**2.A. Determine Communication architecture**

**2.A. 1Unified communications (e.g. convergence, collaboration, messaging)**

**2.A.2 Content type (e.g. data, voice, video, facsimile)**

**2.A.3 Transport mechanisms (e.g. satellite, landlines, microwave, radio, fiber)**

**Token Ring** was designed to be a more fault-tolerant topology than Ethernet, and can be a very resilient topology when properly implemented.

**ARCnet** is a LAN media access method, not a topology. It uses token-passing (LAN transmission protocol) in a star topology on a coaxial cable.

**In a BUS TOPOLOGY,** all the transmissions of the network travel the full length of cable and are received by all other stations. This topology is associated with Ethernet LAN media access. In a ring topology, all nodes are connected by unidirectional transmission links to form a closed loop. In a star technology, all stations are directly connected to a central device. FDDI is not a LAN topology, but a LAN media access method.

Start and stop bits mark the beginning and the end of each transfer in **asynchronous communication.**

**With Cyclic Redundancy Check (CRC)** or Frame Check Sequence (FCS), a single set of check digits is generated for each frame transmitted, based on the contents of the frame, and appended to the tail of the frame. It is used for situations where bursts of errors may be present (parity and block sum checks are not effective at detecting bursts of errors). Block chaining check is not a common error correction method.

**An Ethernet address** is a 48-bit address that is hard-wired into the Network Interface Cards (NIC) of the network node.

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model.

The older coaxial cable has been widely replaced with twisted pair, which is extremely resistant to failure, especially in a **star-wired** configuration.

**Frame relay** uses a public switched network to provide Wide Area Network (WAN) connectivity.

**Thicknet** is a coaxial cable with segments of up to 500 meters, also known as 10Base5. Thinnet is a coaxial cable with segments of up to 185 meters. Unshielded twisted pair (UTP) has three variations: 10 Mbps (10BaseT), 100 Mbps (100BaseT) or 1 Gbps (1000BaseT). ARCnet is a LAN media access method.

**2.A.4 Communication topology (e.g. centralized, distributed, cloud, mesh)**

The main characteristic of a **multi-homed host** is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.

**Frame relay and X.25** are both examples of packet-switching technologies. In packet-switched networks there are no dedicated connections between endpoints, and data is divided into packets and reassembled on the receiving end.

**ATM** is an example of a fast packet-switching network that can be used for either **data, voice or video**, but packets are of fixed size.

**LAN Transmission Methods**

LAN data transmissions fall into three classifications: **unicast, multicast, and broadcast.**

In each type of transmission, a single packet is sent to one or more nodes.

**In a unicast transmission**, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

**A multicast transmission** consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

**A broadcast transmission** consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.

**LAN Topologies**

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks—including 100BaseT—implement a bus topology

**Synchronous Communication** is characterized by very high speed transmission rates that are governed by electronic clock timing signals.

Generally, the methods for **multiplexing** data include the following :

* **Time-division multiplexing (TDM):** information from each data channel is allocated bandwidth based on pre-assigned time slots, regardless of whether there is data to transmit.
* **Asynchronous time-division multiplexing (ATDM):** information from data channels is allocated bandwidth as needed, via dynamically assigned time slots.
* **Frequency division multiplexing (FDM):** information from each data channel is allocated bandwidth based on the signal frequency of the traffic.
* **Statistical multiplexing:** Bandwidth is dynamically allocated to any data channels that have information to transmit.

**IEEE 802.3** specifies the standard for Ethernet and uses CSMA/CD, not token-passing.

**The IEEE 802.5** standard defines the token ring media access method. 802.3 refers to Ethernet's CSMA/CD, 802.11 refers to wireless communications and 802.2 refers to the logical link control.

**Serial Line IP (SLIP)** was developed in 1984 to support TCP/IP networking over low-speed serial interfaces.

**The Point-to-Point Protocol (PPP)** was designed to support multiple network types over the same serial link, just as Ethernet supports multiple network types over the same LAN. PPP replaces the earlier Serial Line Internet Protocol (SLIP) that only supports IP over a serial link. PPTP is a tunneling protocol.

A network topology defines the manner in which the network devices are organized to facilitate communications. Common LAN technologies are:

**bus**

**ring**

**star**

**meshed**

LAN transmission methods refer to the way packets are sent on the network and are:

**unicast**

**multicast**

**broadcast**

LAN transmission protocols are the rules for communicating between computers on a LAN. Common LAN transmission protocols are:

**CSMA/CD**

**polling**

**token-passing**

LAN media access methods control the use of a network (physical and data link layers). They can be:

**Ethernet**

**ARCnet**

**Token ring**

**FDDI**

**Very-high data-rate Digital Subscriber Line (VDSL)** can deliver up to 52 Mbps downstream over a single copper twisted pair over a relatively short distance (1000 to 4500 feet). DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), **HDSL, SDSL, IDSL and VDSL** etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office

**Diverse routing—**This is the practice of routing traffic through different cable facilities. Organizations can obtain both diverse routing and alternate routing, but the cost is not cheap. Most of these systems use buried facilities. These systems usually enter a facility through the basement and can sometimes share space with other mechanical equipment. Recognize that this sharing adds to the risk of potential failure. Also, many cities have aging infrastructures, which is another potential point of failure.

**Alternate routing—**Redundant routing provides use of another transmission line if the regular line is busy or unavailable. This can include using a dialup connection in place of a dedicated connection, cell phone instead of a land line, or microwave communication in place of a fiber connection.

**Last mile protection—**This is a good choice for recovery facilities; it provides a second local loop connection, and is even more redundantly capable if an alternative carrier is used.

**Voice communication recovery—**Many organizations are highly dependent on voice communications. Others have started making the switch to Voice over IP (VoIP) for both voice and fax communication because of the cost savings. Some number of land lines should always be maintained to provide backup capability.

**T1 CONNECTIONS**

A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection.

In fact it would be a Multiplexer at one end and DeMultiplexer at other end or vice versa. Inverse Multiplexer at both end.

In electronics, a multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines, which are used to select which input line to send to the output. Multiplexers are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth. A multiplexer is also called a data selector.

An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal.

On the other hand, a demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the receiving end.

An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch

**Digital Signal level 1 (DS-1)** is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility. DS-0 is the framing specification used in transmitting digital signals over a single 64 Kbps channel over a T1 facility. DS-3 is the framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. DS-2 is not a defined framing specification.

**FRAME**

Ethernet is frame based network technology.

**SEGMENT**

A segment is the unit of end-to-end transmission in the TCP protocol. A segment consists of a TCP header followed by application data. A segment is transmitted by encapsulation inside an IP datagram.

**PACKET**

A packet is the unit of data passed across the interface between the internet layer and the link layer. It includes an IP header and data. A packet may be a complete IP datagram or a fragment of an IP datagram.

**FRAME**

A frame is the unit of transmission in a link layer protocol, and consists of a link-layer header followed by a packet.

**2.B Determine Network Architecture**

**2.B.1 Network types (e.g. public, private, hybrid)**

**2.B.2 Protocols**

IP headers contain 32-bit addresses (in IPv4) and 128 in IPv6. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. The physical machine address is also known as a Media Access Control (MAC) address.

**The Address Resolution Protocol (ARP)** is used to match an IP address to an Ethernet address so the packet can be sent to the appropriate node. **Reverse Address Resolution Protocol (RARP)** is used to match an Ethernet address to an IP address.

**OSI: SET is provided at the application level.** The SET(tm) Specification, is an open technical standard for the commerce industry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet. Digital Certificates create a trust chain throughout the transaction, verifying cardholder and merchant validity, a process unparalleled by other Internet security solutions. Software vendors whose products pass SET Compliance Testing are eligible to display the SET Mark on their products, as are merchants, financial institutions, and promotional sites that utilize or advertise licensed software.

SET was developed by SETco, led by VISA and MasterCard (and involving other companies such as GTE, IBM, Microsoft, Netscape, RSA, Safelayer — formerly SET Projects — and VeriSign. VeriFone - who built one of the earliest Internet Payment gateways used by several leading banks was also closely involved.) starting in 1996. SET was based on X.509 certificates with several extensions. The first version was finalised in May 1997 and a pilot test was announced in July 1998.

SET allowed parties to identify themselves to each other and exchange information securely. SET used a cryptographic blinding algorithm that, in effect, would have let merchants substitute a certificate for a user's credit-card number. If SET were used, the merchant itself would never have had to know the credit-card numbers being sent from the buyer, which would have provided verified good payment but protected customers and credit companies from fraud.

**Connection-oriented protocols** provide reliability of the service provided to the higher layer. It is the responsibility of such protocols in the **transport layer** to enhance the quality of service provided by the network layer.

**Transport Layer Security (TLS)** is a two-layered socket layer security protocol that contains:

TLS Record Protocol and the,

Transport Layer Security (TLS) Handshake Protocol.

**Secure Sockets Layer (SSL)** is the technology used in most Web-based applications. SSL version 2.0 supports strong authentication of the web server, but the authentication of the client side only comes with version 3.0. SSL v4 is not a defined standard.

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.

SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.

According to the cited source, it is operating at the Application/Transport layers.

**S-HTTP -** An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers. SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system.

**SQL**

The Structured Query Language (SQL), implemented at the session layer (layer 5) of the OSI/ISO model provides users with a way to define their information requirements.

SQL is by definition a language for querying and accessing data in databases, which includes transaction management to keep the database consistent. It involves setting up and maintaining sessions (between the host issuing queries and the database server) and it uses the concept of transactions.

Communication between computers is established, maintained and terminated by the session layer. The session layer is layer 5 of the OSI model. SQL is an example of a session layer protocol. The session layer is in contact with the session layer of the remote machine it is communicating with.

**A SOCKS** based server operates at the Session layer of the OSI model.

SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS is an abbreviation for "SOCKetS". As of Version 5 of SOCK, both UDP and TCP is supported.

One of the best known circuit-level proxies is SOCKS proxy server. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct “IP-reachability”The protocol was originally developed by David Koblas, a system administrator of MIPS Computer Systems. After MIPS was taken over by Silicon Graphics in 1992, Koblas presented a paper on SOCKS at that year's Usenix Security Symposium and SOCKS became publicly available. The protocol was extended to version 4 by Ying-Da Lee of NEC. SOCKS includes two components, the SOCKS server and the SOCKS client.

**Remote Procedure Call (RPC, UDP port 111)** is a protocol that allows two computers to coordinate in executing software. RPC can be used by a program on one computer to transfer execution of a subroutine to another computer, and have the results returned to the first. RPC is a fragile service, and most operating systems cannot handle arbitrary data being sent to an RPC port. It is best used in trusted LAN environments and should not usually be allowed through the organization's firewall. RPC is being replaced by Secure-RPC.

Session layer, which establishes, maintains and manages sessions and synchronization of data flow. Session layer protocols control application-to-application communications, which is what an RPC call is.

**Secure RPC provides authentication services.**

Secure RPC is an authentication method that authenticates both the host and the user who is making a request for a service. Secure RPC uses the Diffie-Hellman authentication mechanism. This authentication mechanism uses DES encryption. Applications that use Secure RPC include NFS and the NIS+ name service.

**TFTP** (Trivial File Transfer Protocol) is sometimes used to transfer configuration files from equipments such as routers but the primary difference between FTP and TFTP is that TFTP does not require authentication. Speed and ability to automate are not important.

Both of these protocols (FTP and TFTP) can be used for transferring files across the Internet. The differences between the two protocols are explained below:

**FTP** is a complete, session-oriented, general purpose file transfer protocol. TFTP is used as a bare-bones special purpose file transfer protocol.

**Secure shell (SSH) was** designed as an alternative to the above insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.

SSH’s services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel.

The **Transport layer** sets up communication between computer systems, while the **Session layer** sets up connections between applications.

TCP is the only one of the mentioned protocols to operate at the **transport layer (layer 4).**

The **Internet layer** in the TCP/IP protocol stack corresponds to the **network layer (layer 3) in** the OSI/ISO model. The host-to-host layer corresponds to the transport layer (layer 4) in the OSI/ISO model. The Network access layer corresponds to the data link and physical layers (layers 2 and 1) in the OSI/ISO model. The session layer is not defined in the TCP/IP protocol stack.

In the TCP/IP protocol model, the Internet layer defines the IP datagram and handles the routing of data across networks.

**The OSI/ISO Data Link layer** is made up of two sub-layers; (1) the Media Access Control layer refers downward to lower layer hardware functions and (2) the Logical Link Control refers upward to higher layer software functions. Other choices are distracters.

**Port 119** is normally used for the Network News Transfer Protocol. It is thus not need for a mail server, which would normally listen to ports **25 (SMTP), 110 (POP3) and 143 (IMAP).**

**Network address translation (NAT)** is concerned with IP address translation between two networks and operates at the network layer (layer 3).

With **dynamic translation** (also called Automatic, Hide Mode, or IP Masquerade), a large group of internal clients to share a single or small group of ROUTABLE IP addresses for the purpose of hiding their identities when communicating with external hosts or expanding the internal network address space.

**Static translation** (also called port forwarding), assigns a fixed address to a specific internal network resource (usually a server). Static NAT is required to make internal hosts available for connection from external hosts.

With static translation (also called port forwarding), a specific internal network resource (usually a server) has a fixed translation that never changes. Static NAT is required to make internal hosts available for connection from external hosts. In dynamic translation (also called Automatic, Hide Mode, or IP Masquerade), a large group of internal clients share a single or small group of internal IP addresses for the purpose of hiding their identities or expanding the internal network address space. Load Balancing Translation is used to translate a single IP address and port to a pool of identically configured servers so that a single public address can be served by a number of servers. In Network Redundancy Translation, multiple Internet connections are attached to a single NAT firewall that it chooses and uses based on load and availability.

**Load Balancing Translation** is used to translate a single IP address and port to a pool of identically configured servers so that a single public address can be served by a number of servers. In Network Redundancy Translation, multiple Internet connections are attached to a single NAT firewall that it chooses and uses based on load and availability.

**X.400** is used in e-mail as a message handling protocol. **X.500** is used in directory services**. X.509** is used in digital certificates and **X.800** is used a network security standard.

**2.B.3 Securing common services (e.g. wireless, e-mail, VoIP)**

**VOIP:**

**H323 Protocol**

**SIP**

**SS7**

**PCM**

**Jitter**

**End to End Delay**

**Wireless:**

**WEP, WPA, WPA2**

**802.1x**

**2.C Protect Communications and Networks**

**2.C.1 Communications and network policies**

**2.C.2 Boundary protection (e.g. firewalls, VPNs, airgaps)**

**L2TP and PPTP** were both designed for individual client to server connections; they enable only a single point-to-point connection per session. Dial-up VPNs use L2TP often. Both L2TP and PPTP operate at the data link layer (layer 2) of the OSI model. PPTP uses native PPP authentication and encryption services and L2TP is a combination of PPTP and Layer 2 Forwarding protocol (L2F).

PPTP operates at the data link layer (layer 2) of the OSI model and uses native PPP authentication and encryption services. Designed for individual client to server connections, it enables only a single point-to-point connection per session.

PPTP - Point-to-Point Tunneling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking.

PPTP operates at Layer 2 of the OSI model.

**STATEFUL / SESSIONS -** The question is explict in asking \*easily\*. With a TCP packet there is a distinct state or sequence that can be expected. Consult the references for further details.

ICMP, IP and UDP don't have any concept of a session; i.e. each packet or datagram is handled individually, with no reference to the contents of the previous one. With no sessions, these protocols usually cannot be filtered on the state of the session. Some newer firewalls, however, simulate the concept of state for these protocols, and filter out unexpected packets based upon normal usage. Although these are commonly treated like normal stateful filters, they are more complex to program, and hence more prone to errors.

A stateful packet filter or stateful inspection inspects each packet and only allows known connection states through. So, if a SYN/ACK packet was recieved and there was not a prior SYN packet sent it would filter that packet and not let it in. The correct sequence of steps are known and if the sequence or state is incorrect then it is dropped.

Packets in a **stateful inspection firewall** are queued and then analyzed at all OSI layers, providing a more complete inspection of the data. By examining the state and context of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC).

**2.C.3 Gateways, routers, and switches architecture (e.g. access control, segmentation, out-of-band management, OSI layers)**

**A gateway** is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

**A bridge** operates at the data link layer. Bridges are used to connect two separate networks to form a logical network. They must have storage capacity to store frames and act as a store-and-forward device. Bridges operate at the data link layer by examining the media access control header of a data packet. Routers are switching devices that operate at the network layer by examining network addresses. Repeaters work at the physical layer and amplify transmission signals to reach remote devices by taking a signal from a LAN. Gateways provide access paths to foreign networks.

**A router** is a network layer device for which the two connecting networks must have the same network layer protocol. Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.

**A brouter** is essentially a bridge with some routing functionality.

**Repeaters** offer the simplest form of connectivity. They regenerate received electrical signals at their original strength between cable segments. Bridges are devices used to connect similar or dissimilar LANs together to form an extended LAN. Routers provide packet routing between network segments. Brouter are devices that combine router and bridge functionality.

**Switches** primarily operate at the data link layer (layer 2), although intelligent, extremely fast Layer 3 switching techniques are being more frequently used.

**"First generation firewall"** is the correct answer. The first types of firewalls were packet filtering firewalls. It is the most basic firewall making access decisions based on ACL's. It will filter traffic based on source IP and port as well as destination IP and port. It does not understand the context of the communication and inspects every single packet one by one without understanding the context of the connection.

An important point with packet filtering firewalls is their speed and flexibility, as well as capacity to block denial-of-service and related attacks, makes them ideal for placement at the outermost boundary with and untrusted network. Other choices represent weaknesses of packet filtering firewalls.

Packet filtering firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. This type of firewall is considered a first generation firewall and can operate at either the network of transport layer of the OSI model.

**"Second generation firewall"** is incorrect. The second generation of firewall were Proxy based firewalls. Under proxy based firewall you have **Application Level Proxy** and also the Circuit-level proxy firewall. The application level proxy is very smart and understand the inner structure of the protocol itself. The Circui-Level Proxy is a generic proxy that allow you to proxy protocols for which you do not have an Application Level Proxy. This is better than allowing a direct connection to the net. Today a great example of this would be the SOCKS protocol.

"**Data's origin"** is the correct answer. The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server.

**"Third generation firewall"** is incorrect. The third generation firewall is the Stateful Inspection firewall. This type of firewall makes use of a state table to maintain the context of connections being established.

**"Fourth generation firewall"** is incorrect. The fourth generation firewall is the dynamic packet filtering firewall.

Firewalls can protect a network at multiple layers of the OSI models, however most of the firewalls do not have the ability to monitor the payload of the packets and see if an application level attack is taking place.

Today there are a new breed of firewall called Unified Threat Managers or UTM. They are a collection of products on a single computer and not necessarily a typical firewall. A UTM can address all of the layers but typically a firewall cannot.

Firewalls are security checkpoints at the boundaries of internal networks through which every packet must pass and be inspected, hence they create bottlenecks between the internal and external networks. But since external connections are relatively slow compared to modern computers, the latency caused by this bottleneck can almost be transparent.

By implementing the concept of border security, they centralize security services in machines optimized and dedicated to the task, thus relieving the other hosts on the network from that function.

**The dynamic packet filtering** firewall is able to create ACL's on the fly to allow replies on dynamic ports (higher than 1023).

One the most secure implementations of firewall architectures is the **screened-subnet firewall.** It employs two packet-filtering routers and a bastion host. Like a screened host firewall, this firewall supports both packet-filtering and proxy services.

**IDS**

The deployment of **network-based IDSs** has little impact upon an existing network. Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort.

Network-based IDSs are not vulnerable to attacks is not true, even thou network-based IDSs can be made very secure against attack and even made invisible to many attackers they still have to read the packets and sometimes a well crafted packet might exploit or kill your capture engine.

Network-based IDSs are well suited for modern switch-based networks is not true as most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch.

Most network-based IDSs can automatically indicate whether or not an attack was successful is not true as most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.

Network-based ID systems:

- Commonly reside on a discrete network segment and monitor the traffic on that network segment

- Usually consist of a network appliance with a Network Interface Card (NIC) that is operating in promiscuous mode and is intercepting and analyzing the network packets in real time

"A passive NIDS takes advantage of promiscuous mode access to the network, allowing it to gain visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network, performance, or the systems and applications utilizing the network."

A **HIDS** does not consume large amounts of system resources is the correct choice. HIDS can consume inordinate amounts of CPU and system resources in order to function effectively, especially during an event.

All the other answers are characteristics of HIDSes

**A HIDS can:**

- scrutinize event logs, critical system files, and other auditable system resources;

- look for unauthorized change or suspicious patterns of behavior or activity

- can send alerts when unusual events are discovered

**IDS:**

Communications is the component of an alarm that delivers alerts through a variety of channels such as email, pagers, instant messages and so on.

An Enunciator is the component of an alarm that uses business logic to compose the content and format of an alert and determine the recipients of that alert.

A sensor is a fundamental component of IDS alarms. A sensor detects an event and produces an appropriate notification.

Active and passive IDS

An active IDS (now more commonly known as an intrusion prevention system — IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

**A passive IDS** is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

**Network-based and host-based IDS**

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

**A host-based IDS** requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.

**Knowledge-based and behavior-based IDS**

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

**Statistical analysis-based (also called behaviour-based)** intrusion detection is characterized with a higher rate of false positives, as opposed to knowledge-based intrusion detection. Host-based and network-based intrusion detection are common implementations, not conceptual approaches.

**OSI SESSION LAYER** - Layer 5 of the OSI model is the Session Layer. This layer provides a logical persistent connection between peer hosts. A session is analogous to a conversation that is necessary for applications to exchange information.

The sesstion layer is responsible for establishing, managing, and closing end-to-end connections, called sessions, between applications located at different network endpoints. Dialogue control management provided by the session layer includes full-duplex, half-duplex, and simplex communications. Session layer management also helps to ensure that multiple streams of data stay synchronized with each other, as in the case of multimedia applications like video conferencing, and assists with the prevention of application related data errors.

The session layer is responsible for creating, maintaining, and tearing down the session.

Three modes are offered:

(Full) Duplex: Both hosts can exchange information simultaneously, independent of each other.

Half Duplex: Hosts can exchange information, but only one host at a time.

Simplex: Only one host can send information to its peer. Information travels in one direction only.

The TCP/IP protocol model defines four layers:

**Application,**

**Host-to-host**

The host-to-host layer provides for reliable end-to-end communications, ensures the data's error-free delivery, handles the data's packet sequencing, and maintains the data's integrity. It is comparable to the transport layer of the OSI model.

**Internet**

**Network access.**

The session layer is defined in the OSI/ISO model.

There are six basic security services defined by the OSI:

* Authentication,
* access control,
* data confidentiality,
* data integrity,
* nonrepudiation, and
* logging and monitoring.

**OSI LAYER 1:**

The physical layer (layer 1) defines the X.24, V.35, X.21 and HSSI standard interfaces.

**OSI LAYER 2:**

**PPP**

**RARP**

**L2F**

The Data Link layer provides data transport across a physical link. It handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control.

The Data Link layer of the OSI/ISO model provides SLIP, CSLIP and PPP protocol.

Layer 2 (Data Link layer) transfers information to the other end of the physical link. It handles physical addressing, network topology, error notification, delivery of frames and flow control.

**OSI LAYER 3:**

**ICMP**

The network layer contains the Internet Protocol (IP), the Internet Control Message Protocol (ICMP), and the Internet Group Management Protocol (IGMP)

The main responsibility of the network layer is to insert information into the packet's header so that it can be properly routed. The protocols at the network layer must determine the best path for the packet to take.

**OSI LAYER 4:**

Services located in the transport layer (layer 4) both segment and reassemble the data from upper-layer applications and unite it onto the same data stream, which provides end-to-end data transport services and establishes a logical connection between the sending host and destination host on a network.

As you will see in the explanations below the session layer establish LOGICAL CONNECTIONS between NETWORK DEVICES (not hosts)

The TRANSPORT LAYER establish logical connection between the END POINTS of an internetwork, that is, the originating host and the destination host.

Both does similar tasks but one does it between devices and the other does it between END POINTS hosts.

**OSI LAYER 6:**

**Layer 6 Presentation -** It is responsible for taking information from the "Application layer protocols" and putting it in a form suitable for the application to process.

**2.C.4 Detection and response**

**2.C.5 Content monitoring, inspection and filtering (e.g. email, web, data)**

**2.C.6 Device Control**

**2.D Identify security design considerations and associated risks**

**2.D.1 Interoperability**

**2.D.2 Auditability (e.g. regulatory, legislative, forensic requirements, segregation, verifiability of high assurance systems)**

**2.D.3 Security configuration (e.g. baseline)**

**2.D.4 Remote access**

**2.D.5 Monitoring (e.g. sensor placement, time reconciliation, span of contro, record compatibility)**

**2.D.6 Network configuration (e.g. physical, logical, high availability)**

**2.D.7 Operating environment (e.g. virtualization, cloud computing)**

**2.D.8 Secure sourcing strategy**

**OTHER**

**Incident Response Management -** This management often consists of the following:

- Coordinating the notification and distribution of information pertaining to the incident to the appropriate parties (those with a need to know) through a predefined escalation path

- Mitigating risk to the enterprise by minimizing the disruptions to normal business activities and the costs associated with remediating the incident (including public relations)

- Assembling teams of technical personnel to investigate the potential vulnerabilities and to resolve specific intrusions

**The purposes of RAID** (Redundant Array of Inexpensive Disks) is to provide Redundancy and Higher Data Transfer performance.

The purpose of RAID is Fault Tolerance.

Basically, RAID separates the data into multiple units and stores it on multiple disks by using a process called "striping".

The RAID Advisory Board has defined three classifications of RAID:

**Failure Resistant Disk Systems (FRDSs),**

**Failure Tolerant Disk Systems,**

**Disaster Tolerant Disk Systems.**

RAID Level 1 mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks.

RAID Levels 3 and 4 :- In this implementation, spare drives can be used to replace crashed drives.

RAID Level 5 stripes the data and the parity information at the block level across all the drives in the set.

RAID Level 5 :- The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server while the system is up and running.

A hardware RAID implementation is usually platform-independent.

RAID levels 3 and 5 run faster on hardware.

**RAID systems are mostly concerned with availability and performance.**

Redundant array of inexpensive disks (RAID) are primarily used to implove speed, availability, and redundancy, not integrity. They provide fault tolerance and protection against file server hard disk crashes.

RAID 1 Mirroring has the highest cost per megabyte since every piece of data is written at two different locations simultaneously for redundancy purposes.

The only difference is that level 3 is implemented at the byte level and level 4 is usually implemented at the **block level.**

RAID Level 2 :- It defines a disk drive system with 39 disks: 32 disks of user storage and seven disks of error recovery coding.

**Tape Arrays use a large device with multiple (sometimes 32 or 64) tapes that are configured as a single array.**

**The Digital Linear Tape (DLT)** is only 4mm in size, yet the compression techniques and head scanning process make it a large capacity and fast (5 Mbps) tape.

**Quarter Inch Cartridge drives (QIC).** This format is mostly used for home/small office backups, has a small capacity, and is slow, but inexpensive.

**Differential Backup -** Backup the files that have been modified since the last Full Backup. The archive bit does not change. Take more time while the backup phase is performed and take less time to restore.

**Incremental Backup -** Backup all the files that have changed since the last Full Backup (the first time it is run after a full backup was previously completed) or Incremental Backup (for the second backup and subsequent backups) and sets the archive bit to 0. Take less time during the backup phase but it will take more time to restore. The incremental backup method only copies files that have been recently changed or added. Only files with their archive bit set are backed up. This method is fast and uses less tape space but has some inherent vulnerabilities, one being that all incremental backups need to be available and restored from the date of the last full backup to the desired date should a restore be needed.

**Hierarchical Storage Management (HSM)** provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs.

Hierarchical Storage Management (HSM) is commonly employed in very large data retrieval systems.

**Mirroring,** the system writes the data simultaneously to separate drives or arrays.

The advantage of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk.

The disadvantage of mirroring is that both drives or disk arrays are processing in the writing to disks function, which can hinder system performance.

Mirroring has a high fault tolerance and can be implemented either through a hardware RAID controller or through the operating system. Since it requires twice the disk space than actual data, mirroring is the less cost-efficient data redundancy strategy.

**DMZ = screened subnet.**

**BACKUPS:**

The purpose of a **tape backup method** is to protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and ensuring availability.

All other choices could suffer from corruption and it might not be possible to restore the data without proper backups being done.

**Mirroring** will preserve integrity and restore points in all cases of drive failure. However, if you have corrupted data on the primary set of drives you may get corrupted data on the secondary set as well.

**Remote Journaling provides** Continuous or periodic synchronized recording of transaction data at a remote location as a backup strategy. (http://www.businessdictionary.com/definition/remote-journaling.html) With journaling there might be a gap of time between the data updates being send in batch at regular interval. So some of the data could be lost.

**Database shadowing** is synonymous with Mirroring but it only applies to databases, but not to information and data as a whole.

**BootP** was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN. Over time, it has expanded to allow centralized configuration of many aspects of a host's identity and behavior on the network. Note that DHCP, more complex, has replaced BootP over time.

In general, the term **packet** applies to any message formatted as a packet, while the term **datagram** is generally reserved for packets of an "unreliable" service.

**A smurf attack** occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests.

**An IP spoofing attack** is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A TCP sequence number attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number. Piggybacking refers to an attacker gaining unauthorized access to a system by using a legitimate user's connection. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets.

**A TCP sequence number attack** exploits the communication session which was established between the target and the trusted host that initiated the session. It involves hijacking the session between the host and the target by predicting the target's choice of an initial TCP sequence number. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies.

**The Land attack** involves the perpetrator sending spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening. The packet(s) contain the same destination and source IP address as the host, causing the victim's machine to reply to itself repeatedly. In addition, most systems experience a total freeze up, where as CTRL-ALT-DELETE fails to work, the mouse and keyboard become non operational and the only method of correction is to reboot via a reset button on the system or by turning the machine off.

**The Boink attack**, a modified version of the original Teardrop and Bonk exploit programs, is very similar to the Bonk attack, in that it involves the perpetrator sending corrupt UDP packets to the host. It however allows the attacker to attack multiple ports where Bonk was mainly directed to port 53 (DNS).

**The Teardrop attack** involves the perpetrator sending overlapping packets to the victim, when their machine attempts to re-construct the packets the victim's machine hangs.

**A Smurf attack** is a network-level attack against hosts where a perpetrator sends a large amount of ICMP echo (ping) traffic at broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.

A **teardrop attack** consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets. A buffer overflow attack occurs when a process receives much more data than expected.

**Network Address Hijacking** enables the intruder re-route data traffic from a network device to a personal machine.

In computer networking, **source routing allows** a sender of a packet to specify the route the packet takes through the network.

With source routing the entire path to the destination is known to the sender and is included when sending data. Source routing differs from most other routing in that the source makes most or all of the routing decisions for each router along the way.

**Urgent Pointer**

This could be a sign of covert channels being used in the bank network communications and should be investigated.

The Urgent Pointer is used when some information has to reach the server ASAP. When the TCP/IP stack at the other end sees a packet using the Urgent Pointer set, it is duty bound to stop all ongoing activities and immediately send this packet up the stack for immediate processing. Since the packet is plucked out of the processing queue and acted upon immediately, it is known as an Out Of Band (OOB) packet and the data is called Out Of Band (OOB) data.

The Urgent Pointer is usually used in Telnet, where an immediate response (e.g. the echoing of characters) is desirable.

Covert Channels are not directly synonymous with backdoors. A covert channel is simply using a communication protocol in a way it was not intended to be used or sending data without going through the proper access control mechanisms or channels. For example, in a Mandatory Access Control systems a user at secret has found a way to communicate information to a user at Confidential without going through the normal channels.

In this case the Urgent bit could be use for a few reasons:

1. It could be to attempt a Denial of service where the host receiving a packet with the Urgent bit set will give immediate attention to the request and will be in wait state until the urgent message is receive, if the sender does not send the urgent message then it will simply sit there doing nothing until it times out. Some of the TCP/IP stacks used to have a 600 seconds time out, which means that for 10 minutes nobody could use the port. By sending thousands of packet with the URGENT flag set, it would create a very effective denial of service attack.

2. It could be used as a client server application to transmit data back and forward without going through the proper channels. It would be slow but it is possible to use reserved fields and bits to transmit data outside the normal communication channels.

**IP CLASSES:**

For Class A, the addresses are 0.0.0.0 - 127.255.255.255

The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000

For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255.

The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000

For Class C, the addresses are 192.0.0.0 - 223.255.255.255

The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000

For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast)

The lowest Class D address is represented in binary as 11100000.00000000.00000000.00000000

For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage)

The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000

Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called **"signature-based detection."**

The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

**The actual IP address (IPv4) is composed of 32 bits. An IPv6 address is composed of 128 bits.**

**Classification:**

According to the AIO 3rd edition, these are the necessary steps for a proper classification program:

1. Define classification levels.

2. Specify the criteria that will determine how data is classified.

3. Have the data owner indicate the classification of the data she is responsible for.

4. Identify the data custodian who will be responsible for maintaining data and its security level.

5. Indicate the security controls, or protection mechanisms, that are required for each classification level.

6. Document any exceptions to the previous classification issues.

7. Indicate the methods that can be used to transfer custody of the information to a different data owner.

8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.

9. Indicate termination procedures for declassifying the data.

10. Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels

**IPSec:**

In tunnel mode, the entire packet is encrypted and encased into an IPSec packet.

In transport mode, only the datagram (payload) is encrypted, leaving the IP address visible within the IP header.

Authentication mode and safe mode are not defined IPSec operational modes.

**IPSec Transport mode:**

* Set-up when end-point is host or communications terminates at end-points
* If used in gateway-to-host communication, gateway must act as host
* When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet

**IPSec Tunnel mode:**

* Fundamentally an IP tunnel with encryption and authentication
* Have two sets of IP headers
* Established for gateway service

IPSec provides confidentiality and integrity to information transferred over IP networks **through network** (not transport) layer encryption and authentication. All other statements are correct.

**IP**

This IP address contains the information that aids in routing the information to the destination address. It is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.

Within an isolated network, you can assign IP addresses at random as long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates.

The four numbers in an IP address are used in different ways to identify a particular network and a host on that network. Four regional Internet registries -- ARIN, RIPE NCC, LACNIC and APNIC -- assign Internet addresses from the following three classes.

- Class A - supports 16 million hosts on each of 126 networks

- Class B - supports 65,000 hosts on each of 16,000 networks

- Class C - suports 254 hosts on each of 2 million networks

The number of unassigned Internet addresses is running out, so a new classless scheme called CIDR is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6.

IP addresses do not protect resources from intrusion.

Encapsulation is a technique used to add header information to the protocol data unit from the layer above.

Broadcasts are packets that are transmitted to every node on a local network segment.

**If the protocol field has a value of 6 then it would indicate it was TCP.**

**ICMP. Is incorrect because the value for an ICMP protocol would be 1.**

**UDP. Is incorrect because the value for an UDP protocol would be 17.**

**IGMP. Is incorrect because the value for an IGMP protocol would be 2.**

**Network File System (NFS)** is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture.

**Piggy Backing**

In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain. The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act.

To describe the act of an unauthorized person who follows someone to a restricted area without the consent of the authorized person, the term tailgating is also used. "Tailgating" implies without consent (similar to a car tailgating another vehicle on the freeway), while "piggybacking" usually implies consent of the authorized person.

Piggybacking came to the public's attention particularly in 1999, when a series of weaknesses were exposed in airport security. While a study showed that the majority of undercover agents attempting to pass through checkpoints, bring banned items on planes, or board planes without tickets were successful, piggybacking was revealed as one of the methods that was used in order to enter off-limits areas.

**Concealing**

Concealment (also called abscondence or hiding) is obscuring something from view or rendering it inconspicuous, the opposite of exposure. A military term is CCD: camouflage (object looks like its surroundings), concealment (object cannot be seen), and deception (object looks like something else); in a broad sense, all three are forms of concealment.

The objective of hiding is often to keep the presence of an object or person secret, but in other cases not the presence is a secret, but only the location.

This can be a weakness for **Callback systems.** The modem calls the registered telephone number and if call forwarding is enabled, the call can be forwarded anywhere and the modem/system has no idea or control over that.

**A between-the-lines** entry attack is a wire tap. This would not be a weakness specifically of a callback system because this type of attack could impact any dial-up system.

The correct answer is **1024 to 49151 as it has been defined as REGISTERED PORTS by IANA.**

The other answers are not correct as they do not lie with in the range defined by IANA for registered ports.

**A bastion host** is a special purpose computer on a network specifically designed and configured to withstand attack. The computer hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of the firewall or in the DMZ and usually involves access from untrusted networks or computers.

**TCP Wrappers** can control when a UDP server starts but has little control afterwards because UDP packets can be sent randomly.

**A SYN attack** occurs when an attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to "time out" while waiting for the proper response, which makes the system crash or become unusable. A buffer overflow attack occurs when a process receives much more data than expected. One common buffer overflow attack is the ping of death, where an attacker sends IP packets that exceed the maximum legal length (65535 octets). A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets.

**ARP table poisoning,** also referred to as ARP cache poisoning, is the process of altering a system's ARP table so that it contains incorrect IP to MAC address mappings. This allows requests to be sent to a different device instead of the one it is actually intended for. It is an excellent way to fool systems into thinking that a certain device has a certain address so that information can be sent to and captured on an attacker's computer.

**Pivoting refers** to method used by penetration testers that uses compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines. For example, an attacker compromises a web server on a corporate network, the attacker can then use the compromised web server to attack other systems on the network. These types of attacks are often called multi-layered attacks. Pivoting is also known as island hopping.

Pivoting can further be distinguished into proxy pivoting and VPN pivoting:

Proxy pivoting generally describes the practice channeling traffic through a compromised target using a proxy payload on the machine and launching attacks from this computer.[1] This type of pivoting is restricted to certain TCP and UDP ports that are supported by the proxy.VPN pivoting enables the attacker to create an encrypted layer 2 tunnel into the compromised machine to route any network traffic through that target machine, for example to run a vulnerability scan on the internal network through the compromised machine, effectively giving the attacker full network access as if they were behind the firewall.

**A TCP Segment** is the group of TCP data tramsmitted at the Transport Layer. TCP is segment based network technology.

The message is sent to the transport layer, where TCP does its magic on the data. The bundle of data is now a segment. If the message is being transmitted over TCP, it is referred to as a “segment.” If it is being transmitted over UDP, it is referred to as a “datagram.

**Echo replies** outbound should be dropped, not allowed.

By allowing inbound echo requests and outbound echo replies, it makes it easier for attackers to learn about the internal network.

The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.

**Explicit Congestion Notification (ECN)** is an extension to the Internet Protocol and to the Transmission Control Protocol and is defined in RFC 3168 (2001). ECN allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.

Conventionally, TCP/IP networks signal congestion by dropping packets. When ECN is successfully negotiated, an ECN-aware router may set a mark in the IP header instead of dropping a packet in order to signal impending congestion. The receiver of the packet echoes the congestion indication to the sender, which reduces its transmission rate as though it detected a dropped packet.

The network layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

**The MAC address** is 48 bits long, 24 of which identify the vendor, as provided by the IEEE. The other 24 bits are provided by the vendor.