Name: Muhammad Ali Khan

ID: 15614

Sessional Assignment 2020

Subject: Advance Computer Networks (MS EE)

Submission date: 08th June 2020

IQRA NATIONAL UNIVERSITY PESHAWAR

Submitted to: Prof. DR Naeem Jan

Q1: Differentiate between a Hub, Switch and Router?

HUB

A hub is to send out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.

SWITCH

A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.

ROUTER

Router is actually a small computer that can be programmed to handle and route the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.

What Is the Difference?

HUB VS SWITCH

A hub works on the physical layer (Layer 1) of OSI model while Switch works on the data link layer (Layer 2). Switch is more efficient than the hub. A switch can join multiple computers within one LAN, and a hub just connects multiple Ethernet devices together as a single segment. Switch is smarter than hub to determine the target of the forwarding data. Since switch has a higher performance, its cost will also become more expensive.

SWITCH VS ROUTER

In the OSI model, router is working on a higher level of network layer (Layer 3) than switch. Router is very different from the switch because it is for routing packet to other networks. It is also more intelligent and sophisticated to serve as an intermediate destination to connect multiple area networks together. A switch

is only used for wired network, yet a router can also link with the wireless network. With much more functions, a router definitely costs higher than a switch.

HUB VS ROUTER

As mentioned above, a hub only contains the basic function of a switch. Hence, differences between hub and router are even bigger. For instance, hub is a passive device without software while router is a networking device, and data transmission form in hub is in electrical signal or bits while in router it is in form of packet.

CONCLUSION

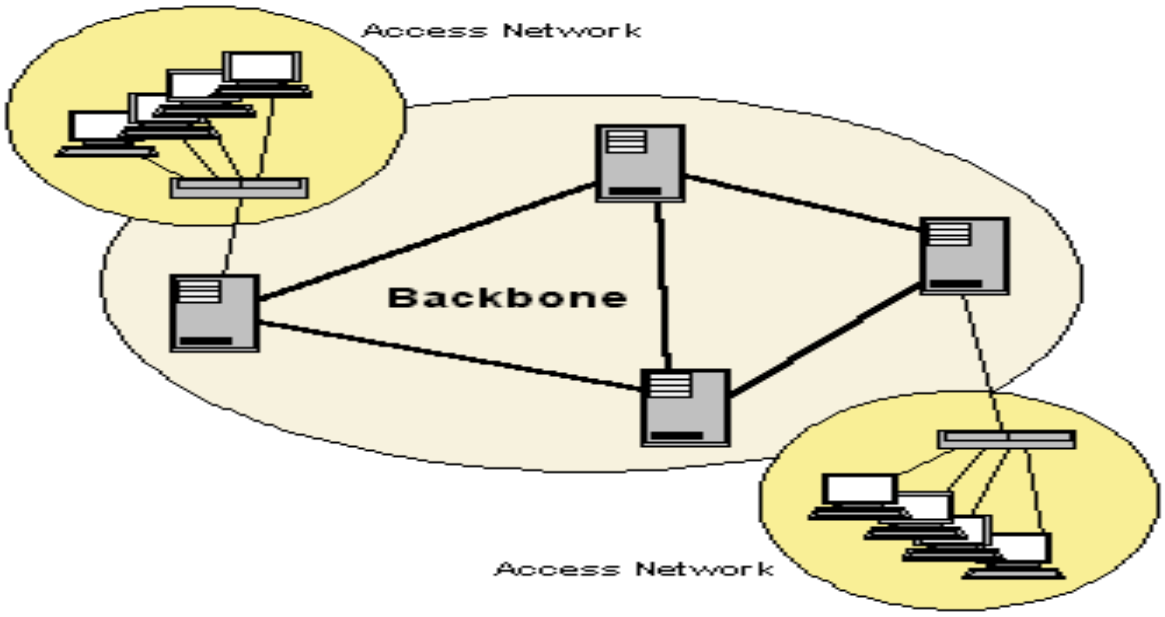
Hubs are “dumb” devices that pass on anything received on one connection to all other connections. Switches are semi-intelligent devices that learn which devices are on which connection. Routers are essentially small computers that perform a variety of intelligent tasks.

Q2: What does a backbone network means?

DEFINITION

A network backbone connects multiple networks together, allowing them to communicate with each other. A backbone is the part of the computer network infrastructure that interconnects different networks and provides a path for exchange of data between these different networks. A backbone may interconnect different local area networks in offices, campuses or buildings. When several local area networks (LAN) are being interconnected over a considerable area, the result is a wide area network (WAN), or metropolitan area network (MAN) if it happens to serve the whole city.

From Computer Desktop Encyclopedia
© 2004 The Computer Language Co. Inc.



Overview

Discrete networks have several ways of “talking” with each other. If you have two separate networks, say between two Point-of-presence” (PoP) locations they can send traffic over the public Internet, establish encrypted tunnels over the public Internet, or link together via a dedicated physical circuit which only connects between them.

StackPath uses dedicated physical circuits, also known as “dark fiber,” between its PoPs. This results in higher performance, better security, greater operational flexibility, and serves as one of the cornerstones of the Stackpath, platform. Current services utilize it and future services will continue to be built on top of it.

How a Network Backbone Works

Each PoP has a local switched network, which is separate and discrete from the other. The network backbone is a physical circuit that connects the discrete PoPs together, allowing one PoP’s local network to communicate with a second PoP’s local network, and vice-versa. The StackPath routing table controls which traffic utilizes the network backbone.

Q3: Explain the protocols used at different TCP/IP layers?

What is a Protocol?

A protocol is a set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another.

What is a Protocol Suit?

A protocol suite is a collection of protocols that are designed to work together.

Before TCP/IP became the de-facto standard other protocol suites like IPX and SPX were common (Novell).

Protocol Stacks

It is possible to write a single protocol that takes data from one computer application and sends it to an application on another computer.- A Single stack Protocol

The problem with this approach is that it very inflexible, as any changes require changing the entire application and protocol software.

The approach used in networking is to create layered protocol stacks.

Each level of the stack performs a particular function and communicates with the levels above and below it.

This layered arrangement is not confined to networking, and how it works is probably best understood if you compare it to real life example.

Lets take an example of a parcel service between two offices.

The task is simple – send parcels between people in each office.

We will divide the task into two distinct processes as follows:

1. Take a package, wrap it and address it.
2. Send it to the destination

At the receiving end

1. Receive the package
2. Deliver it to the recipient

Typically you would have an internal mail man that:

1. Collects the parcels from the senders and takes then to a mail dispatch room.
2. The parcels are placed in a van by the dispatcher and then driven to the remote office.

At the remote office

1. The parcels are received by the dispatcher and placed into a tray for the mail man
2. The mail man collects the parcels and delivers them to the recipients,

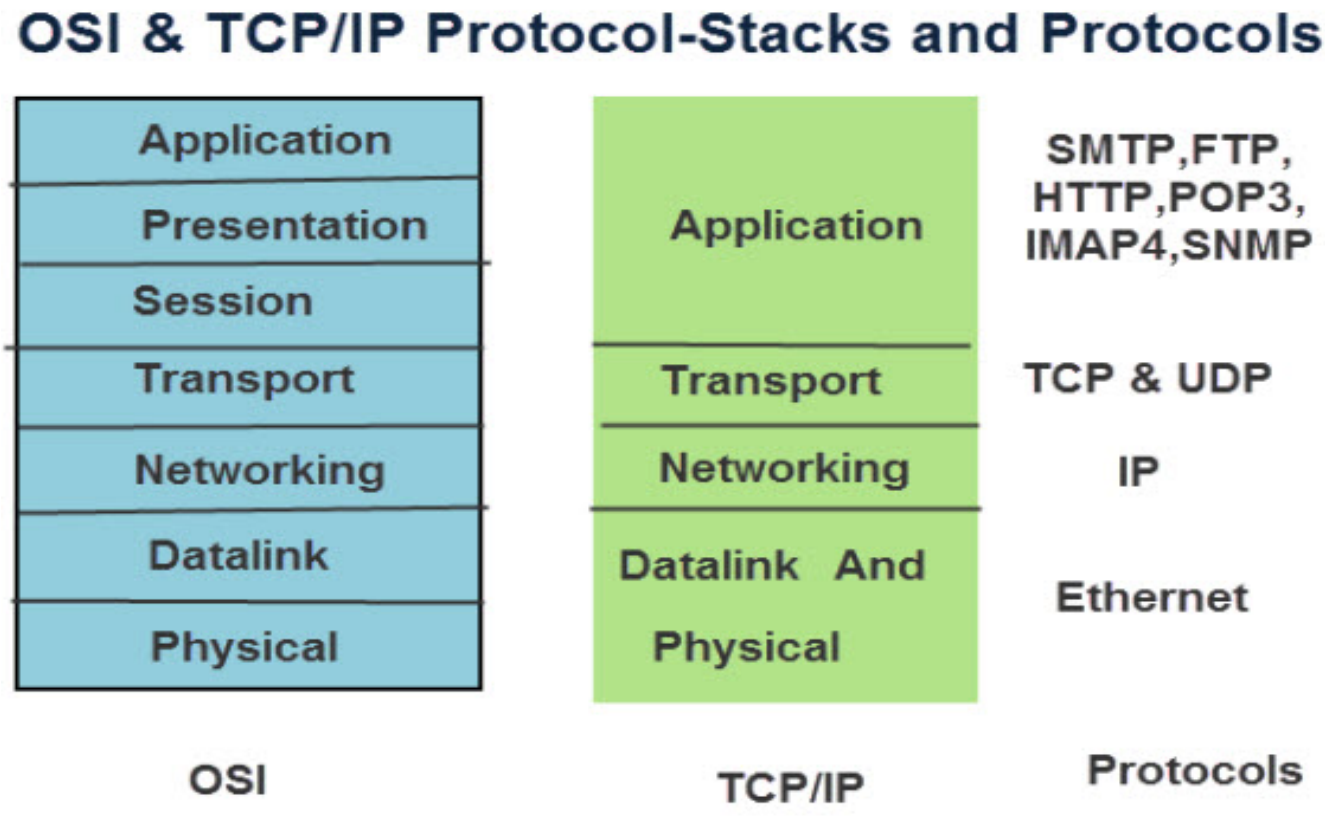
The OSI and TCP/IP Networking Models

All networking courses teach the **7-layer OSI model**.

It is important to understand that this **model** provides for a conceptual framework, and no modern protocols implement this model fully.

The **TCP/IP protocol suite** uses a **4-layer model**.

The diagram shows how the TCP/IP and OSI models compare



Q4: What is anonymous FTP?

Anonymous FTP (File Transfer Protocol)

Using the Internet's File Transfer Protocol (FTP), anonymous FTP is a method for giving users access to files so that they don't need to identify themselves to

the server. Using an FTP program or the FTP command interface, the user enters "anonymous" as a user ID. Usually, the password is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available.

If someone tells you to use anonymous FTP and gives you the server name, just remember to use the word "anonymous" for your user ID. Usually, you can enter anything as a password.

Anonymous File Transfer Protocol (FTP) allows the public to log into an FTP server with a common login (usually "ftp" or "anonymous") and any password (usually the person's e-mail address) to access the files on the server.

Anonymous FTP is beneficial for the distribution of large files to the public, without having to assign large numbers of login and password combinations for FTP access.

Using the Internet's File Transfer Protocol (FTP), anonymous FTP is a method for giving users access to files so that they don't need to identify themselves to the server. Using an FTP program or the FTP command interface, the user enters "anonymous" as a user ID.

Q5: What is subnet mask?

An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses (<network><host>). Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>) if additional subnetwork is needed. Use the Subnet Calculator to retrieve subnetwork information from IP address and Subnet Mask. It is called a subnet mask because it is used to identify network address of an IP address by preforming a bitwise AND operation on the netmask.

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts.

Class	Address	# of Hosts	Netmask (Binary)	Netmask (Decimal)
CIDR	/4	240,435,456	11110000 00000000 00000000 00000000	240.0.0.0
CIDR	/5	134,217,728	11111000 00000000 00000000 00000000	248.0.0.0
CIDR	/6	67,108,864	11111100 00000000 00000000 00000000	252.0.0.0
CIDR	/7	33,554,432	11111110 00000000 00000000 00000000	254.0.0.0

A	/8	16,777,216	11111111 00000000 00000000 00000000	255.0.0.0
CIDR	/9	8,388,608	11111111 10000000 00000000 00000000	255.128.0.0

Subnetting an IP network is to separate a big network into smaller multiple networks for reorganization and security purposes. All nodes (hosts) in a subnetwork see all packets transmitted by any node in a network. Performance of a network is adversely affected under heavy traffic load due to collisions and retransmissions.

Applying a subnet mask to an IP address separates network address from host address. The network bits are represented by the 1's in the mask, and the host bits are represented by 0's. Performing a bitwise logical AND operation on the IP address with the subnet mask produces the network address. For example, applying the Class C subnet mask to our IP address 216.3.128.12 produces the following network address:

IP: 1101 1000. 0000 0011. 1000 0000. 0000 1100 (216.003.128.012)

Mask: 1111 1111. 1111 1111. 1111 1111. 0000 0000 (255.255.255.000)

A subnet mask is a number that defines a range of IP address available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets). Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a router

A subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used).

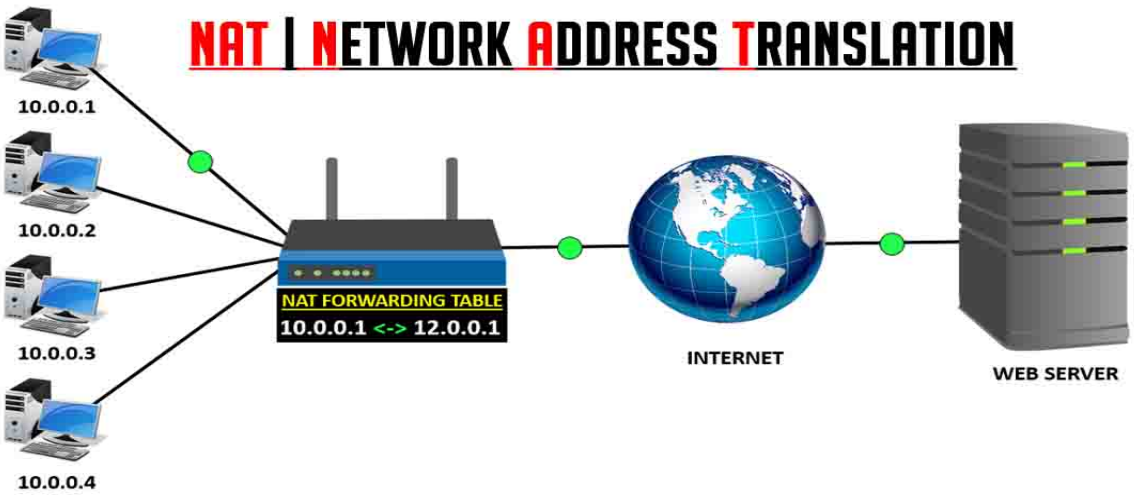
Q6: What is NAT?

NAT

Stands for "Network Address Translation." NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a Firewall, only allowing authorized systems to access the computers within the network.

Once a system from outside the network has been allowed to access a computer within the network, the IP address is then translated from the router's address to the computer's unique address. The address is found in a "NAT table" that defines the internal IP addresses of computers on the network. The NAT table also defines the global address seen by computers outside the network. Even though each computer within the local network has a specific IP address, external systems can only see one IP address when connecting to any of the computers within the network.

To simplify, network address translation makes computers outside the local area network (LAN) see only one IP address, while computers within the network can see each system's unique address. While this aids in network security, it also limits the number of IP addresses needed by companies and organizations. Using NAT, even large companies with thousands of computers can use a single IP address for connecting to the Internet. Now that's efficient.



Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

Q7: Differentiate between TCP and UDP?

What is TCP?

Transmission Control Protocol (TCP) is a connection-oriented protocol that computers use to communicate over the internet. It is one of the main protocols in TCP/IP networks. TCP provides error-checking and guarantees delivery of data and those packets will be delivered in the order they were sent.

What is UDP?

User Datagram Protocol (UDP) is a connectionless protocol that works just like TCP but assumes that error-checking and recovery services are not required. Instead, UDP continuously sends datagrams to the recipient whether they receive them or not.

What's the difference?

TCP and UDP have many differences and similarities. They are the most commonly used protocols for sending packets over the internet. They both work on the transport layer of the TCP/IP protocol stack and both use the IP protocol.

Let's take a look at some of the key differences.

Connection and connectionless

TCP is a connection-oriented protocol and UDP is a connection-less protocol. TCP establishes a connection between a sender and receiver before data can be sent. UDP does not establish a connection before sending data.

Q8: What are RIP and its key features?

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a dynamic routing protocol, which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol, which has AD value 120, and works on the application layer of OSI model. RIP uses port number 520.

RIP Concepts and Operation

The Routing Information Protocol (RIP) was the first commonly used IGP in the history of TCP/IP. Organizations used RIP inside their networks commonly in the 1980s, and into the 1990s. RIPv2, created in the mid-1990s, improved RIPv2, giving engineers an option for easy migration and co-existence to move from RIPv1 to the better RIPv2.

This second of four major sections of the chapter compares RIPv1 and RIPv2, while discussing a few of the core features that apply to both.

Features of Both RIPv1 and RIPv2

Like all IGPs, both RIPv1 and RIPv2 perform the same core features. That is, when using either RIPv1 or RIPv2, a router advertises information to help other routers learn routes; a router learns routes by listening to messages from other routers; a router chooses the best route to each subnet by looking at the metric of the competing routes; and the routing protocol converges to use new routes when something changes about the network.

RIPv1 and RIPv2 use the same logic to achieve most of those core functions. The similarities include the following:

Both send regular full periodic routing updates on a 30-second timer, with *full* meaning that the update messages include all known routes.

Both use split-horizon rules,

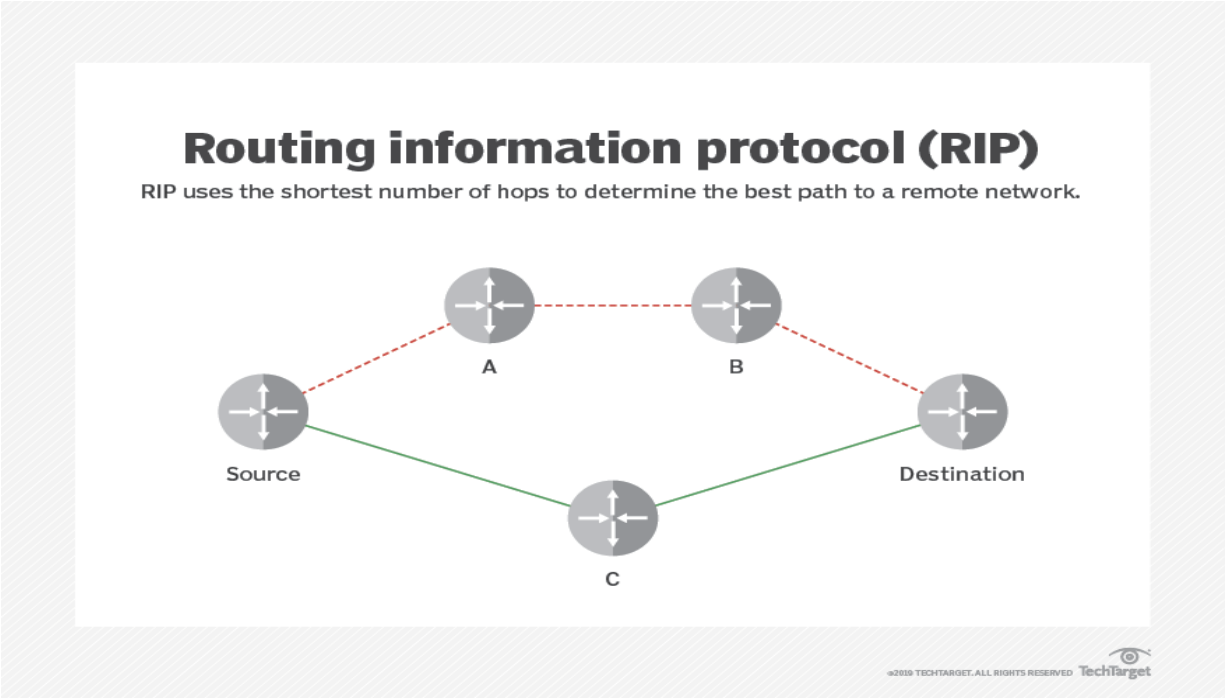
Both use hop count as the metric.

Both allow a maximum hop count of 15.

Both use route poisoning as a loop-prevention mechanism with hop count 16 used to imply an unusable route with an infinite metric.

Although you might be puzzled why the creators of RIPv2 made it so much like RIPv1, the goal was simple: interoperability. A network that used RIPv1 could slowly migrate to RIPv2, enabling RIPv2 on some routers on one weekend, some

more on the next, and so on. Done correctly, the network could migrate over time. The fact that both RIPv1 and RIPv2 used the same metric, and same loop-prevention mechanisms, allowed for a smooth migration.



Differences Between RIPv1 and RIPv2

Of course, RIPv2 needed to be better than RIPv1 in some ways, otherwise, what is the point of having a new version of RIP? RIPv2 made many changes to RIPv1: solutions to known problems, improved security, and new features as well. However, while RIPv2 improved RIP beyond RIPv1, it did not compete well with OSPF and EIGRP, particularly due to somewhat slow convergence compared to OSPF and EIGRP. However, for the sake of completeness, the next few pages walk through a few of the differences.

Q9: Explain what is a firewall?

DIFINITION

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

Types of firewalls.

1. Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

2. Stateful inspection firewall

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

3. Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

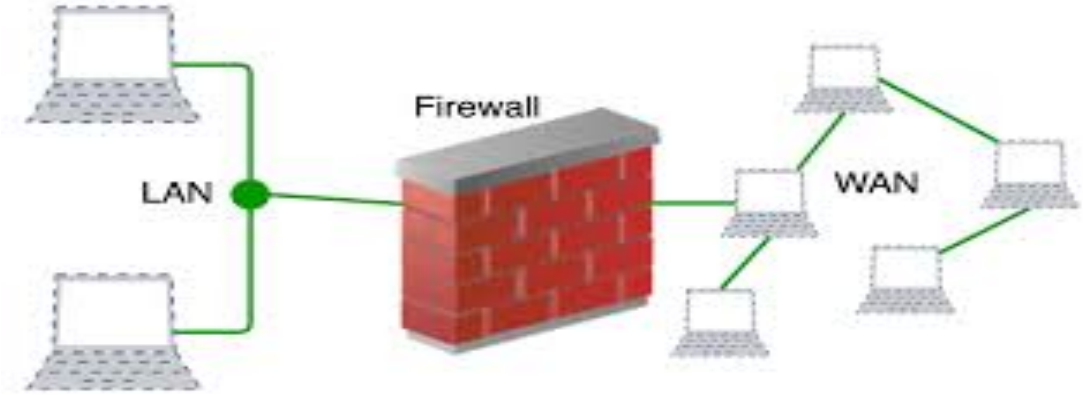
4. Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying Next-generation firewall to block modern threats such as advanced malware and application-layer attacks.

According to Gartner, Inc.’s definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps

- Upgrade paths to include future information feeds
- Techniques to address evolving security threats



CONCLUSION

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet (the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Q10: What is NOS?

A network operating system (NOS) is an operating system that manages network resources essentially, A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations an operating system that includes special functions for connecting computers and devices into a local area network (LAN). The NOS manages multiple requests (inputs) concurrently and provides the security necessary in a multiuser environment. It may be a completely self-contained operating system, such as NetWare, UNIX, Windows 2000, or Mac OS X, or it may require an existing operating system in order to function (e.g., Windows 3.11 for Workgroups requires DOS; LAN Server requires OS/2; LANtastic requires DOS). In addition to file and print services, a NOS may also offer directory services and a messaging system (email), as well as network management and multiprotocol routing capabilities

The salient features of network operating systems are:

- Basic operating system features support like protocol support, processor support, hardware detection and multiprocessing support for applications
- Security features like authentication, restrictions, authorizations and access control
- Features for file, Web service, printing and replication
- Directory and name services management
- User management features along with provisions for remote access and system management
- Internetworking features like routing and WAN ports
- Clustering capabilities

A network operating system is an operating system designed for the sole purpose of supporting workstations, database sharing, and application sharing and file and printer access sharing among multiple computers in a network. Certain standalone operating systems, such as Microsoft Windows NT and Digital's OpenVMS, come with multipurpose capabilities and can also act as network operating systems. Some of the most well-known network operating systems include Microsoft Windows Server 2003, Microsoft Windows Server 2008, Linux and Mac OS X.

Network Operating System is a computer operating system that facilitates to connect and communicate various autonomous computers over a network. An Autonomous computer is an independent computer that has its own local memory, hardware, and O.S. It is self-capable to perform operations and processing for a single user. They can either run the same or different O.S.

The Network O.S. mainly runs on a powerful computer, that runs the server program. It facilitates the security and capability of managing the data, user, group, application, and other network functionalities. The main advantage of using a network o.s. is that it facilitates the sharing of resources and memory amongst the autonomous computers in the network. It can also facilitate the client computers to access the shared memory and resources administered by the Server computer. In other words, the Network O.S. is mainly designed to allow multiple users to share files and resources over the network.

The Network O.S. is not transparent in nature. The workstations connected in the network are aware of the multiplicity of the network devices. The Network Operating Systems can distribute their tasks and functions amongst connected nodes in the network, which enhances the system overall performance. It can allow multiple access to the shared resources concurrently, which results in efficiency. One of the major importance of using a Network O.S. is remote

access. It facilitates one workstation to connect and communicate with another workstation in a secure manner. For providing security, it has authentication and access control functionality. The network o.s. implements a lot of protocols over the network, which provides a proper implementation of the network functionalities. One drawback of Network O.S. is its tightly coupled nature in the network.

Some examples of Network O.S. are Novel Netware, Microsoft Windows server (2000, 2003, 2008), Unix, Linux, etc.

There are mainly two types of Network O.S., they are:

Peer-to-Peer

Client-Serve

Peer-to-Peer

Peer-to-Peer Network Operating System is an operating system in which all the nodes are functionally and operationally equal to each other. No one is superior or inferior. They all are capable to perform similar kinds of tasks. All the nodes have their own local memory and resources. Using the Network O.S., they can connect and communicate with each other. They can also share data and resources with one another. One node can also communicate and share data and resources with a remote node in the network by using the authentication feature of the Network O.S. The nodes are directly connected with each other in the network with the help of a switch or a hub.

Following are the advantages of the Peer-to-Peer Network Operating System:

- Easy to install and setup.
- The setup cost is low.
- There is no requirement for any specialized software.
- The sharing of information and resources is fast and easy.

Following are the disadvantages of the Peer-to-Peer Network Operating System:

The performance of autonomous computers may not be so good when sharing some resources.

- There is no centralized management.
- It is less secure.
- It does not have backup functionalities.
- There is no centralized storage system.

Client-Server

The Client-Serve Networking Operating System operates with a single server and multiple client computers in the network. The Client O.S. runs on the client machine, while the Network Operating System is installed on the server machine. The server machine is a centralized hub for all the client machines. The client machines generate a request for information or some resource and forward it to the server machine. The server machine, in turn, replies to the client machine by providing appropriate services to it in a secure manner. The server machine is a very powerful computer that is capable of tackling large calculations and operations. It can also have the ability to administer the whole network and its resources. It can be multiprocessing in nature, which can process multiple client requests at the same time. The Network O.S. enhances the reach of client machines by providing remote access to other nodes and resources of the network in a secure manner.

Following are the advantages of the Client-Server Network Operating System:

- It has centralized control and administration.
- It has a backup facility for lost data.
- Multiple clients can access the shared data and resources concurrently.
- It has better reliability and performance.

Following are the disadvantages of the Client-Server Network Operating System:

The setup cost is very high.

- There is a requirement of specialized software for client and server machines to function properly.
- There is a need for an administrator to administer the network.
- There may be network failure, in case of central server failure.
- A huge amount of client requests may overload the server.

Following are the common functionalities of the Network Operating System:

1. Data and Resource sharing
2. Performance
3. Security
4. Robustness
5. Scalability
6. Memory management

Q11: What is Denial of Service (DoS)?

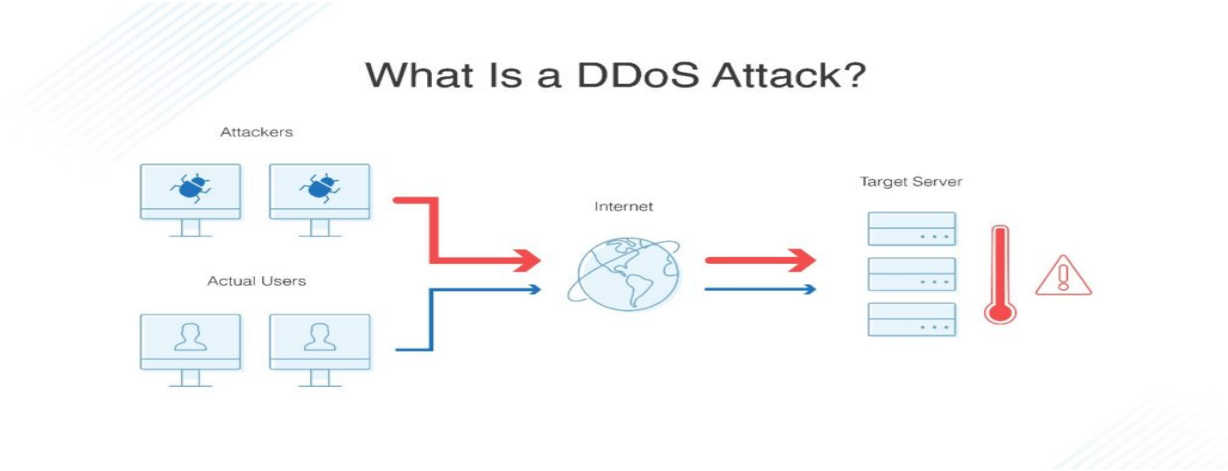
DOS

A denial of service (DoS) event is a cyber attack in which hackers or cybercriminals seek to make a host machine, online service or network resource unavailable to its intended users.
Distributed denial of service attacks may be the most well-known type of hacking incident – the 2018 GitHub and 2016 Dyn DDoS attacks being the most prominent – but there are many other kinds of denial of service attacks that don't necessarily involve the distributed or botnet approach. In virtually all cases, however, denial of service events are characterized by the target machine or service getting flooded with incoming traffic to the point where processing or bandwidth resources are overwhelmed and taken offline.

Origins of Denial of Service Threats

In conventional denial of service attacks, the hacker transmits multiple requests to the target machine or service with fictitious return Internet Protocol (IP) addresses. When the server attempts to authenticate these addresses, it encounters a wave of error code responses, setting off a recurring chain of SMTP traffic that can quickly saturate the server. Similarly, with a Smurf Attack, the hacker would broadcast packets to multiple hosts with a spoofed IP address belonging to those target machines. When the recipient host machines respond, they effectively flood themselves with responding packet traffic.

In a SYN flood, an attacker takes advantage of the TCP 3-Way Handshake (SYN, SYN-ACK, ACK) process to take a service offline. In the 3-Way Handshake, server A would initiate a TCP Synchronize request message to server B. On receiving the request, host B (the target machine) sends a SYNchronize-ACKnowledgement packet back to server A. It's at this point that the denial of service attack occurs. In a legitimate exchange to establish a TCP socket connection, the next step would be for host A to send an Acknowledge message back to host B, but when the hacker controlling host A prevents this from happening, the handshake can't be completed. The upshot is that host B has a connected port that's unavailable for additional requests. When the attacker sends repeated requests of this nature, all available ports on host B can quickly hang up and become unavailable.



In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Q12: What is piggybacking?

Piggybacking -

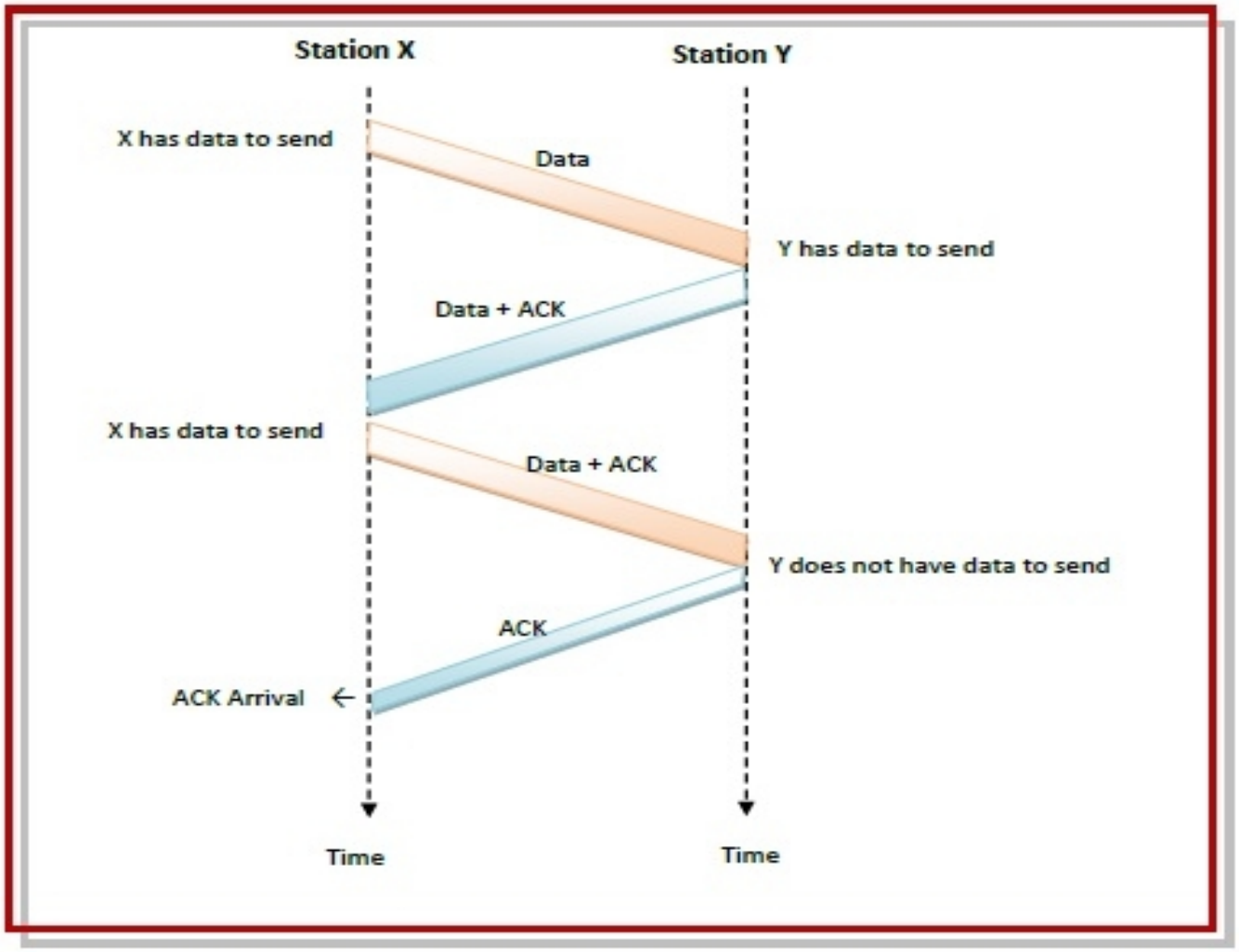
Gaining access to a restricted communications channel by using the session another user already established. Piggybacking can be defeated by logging out before walking away from a workstation or terminal or by initiating a screensaver that requires re-authentication when resuming. See replay attack and Hijacking

Using a Wi-Fi hotspot of neighbors who have not secured their network. See WI-FI Piggybacking and WI-FI Hotspot

(3) Embedding the names of popular brands or companies into the hidden meta-data of a Web page in order to rank high up on a search engine's results page.

In reliable full - duplex data transmission, the technique of hooking up acknowledgments onto outgoing data frames is called piggybacking.

In two-way communication, wherever a frame is received, the receiver waits and does not send the control frame back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.



The following diagram illustrates the three scenarios

Working Principle

Suppose that there are two communication stations X and Y. The data frames transmitted have an acknowledgment field, *ack* field that is of a few bits length. Additionally, there are frames for sending acknowledgments, ACK frames. The purpose is to minimize the ACK frames.

The three principles governing piggybacking when the station X wants to communicate with station Y are:

1. If station X has both data and acknowledgment to send, it sends a data frame with the *ack* field containing the sequence number of the frame to be acknowledged.

2. If station X has only an acknowledgment to send, it waits for a finite period of time to see whether a data frame is available to be sent. If a data frame becomes available, then it piggybacks the acknowledgment with it. Otherwise, it sends an ACK frame.
3. If station X has only a data frame to send, it adds the last acknowledgment with it. The station Y discards all duplicate acknowledgments. Alternatively, station X may send the data frame with the *ack* field containing a bit combination denoting no acknowledgment.

Q13: What is DNS?

DNS

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

The Domain Name System resolves the names of Internet sites with their underlying IP addresses adding efficiency and even security in the process. Each device connected to the Internet has a unique IP address, which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00: 2048:1:c629: d7a2 (in IPv6).

The Domain Name System (DNS) is one of the foundations of the Internet, yet most people outside of networking probably don't realize they use it every day to do their jobs, check their email or waste time on their smartphones. At its most basic, DNS is a directory of names that match with numbers. The numbers, in this case are IP addresses, which computers use to communicate with each other. Most descriptions of DNS use the analogy of a phone book, which is fine for people over the age of 30 who know what a phone book is.

How DNS servers work

The DNS directory that matches name to numbers isn't located all in one place in some dark corner of the internet. Like the Internet itself, the directory is distributed around the world, stored on domain name servers that all communicate with each other on a very regular basis to provide updates and redundancies. With more than 332 million domain names listed at the end of 2017, a single directory would be very large indeed.

Each named site can correspond to more than one IP address. In fact, some sites have hundreds or more IP addresses that correspond with a single domain name. For example, the server your computer reaches for **www.google.com** is

likely completely different from the server that someone in another country would reach by typing the same site name into their browser.

Another reason for the distributed nature of the directory is the amount of time it would take for you to get a response when you were looking for a site if there was only one location for the directory, shared among the millions, probably billions, of people also looking for information at the same time. That's one long line to use the phone book.

Instead, DNS information is shared among many servers, but is also cached locally on client computers. Chances are that you use google.com several times a day. Instead of your computer querying the DNS name server for the IP address of google.com every time, that information is saved on your computer so it doesn't have to access a DNS server to resolve the name with its IP address. Additional caching can occur on the routers used to connect clients to the internet, as well as on the servers of the user's Internet Service Provider (ISP). With so much caching going on, the number of queries that actually make it to DNS name servers is a lot lower than it would seem.

CONCLUSION

The Domain Name System (or DNS) converts human readable domain names (like: www.google.com) into Internet Protocol (IP) addresses (like: 173.194.39.78).

Computers can only communicate using series of numbers, so DNS was developed as a sort of "phone book" that translates the domain you enter in your browser into a computer readable IP.

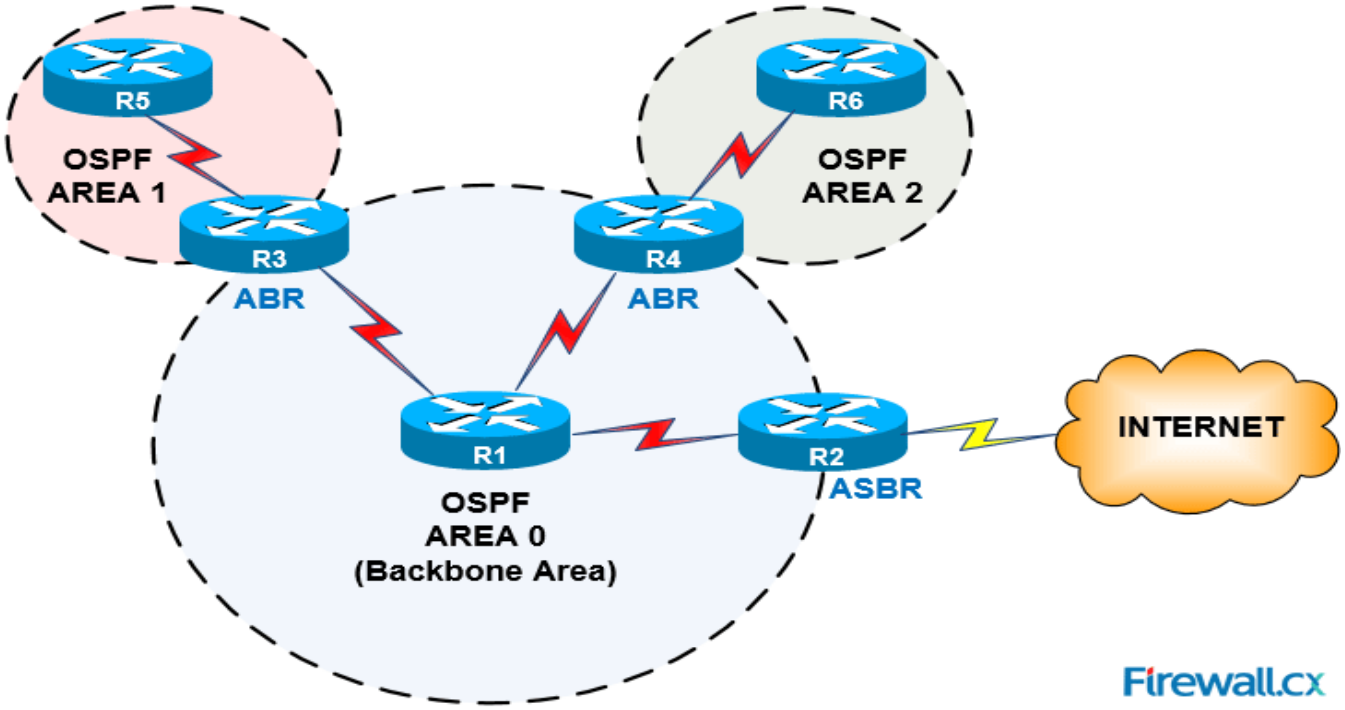
Q14: What is OSPF?

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network

Open Shortest Path First (OSPF) is a standard routing protocol that's been used the world over for many years. Supported by practically every routing vendor, as well as the open source community, OSPF is one of the few protocols in the IT industry you can count on being available just about anywhere you might need it.

Areas in OSPF are collections of routers grouped together. With the exception of area border routers, OSPF routers in one area don't neighbor with routers in other areas. Among other reasons, areas were once used to scale large OSPF networks.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.



The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.

Q15: What is a ping?

A ping is a signal sent to a host that requests a response. It serves two primary purposes

1) To check if the host is available and

2) To measure how long the response takes.

A ping request can be performed using a ping command, which is a standard command in most command line interfaces. Several network utilities provide a ping feature, which allows you to ping a server by simply entering the IP address or domain name. Most ping programs send multiple pings and provide and average of the pings at the end.

To perform a ping command from a command line interface, simply type "ping" followed by the IP address or domain name of the host you want to ping (e.g., ping 123.123.123.123)

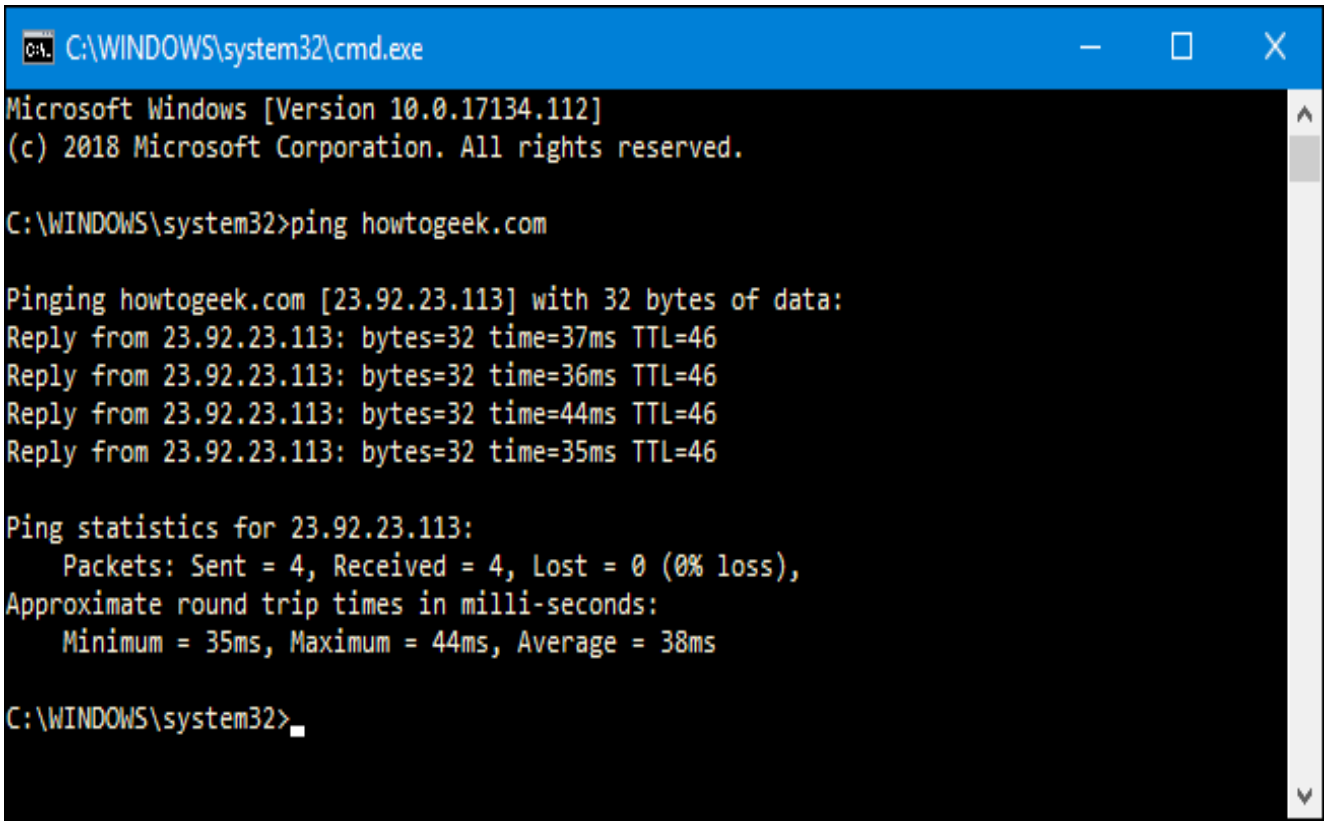
The ping itself consists of a single packet (often 32 or 56 bytes) that contains an "echo" request. The host, if available, responds with a single packet as a reply. The ping time, measured in milliseconds, is the round trip time for the packet to reach the host and for the response to return to the sender.

Ping response times are important because they add overhead to any requests made over the Internet. For example, when you visit a webpage the ping time is added to the time it takes a server to transmit the HTML and related resources to your computer. Pings are especially important in online gaming, where events happen in real-time.

While Internet connection speeds can affect pings, ping response time is often directly related to the physical distance between the source and destination systems. Therefore, a fast connection between New York and Tokyo will likely have a longer ping than a slow connection between New York and Philadelphia. Network congestion may slow down pings, which is why pings are often used for troubleshooting.

CONCLUSION

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.



Good Ping Response Time

< 30 ms - excellent ping; almost unnoticeable; ideal for online gaming

30 to 50 ms - average ping; still ok for online gaming

50 to 100 ms - somewhat slow ping time; not too noticeable for web browsing but may affect gaming

100 ms to 500 ms - slow ping; minimal effect on web browsing, but will create noticeable lag in online gaming

> 500 ms - pings of a half second or more will add a noticeable delay to all requests; typically happens when the source and destination are in different parts of the world

Q16: In a network that contains two servers and twenty workstations, where is the best place to install an Anti-Virus program?

The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

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.

What happens if a virus infects a computer without an antivirus?

If a virus infects a computer without an antivirus program, it may delete files, prevent access to files, send spam, spy on you, or perform other malicious actions. In some situations, a computer may not be compatible with your computer and the virus would only be used to spread to other computers.

Examples of antivirus programs

Today, there are dozens of different companies and antivirus products available for computers, servers, and even phones. New versions of Microsoft Windows even include Windows Defender, which with the latest versions of Windows can defend against computer viruses. Other well-known antivirus programs include **Norton antivirus** and **McAfee**, and popular free antivirus programs include **AVAST** and **AVG**

There are also antivirus programs that can run from a USB flash drive or a CD/DVD, making it portable and available to run without having to install software. Many portable antivirus programs provide a GUI to run antivirus scans, while others provide a command line interface to run scans from the command line. Additionally, some portable antivirus programs are bootable, meaning they can be used to scan a computer at boot up. A bootable antivirus program is especially helpful if a computer will not load into an operating system, due to a virus infection or other problems.

Antivirus software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers and such. Antivirus programs function to scan, detect and

remove viruses from your computer. There are many versions and types of anti-virus programs that are on the market. However, the prime objective of any antivirus program is to protect computers and remove viruses once detected.

Most antivirus programs incorporate both automated and manual filtering abilities. The instant scanning option may check files - downloaded from the Internet, discs that are embedded into the PC, and files that are made by software installers. The programmed scanning process may likewise check the entire hard drive on a day-to-day basis. The manual scanning system enables you to check single documents or even to scan the complete network at whatever point you feel it is necessary.

Q17: What is the difference between CSMA/CD and CSMA/CA?

CSMA/CD

CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection is a network protocol for carrier transmission. It is operated in the medium access control layer. It senses of the shared channel is busy for broadcasting and interrupt the broadcast until the channel is free. In CSMA/CD collision is detected by broadcast sensing from the other stations. Upon collision detection in CSMA/CD, the transmission is stopped and a jam signal is send by the stations and then station waits for a random time context before retransmission.

CSMA/CA:

CSMA/CD stands for Carrier Sense Multiple Access / Collision Avoidance is a network protocol for carrier transmission. Like CSMA/CD it is also operated in the medium access control layer. Unlike CSMA/CD (that is effective after a collision) CSMA / CA is effective before a collision.

S.no	CSMA/CD	CSMA/CA
1	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision
2	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks
3	It only reduces the recovery time	Whereas CSMA/ CA minimizes the possibility of collision.

4	CSMA / CD resend the data frame whenever a conflict occurs. CSMA / CD is used in 802.3 standard.	Whereas CSMA / CA will first transmit the intent to send for data transmission. While CSMA / CA is used in 802.11 standard.
5	It is more efficient than simple CSMA (Carrier Sense Multiple Access)	While it is similar to simple CSMA (Carrier Sense Multiple Access).

It is a network protocol for transmission. It operates in the Medium Access Control Layer. This protocol is effective before the collision

Another difference between CSMA CD and CSMA CA is where they are typically used. CSMA CD is used mostly in wired installations because it is possible to detect whether a collision has occurred. With wireless installations, it is not possible for the transmitter to detect whether a collision has occurred or not. That is why wireless installations often use CSMA CA instead of CSMA CD.

Q18: What is RSA Algorithm?

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography:

A client (for example browser) sends its public key to the server and requests for some data.

The server encrypts the data-using client's public key and sends the encrypted data.

Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

Algorithm

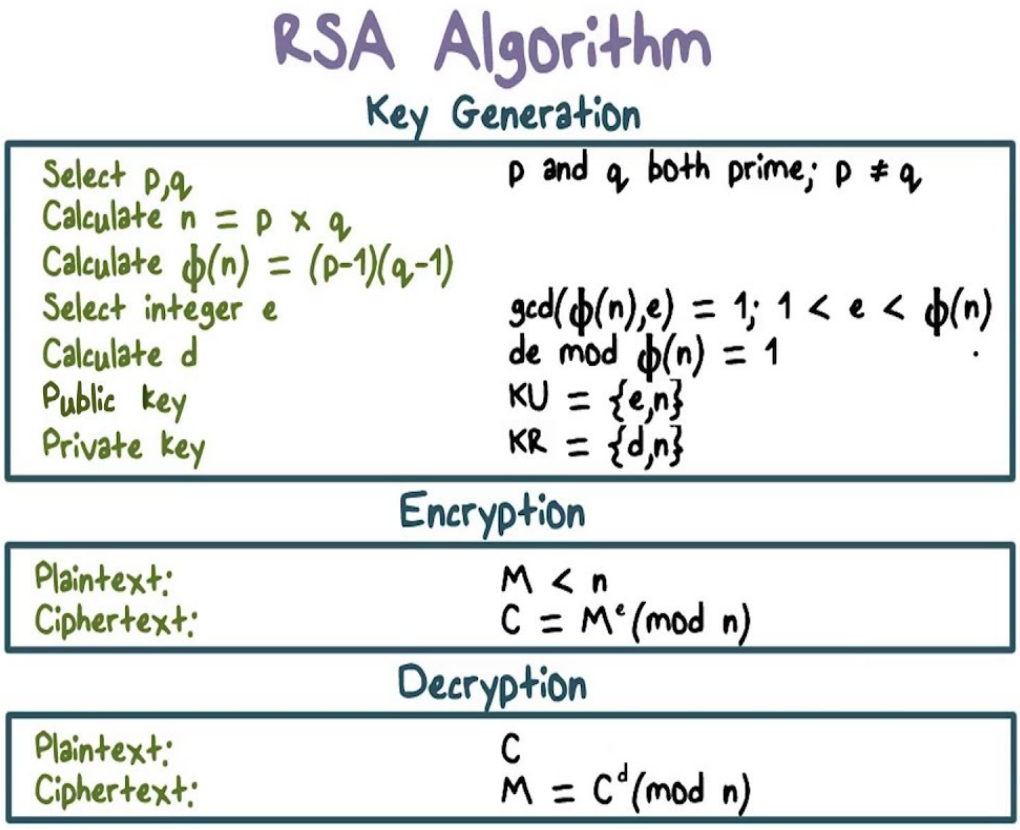
The RSA algorithm holds the following features −

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

is done to make encryption and signature verification faster on small devices like smart cards but small public exponents may lead to greater security risks.

Steps 4 and 5 can be performed with the extended Euclidean algorithm see modular arithmetic



The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of

two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Q19: What are the components of Protocol?

Protocol is a set of rules that governs communication. The key elements of protocol are syntax, semantics and timing. Syntax: Syntax refers the structure and format of the information data.

Protocols provide us with a medium and set of rules to establish communication between different devices for the exchange of data and other services.

Protocols are needed in every field like society, science & technology, Data Communication, media, etc. But in this blog, we'll mainly concentrate on the protocols used in computer networks and data communication. We'll further focus on the types, key elements, and functionalities of protocols. So, let's get started with the basics of protocols.

Levels of a Protocol

There are mainly three levels of a protocol, they are as follows:

1. Hardware Level: In this level, the protocol enables the hardware devices to connect and communicate with each other for various purposes.
2. Software Level: In the software level, the protocol enables different software to connect and communicate with each other to work collaboratively.
3. Application Level: In this level, the protocol enables the application programs to connect and communicate with each other for various purposes.

Hence protocols can be implemented at the hardware, software, and application levels.

Types of Protocols

Protocols can be broadly divided into the following two types:

- Standard Protocols
- Proprietary Protocols

Standard Protocols

A standard protocol is a mandated protocol for all devices. It supports multiple devices and acts as a standard.

Standard protocols are not vendor-specific i.e. they are not specific to a particular company or organization. They are developed by a group of experts from different organizations.

These protocols are publicly available, and we need not pay for them.

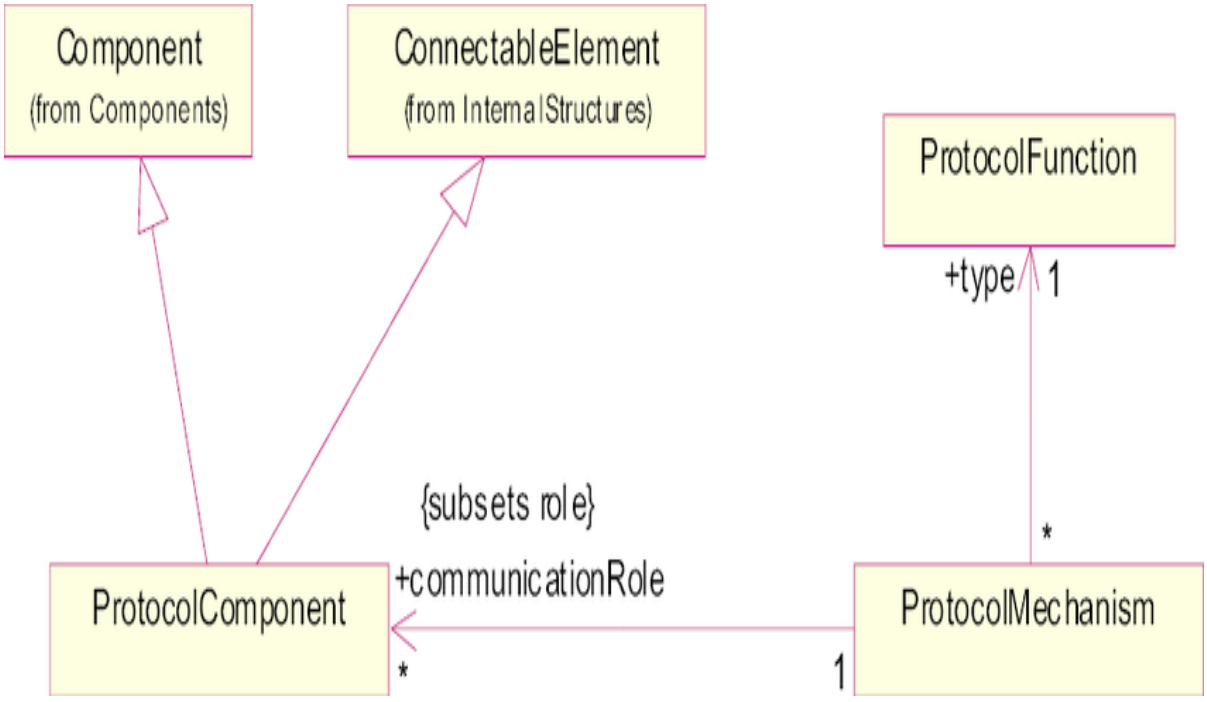
Some of the examples of Standard Protocols are *FTP, DNS, DHCP, SMTP, TELNET, TFTP, etc.*

Proprietary Protocols

Proprietary protocols are developed by an individual organization for their specific devices. We have to take permission from the organization if we want to use their protocols.

It is not a standard protocol and it supports only specific devices. We may have to pay for these protocols.

Some of the examples of Proprietary Protocols are *IMessage, Apple Talk, etc.*



Functions of protocols

Following are the main functionalities of a protocol:

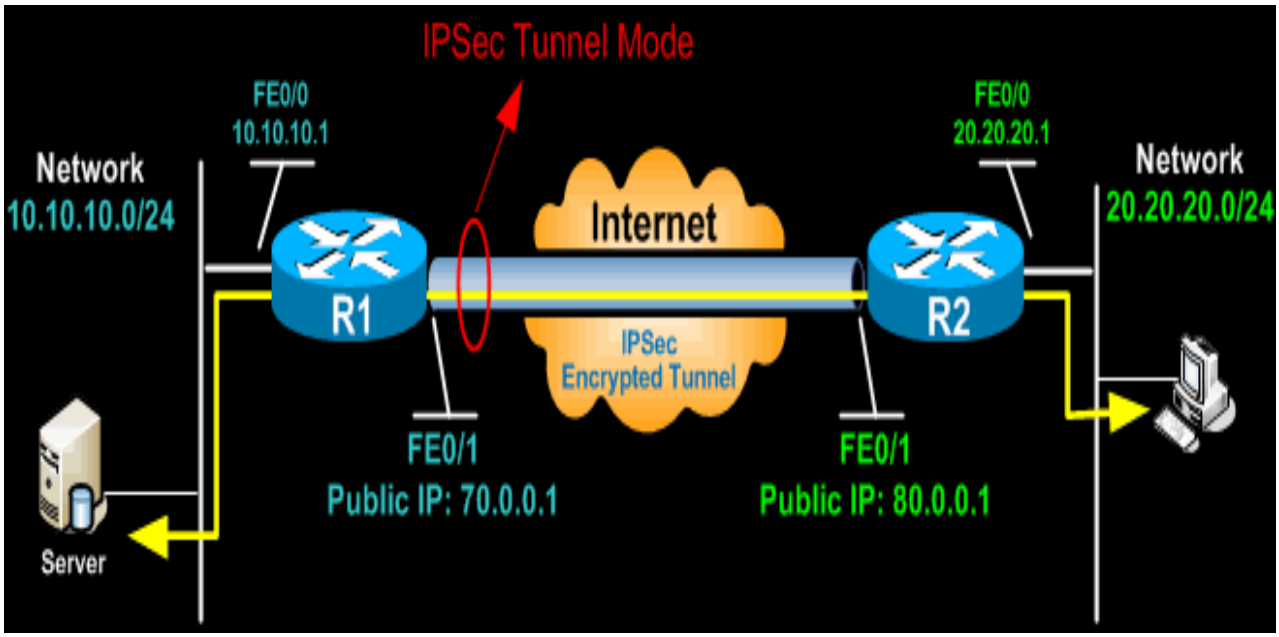
- **Data Sequencing**: It mainly refers to dive data into packets i.e. it divided the whole data into some packets.
- **Data Flow:** It mainly deals with sending data to the correct destination i.e. the flow of the data is correct or not.
- **Data Routing**: It refers to select the best path for data transmission between a sender and a receiver because there can be many routes from sender to receiver and you should select the best possible route.
- **Encapsulation**: It refers to the process of taking one protocol and transferring it to some other another protocol.
- **Segmentation & Reassembly**: It deals with segmenting the data message i.e. diving the data into packets when data flows from the upper protocol layer to lower, and reassembly is vice-versa of segmentation i.e. all the segmented packets are recollected in the correct order at the receiver side.
- **Connection Control:** It ensures connection oriented data transfer for lengthy data items.
- **Multiplexing:** It allows combining multiple transmission unit signals or channels of higher-level protocols in one transmission unit of a lower-level protocol. Multiplexing can be upward or downward.
- **Ordered Delivery**: Protocol facilitates ordered delivery of data, by providing a unique sequence number to each data packet. It is the function of the sender to maintain ordered delivery. By doing so, the receiver will receive the data in the same order as sent by the sender.
- **Transmission Services**: It mainly deals with priority, Quality of Service (QoS), and security of data packets.
- **Addressing:** It mainly deals with addressing levels, addressing scope, communication identifiers, and addressing modes.
- **Flow Control**: It facilitates to limit the flow of data. It is the function of the receiver's end to maintain flow control of data.
- **Error Control**: It deals with error detection (using the checksum bits) and its control. If any error is detected during the transmission of the data, the receiver sends a request for retransmission of data to the sender, and the corrupt data packet is discarded.

Q20: What is Tunnel mode?

Tunnel mode is most commonly used between gateways (Cisco routers or ASA firewalls), or at an end-station to a gateway, the gateway acting as a proxy for the

hosts behind it. Tunnel mode is used to encrypt traffic between secure IPSec Gateways, for example two Cisco routers connected over the Internet via IPSec VPN.

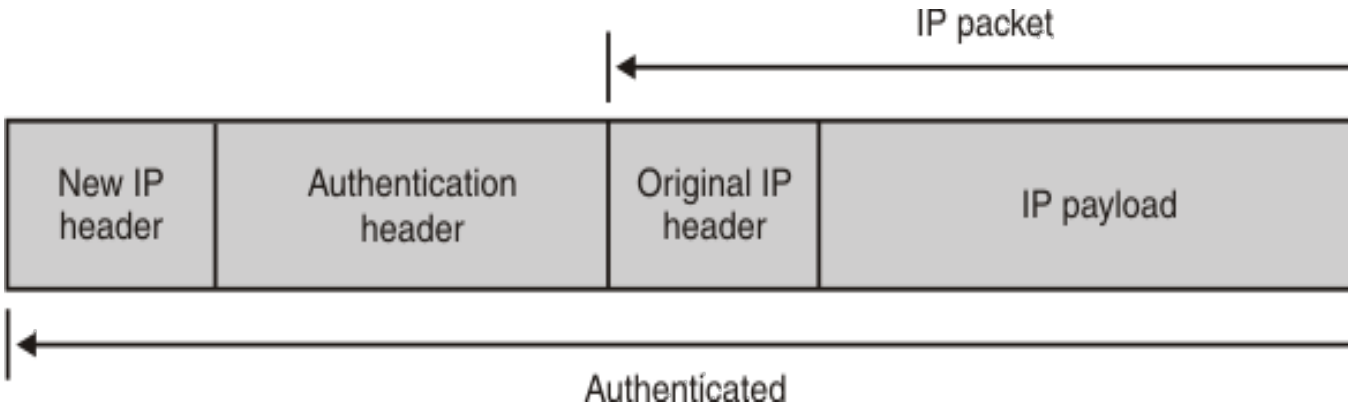
Configuration and setup of this topology is extensively covered in our Site-to-Site IPSec VPN article. In this example, each router acts as an IPSec Gateway for their LAN, providing secure connectivity to the remote network:



Tunnel mode encapsulation builds a new IP header containing the source and destination address of the security endpoints. When tunnel mode is used, the outer IP header reflects the source and destination of the security endpoints, which might or might not be the same as the original source and destination IP address of the data connection. The choice of transport or tunnel mode depends on the structure of the network and relies heavily on logical connections between the endpoints. Tunnel mode is required if one of the IKE peers is a security gateway that is applying IPSec on behalf of another host or hosts. A datagram that is encapsulated in tunnel mode is routed, or tunneled, through the security gateways, with the possibility that the secure IPSec packet will not flow through the same network path as the original datagram. To successfully encapsulate and send an outbound packet, the route table must contain a route that can be used to reach the security gateway, as well as a route that can be used to reach the data endpoint. If policy-based routing is being used on a TCP/IP stack where IP security is active, it is important to understand how the two functions interact.

In this figure shows an IPv4 packet that is encapsulated using AH in tunnel mode:

Figure. IPv4 packet encapsulated using AH in tunnel mode



- Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by another set of IP headers.
- It is widely implemented in site-to-site VPN scenarios.
- NAT traversal is supported with the tunnel mode.
- Additional headers are added to the packet; so the payload MSS is less.