"

**netstat -nap | grep port** will display process id of application which is using that port

**netstat -a** or **netstat -all** will display all connections including TCP and UDP  
**netstat --tcp** or **netstat -t** will display only TCP connection  
**netstat --udp** or **netstat -u** will display only UDP connection  
**netstat -g** will display all multicast network subscribed by this host.

### **nslookup**

If you know the IP address it will display hostname. To find all the IP addresses for a given domain name, the command nslookup is used. You must have a connection to the internet for this utility to be useful.

E.g. **nslookup blogger.com**

You can also use nslookup to [convert hostname to IP Address](#) and from IP Address from hostname.

### **traceroute**

A handy utility to view the number of hops and response time to get to a remote system or web site is traceroute. Again you need an internet connection to make use of this tool.

### **finger**

View user information, displays a user's login name, real name, terminal name and write status. this is pretty old unix command and rarely used now days.

### **telnet**

Connects destination host via telnet protocol, if telnet connection establish on any port means connectivity between two hosts is working fine.

**telnet hostname port** will telnet hostname with the port specified. Normally it is used to see whether host is alive and network connection is fine or not.