ACN Ans (Click on the question, to directly jump on the answer)

Unit 1

Unit 2

Unit 3

Unit 4

Unit 5

Unit 1

1) How would you define is TCP/IP? Explain

TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet). The entire internet protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP, though others are included in the suite. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

The two main protocols in the internet protocol suite serve specific functions:

- TCP: defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.
- IP: defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

2) How would you elaborate The history of TCP/IP

The Defense Advanced Research Projects Agency (DARPA), the research branch of the U.S. Department of Defense, created the TCP/IP model in the 1970s for use in ARPANET(Advanced Research Projects Agency NET), a wide area network that preceded the internet. TCP/IP was originally designed for the Unix operating system, and it has been built into all of the operating systems that came after it. The TCP/IP model and its related protocols are now maintained by the Internet Engineering Task Force (IETF)

3) How would you describe TCP/IP model layers

TCP/IP functionality is divided into four layers, each of which include specific protocols.

- Application Layer

  Provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

- Transport Layer

  Responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

- Network Layer

  Also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

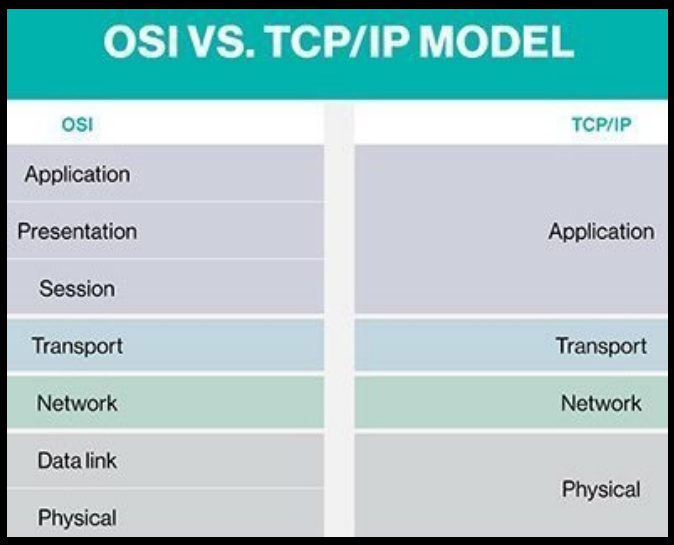
- Physical Layer

  Consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

4) What are the Advantages of TCP/IP

TCP/IP is non-proprietary and, as a result, is not controlled by any single company. Therefore, the internet protocol suite can be modified easily. It is compatible with all operating systems, so it can communicate with any other system. The internet protocol suite is also compatible with all types of computer hardware and networks.

5) How would you Differentiate Between TCP/IP and OSI



- TCP refers to Transmission Control Protocol. OSI refers to Open Systems Interconnection.
- TCP/IP has 4 layers. OSI has 7 layers.
- TCP/IP is more reliable. OSI is less reliable.
- TCP/IP does not have very strict boundaries. OSI has strict boundaries.
- TCP/IP follow a horizontal approach. OSI follows a vertical approach.
- TCP/IP uses both session and presentation layer in the application layer itself. OSI uses different session and presentation layers.
- TCP/IP developed protocols then model. OSI developed model then protocol.

6) What is Static routing? Explain

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in the event that dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Static routing may have the following uses:

- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.

- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.

- Static routing is often used as a complement to dynamic routing to provide a failsafe backup in the event that a dynamic route is unavailable.

- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

7) How would you elaborate different types of static routes in detail?

- Directly Connected Static Routes

  You must specify only the output interface (the interface on which all packets are sent to the destination network) in a directly connected static route. The router assumes the destination is directly attached to the output interface and the packet destination is used as the next-hop address. The next hop can be an interface, only for point-to-point interfaces. For broadcast interfaces, the next hop must be an IPv4/IPv6 address.

- Fully Specified Static Routes

  You must specify either the output interface (the interface on which all packets are sent to the destination network) or the next-hop address in a fully specified static route. You can use a fully specified static route when the output interface is a multi-access interface and you need to identify the next-hop address. The next-hop address must be directly attached to the specified output interface.

- Floating Static Routes

  A floating static route is a static route that the router uses to back up a dynamic route. You must configure a floating static route with a higher administrative distance than the dynamic route that it backs up. In this instance, the router prefers a dynamic route to a

floating static route. You can use a floating static route as a replacement if the dynamic route is lost.

Unit 2

1) What are the Interior Gateway Protocols? Explain

An interior gateway protocol (IGP) is a dynamic route update protocol used between routers that run on TCP/IP hosts within a single autonomous system. The routers use this protocol to exchange information about IP routes.

Some of the more common interior gateway protocols are:

- Routing Information Protocol (RIP)

  RIP uses a distance vector algorithm to calculate the best path to a destination based on the number of hops in the path. RIP has several limitations. Some of the limitations which exist in RIP Version 1 are resolved by RIP Version 2.

- RIP Version 2

  RIP Version 2 extends RIP Version 1. Among the improvements are support for multicasting and variable subnetting. Variable subnetting allows the division of networks into variable size subnets. For example, one route can represent addresses from 9.1.1.0 through 9.1.1.255 (the 9.1.1.0/255.255.255.0 subnet) while another can represent addresses from 9.2.0.0 through 9.2.255.255 (the 9.2.0.0/255.255.0.0 subnet).

- IPv6 RIP

  IPv6 RIP uses the same distance vector algorithm used by RIP to calculate the best path to a destination. It is intended to allow routers to exchange information for computing routes through an IPv6-based network.

- Open Shortest Path First (OSPF)

  OSPF uses a link state or shortest path first algorithm. OSPF's most significant advantage compared to RIP is the reduced time needed to converge after a network change. In general, OSPF is more complicated to configure than RIP and might not be suitable for small networks.

- IPv6 OSPF

  IPv6 OSPF also uses a link state or shortest path first algorithm to calculate the best path to a destination. IPv6 OSPF has the same advantages and more complicated configuration compared to IPv6 RIP, like OSPF compared to RIP.

2) How would you Elaborate RIP?

Routing Information Protocol (RIP) is an interior gateway protocol (IGP). IGP is a dynamic route update protocol used between routers that run on TCP/IP hosts within a single autonomous system. The routers use this protocol to exchange information about IP routes.

Some of the more common RIP protocols:

- Routing Information Protocol (RIP)

  RIP uses a distance vector algorithm to calculate the best path to a destination based on the number of hops in the path. RIP has several limitations. Some of the limitations which exist in RIP Version 1 are resolved by RIP Version 2.

- RIP Version 2

  RIP Version 2 extends RIP Version 1. Among the improvements are support for multicasting and variable subnetting. Variable subnetting allows the division of networks into variable size subnets. For example, one route can represent addresses from 9.1.1.0 through 9.1.1.255 (the 9.1.1.0/255.255.255.0 subnet) while another can represent addresses from 9.2.0.0 through 9.2.255.255 (the 9.2.0.0/255.255.0.0 subnet).

- IPv6 RIP

  IPv6 RIP uses the same distance vector algorithm used by RIP to calculate the best path to a destination. It is intended to allow routers to exchange information for computing routes through an IPv6-based network.

3) How would you Elaborate Interior Routing Protocols

All interior routing protocols perform the same basic functions. They determine the "best" route to each destination, and they distribute routing information among the systems on a

network. How they perform these functions, in particular, how they decide which routes are best, is what makes routing protocols different from each other.

There are several interior protocols:

- Routing Information Protocol (RIP)

  Interior protocol most commonly used on UNIX systems. RIP is included as part of the UNIX software delivered with most systems. It is adequate for local area networks and is simple to configure. RIP selects the route with the lowest "hop count" (metric) as the best route. The RIP hop count represents the number of gateways through which data must pass to reach its destination. RIP assumes that the best route is the one that uses the fewest gateways. This approach to route choice is called a distance-vector algorithm.

- Hello

  Protocol that uses delay as the deciding factor when choosing the best route. Delay is the length of time it takes a datagram to make the round trip between its source and destination. A Hello packet contains a time stamp indicating when it was sent. When the packet arrives at its destination, the receiving system subtracts the time stamp from the current time, to estimate how long it took the packet to arrive. Hello is not widely used. It was the interior protocol of the original 56 kbps NSFNET backbone and has had very little use otherwise.

- Intermediate System to Intermediate System (IS-IS)

  Interior routing protocol from the OSI protocol suite. It is a Shortest Path First (SPF) link-state protocol. It was the interior routing protocol used on the T1 NSFNET backbone, and it is still used by some large service providers.

- Open Shortest Path First (OSPF)

  Link-state protocol developed for TCP/IP. It is suitable for very large networks and provides several advantages over RIP.

4) How would you Elaborate Exterior Gateway Protocol

Exterior Gateway Protocol (EGP) is the mechanism that allows the exterior gateway of an autonomous system to share routing information with exterior gateways on other autonomous

systems. An autonomous system is a group of networks and gateways for which one administrative authority has responsibility.

Exterior Gateway Protocol (EGP) is a defunct routing protocol used in autonomous systems to exchange data between surrounding gateway sites. Border Gateway Protocol supplanted EGP, widely utilized by research institutes, universities, government agencies, and commercial companies (BGP). EGP is built on poll instructions to request update answers and periodic message exchange polling for neighbor reachability. RFC 904, which was issued in April of 1984, details EGP. External Gateway Protocol is another name for the Exterior Gateway Protocol.

5) Explain the core working of Working of EGP

Internet hosts used EGP for data table routing exchanges before BGP was introduced. Available routers, addresses, cost metrics, and each optimal route selection path are all listed in the EGP routing table. The EGP model is designed to automate limited events, actions, and transitions.

The EGP mechanisms are as follows:

- Obtain neighbors
- Keep an eye on your neighbors.
- Data is exchanged via update messages.
- EGP allows neighboring routers in different domains to share information, whereas Interior Gateway Protocols are utilized within a domain.

The Advanced Research Projects Agency Network's main routers use EGP to convey reachability to and from them (ARPANET). Individual source nodes in separate Internet administrative domains known as autonomous systems (ASs) sent information to the core routers, then relayed down via the backbone until it reached the destination network within another AS.

Unlike most other protocols, EGP is solely concerned with network reachability and uses no metrics to choose the optimum way.

6) How would you Elaborate OSPF?

OSPF (Open Shortest Path First) is a link state routing protocol. Because it is an open standard, it is implemented by a variety of network vendors. OSPF will run on most routers that doesn’t necessarily have to be Cisco routers (unlike EIGRP which can be run only on Cisco routers).

Here are the most important features of OSPF:

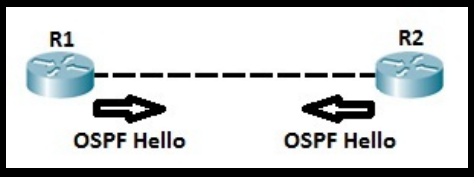
- A classless routing protocol
- Supports vlsm, cidr, manual route summarization, equal cost load balancing
- Incremental updates are supported
- Uses only one parameter as the metric – the interface cost.
- The administrative distance of ospf routes is, by default, 110.
- Uses multicast addresses 224.0.0.5 and 224.0.0.6 for routing updates.

Routers running OSPF have to establish neighbor relationships before exchanging routes. Because OSPF is a link state routing protocol, neighbors don't exchange routing tables. Instead, they exchange information about network topology. Each OSFP router then runs SFP algorithm to calculate the best routes and adds those to the routing table. Because each router knows the entire topology of a network, the chance for a routing loop to occur is minimal.

Each OSPF router stores routing and topology information in three tables:

- Neighbor table – stores information about OSPF neighbors
- Topology table – stores the topology structure of a network
- Routing table – stores the best routes
- OSPF neighbors

OSPF routers need to establish a neighbor relationship before exchanging routing updates. OSPF neighbors are dynamically discovered by sending Hello packets out each OSPF-enabled interface on a router. Hello packets are sent to the multicast IP address of 224.0.0.5.



7) What are the OSPF neighbor states? Explain

Before establishing a neighbor relationship, OSPF routers need to go through several state changes. These states are explained below.

1) Init state – a router has received a Hello message from the other OSFP router
2) 2-way state – the neighbor has received the Hello message and replied with a Hello message of his own
3) Exstart state – beginning of the LSDB exchange between both routers. Routers are starting to exchange link state information.
4) Exchange state – DBD (Database Descriptor) packets are exchanged. DBDs contain LSAs headers. Routers will use this information to see what LSAs need to be exchanged.
5) Loading state – one neighbor sends LSRs (Link State Requests) for every network it doesn't know about. The other neighbor replies with the LSUs (Link State Updates) which contain information about requested networks. After all the requested information have been received, other neighbor goes through the same process
6) Full state – both routers have the synchronized database and are fully adjacent with each other

8) How would you Describe OSPF Network Topology?

OSPF is capable of routing over every type of data link, but OSPF makes assumptions that do not hold true for all topologies. OSPF assumes that—within a subnet—all routers can communicate directly using multicasts and that no router is uniquely positioned in the topology. Both assumptions are fine for Ethernet: If five routers are attached to a switch, a multicast from one reaches the other four and each would be fine as a designated router (DR).

The aforementioned assumptions do not hold for nonbroadcast multiaccess (NBMA) environments. In a Frame Relay network, for example, multicasts and broadcasts are not supported on "NBMA" OSPF-network-type interfaces on Cisco routers.

The following are the OSPF network types available on Cisco router interfaces:

- Broadcast multiaccess
- Point-to-point
- Point-to-multipoint (default is point-to-multipoint broadcast; nonbroadcast option is available)
- Nonbroadcast multiaccess (NBMA)

To account for the lack of multicast and broadcast support inherent in NBMA OSPF-network-type interfaces on Cisco routers, multicasts are simulated by replicating an advertisement

to each neighbor. This chapter describes several strategies for dealing with neighbor discovery and communication in an NBMA topology.

9) Explain OSPF Route Stigmatization/Summarization

Area border routers (ABRs) send summary link advertisements to describe the routes to other areas. Depending on the number of destinations, an area can get flooded with a large number of link-state records, which can utilize routing device resources. To minimize the number of advertisements that are flooded into an area, you can configure the ABR to coalesce, or summarize, a range of IP addresses and send reachability information about these addresses in a single link-state advertisement (LSA). You can summarize one or more ranges of IP addresses, where all routes that match the specified area range are filtered at the area boundary, and the summary is advertised in their place.

For an OSPF area, you can summarize and filter intra-area prefixes. All routes that match the specified area range are filtered at the area boundary, and the summary is advertised in their place. For an OSPF not-so-stubby area (NSSA), you can only coalesce or filter NSSA external LSAs before they are translated into AS external LSAs and enter the backbone area. All external routes learned within the area that do not fall into the range of one of the prefixes are advertised individually to other areas.

In addition, you can also limit the number of prefixes (routes) that are exported into OSPF. By setting a user-defined maximum number of prefixes, you prevent the routing device from flooding an excessive number of routes into an area

10) How would Differentiate between IGP and EGP?

- IGP stands for Interior Gateway Protocol, while EGP stands for Exterior Gateway Protocol.
- Purpose: IGP is used to exchange routing information within a single autonomous system, while EGP is used to exchange routing information between different autonomous systems.
- Examples: OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) are examples of IGPs, while Border Gateway Protocol (BGP) is an example of EGP.

- Scope: IGPs are used for routing within a single autonomous system, while EGPs are used for routing between autonomous systems.

- Protocols: IGPs are typically used for routing within a local area network (LAN) or a wide area network (WAN), while EGPs are used for inter-network routing.

- Configuration: IGPs are typically configured on routers within an autonomous system, while EGPs are configured on routers that connect different autonomous systems.

- Routing tables: IGPs maintain a separate routing table for each autonomous system, while EGPs maintain a single routing table for all autonomous systems.

- Path selection: IGPs use algorithms such as open shortest path first (OSPF) to select the best path within an autonomous system, while EGPs use complex routing policies to select the best path between autonomous systems.

In summary, IGP is used to exchange routing information within a single autonomous system, while EGP is used to exchange routing information between different autonomous systems.

Unit 3

1) How would you elaborate What is policy-based routing?

Policy-based routing (PBR) is a technique that forwards and routes data packets based on policies or filters. Network administrators can selectively apply policies based on specific parameters such as source and destination IP address, source or destination port, traffic type, protocols, access list, packet size, or other criteria and then route the packets on user-defined routes.

The goal of PBR is to make the network as agile as possible. By defining routing behavior based on application attributes, PBR provides flexible, granular traffic-handling capabilities for forwarding packets. In this way, PBR enables network administrators to achieve optimal bandwidth utilization for business-critical applications.

2) How would you describe Problems Policy-Based Routing Addresses

Traditional routing systems route traffic based on the destination of the traffic. However, the relentless growth of cloud computing, mobility, and Web-based applications requires that the network know each application traffic type traversing the network. PBR handles each application type separately to effectively prioritize, segregate, and route traffic without compromising performance or availability.

Additionally, the complexity caused by voice, data, video, and applications running on the same network is making networks vulnerable to threats or rendering them unable to respond to threats. Today's core business applications are heavily targeted by cyber-attackers using multifaceted attacks. PBR enables network administrators to classify the traffic based on applications and mark them for further analysis to provide greater visibility, enforcement, control, and protection to network security.

3) What Can You Do with Policy-Based Routing? Explain

You can use PBR to:

- Prioritize applications by selecting high-bandwidth, low-latency links for important applications, when more than one link is available. For example, prioritize corporate data over a fast link and Internet browsing traffic over a slow link. (QoS)

- Load share by creating a fallback link for important traffic if the main link carrying the important application traffic suffers an outage.
- Segregate the traffic for deep inspection or analysis. The network administrator classifies application traffic that must go through a deep inspection and audit. Optionally, the network administrator can route this traffic to a different device.
- Control the flow of subscriber traffic in service provider networks through traffic management policies and rules based on subscribers' profiles. For example, PBR can prioritize and route certain types of application traffic to a specific routing path as per SLA or by placing certain user requests higher than others (for example, gold, silver, bronze).
- Provide a guaranteed service-level agreement (SLA) for the delivery of the certain traffic (such as video traffic) by ensuring that the approved traffic receives the appropriate priority, routing, and bandwidth required to ensure the maximum user quality of experience.
- Send specific applications for WAN optimization. For instance, certain applications are optimized for transfer over WAN links. With PBR, the network administrator can classify the traffic based on applications, and send traffic to the WAN optimizer to speed up access to important applications and data.

4) How would you Discuss Securing BGP

The Border Gateway Protocol (BGP) is the protocol used throughout the Internet to exchange routing information between networks. It is the language spoken by routers on the Internet to determine how packets can be sent from one router to another to reach their final destination. BGP has worked extremely well and continues to the be protocol that makes the Internet work.

The challenge with BGP is that the protocol does not directly include security mechanisms and is based largely on trust between network operators that they will secure their systems correctly and not send incorrect data. Mistakes happen, though, and problems could arise if malicious attackers were to try to affect the routing tables used by BGP.

5) How would you define BGP Sessions (Internal and External)

BGP supports these session types between neighbors:

- Internal (iBGP) - Runs between routers in the same autonomous system.
- External (eBGP) - Runs between routers in different autonomous systems.

When you send routes to an external peer, the local AS number is prepended to the AS path. Routes received from an internal neighbor have the same AS path that the route had when it was received from an external peer.

BGP sessions might include a single metric (Multi-Exit Discriminator or MED) in the path attributes. Smaller values are preferred. These values are used to break ties between routes with equal preference from the same neighbor AS.

Internal BGP sessions carry at least one metric in the path attributes that BGP calls the local preference. The size of the metric is identical to the MED. Use of these metrics depends on the type of internal protocol processing.

For BGP implementation, external peers are directly attached to a shared subnet and advertise next hops that are host addresses on the subnet. If you enable the multihop option in the BGP peer template during configuration, this constraint is relaxed.

6) What are the BGP Path Attributes? Explain.

A path attribute is a list of AS numbers that a route has traversed to reach a destination. BGP uses path attributes to provide more information about each route and to help prevent routing loops in an arbitrary topology. You can also use path attributes to determine administrative preferences.

BGP collapses routes with similar path attributes into a single update for advertisement. Routes that are received in a single update are readvertised in a single update. The churn caused by the loss of a neighbor is minimized, and the initial advertisement sent during peer establishment is maximally compressed.

BGP does not read information that the kernel forms message by message. Instead, it fills the input buffer. BGP processes all complete messages in the buffer before reading again. BGP also performs multiple reads to clear all incoming data queued on the socket.

Attribute and their description:

- AS_PATH
  Identifies the autonomous systems through which routing information carried in an UPDATE message passed. Components of this list can be AS_SETs or AS_SEQUENCES.

- NEXT_HOP
  Defines the IP address of the border router that should be used as the next hop to the destinations listed in the UPDATE message.

- MULTI_EXIT_DISC
  Discriminates among multiple exit or entry points to the same neighboring autonomous system. Used only on external links.

- LOCAL_PREF
  Determines which external route should be taken and is included in all iBGP UPDATE messages. The assigned BGP speaker sends this message to BGP speakers within its own autonomous system but not to neighboring autonomous systems. Higher values of a LOCAL_PREF are preferred.

- ATOMIC_AGGREGATE
  Specifies to a BGP speaker that a less specific route was chosen over a more specific route. The BGP speaker attaches the ATOMIC_AGGREGATE attribute to the route when it reproduces it to other BGP speakers. The BGP speaker that receives this route cannot remove the ATOMIC_AGGREGATE attribute or make any Network Layer Reachability Information (NLRI) of the route more specific. This attribute is used only for debugging purposes.

7) How would you Elaborate IPv6? In detail

IPv6 is the next generation Internet Protocol (IP) address standard intended to supplement and eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, home automation component, IoT sensor and any other device connected to the Internet needs a numerical IP address to communicate between other devices. The original IP

address scheme, called IPv4, is running out of addresses due to its widespread usage from the proliferation of so many connected devices.

8) Why to Support IPv6? What are the benefits of IPv6? Explain

IPv6 (Internet Protocol version 6) is the sixth revision to the Internet Protocol and the successor to IPv4. It functions similarly to IPv4 in that it provides the unique IP addresses necessary for Internet-enabled devices to communicate. However, it does have one significant difference: it utilizes a 128-bit IP address.

Key benefits to IPv6 include:

- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (no more DHCP)

IPv4 uses a 32-bit address for its Internet addresses. That means it can provide support for 2^32 IP addresses in total â” around 4.29 billion. That may seem like a lot, but all 4.29 billion IP addresses have now been assigned, leading to the address shortage issues we face today.

IPv6 utilizes 128-bit Internet addresses. Therefore, it can support 2^128 Internet addresses. The number of IPv6 addresses is 1028 times larger than the number of IPv4 addresses. So there are more than enough IPv6 addresses to allow for Internet devices to expand for a very long time.

The text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit, representing 4 bits. Leading zeros can be omitted. The double colon (::) can be used once in the text form of an address, to designate any number of 0 bits.

With Dual-IP stacks, your computers, routers, switches, and other devices run both protocols, but IPv6 is the preferred protocol. A typical procedure for businesses is to start by enabling both TCP/IP protocol stacks on the wide area network (WAN) core routers, then perimeter routers and firewalls, followed by data-center routers and finally the desktop access routers.

9) How would you Describe Types of IPv6 Address

Types of IPv6 Address

- Unicast addresses
  It identifies a unique node on a network and usually refers to a single sender or a single receiver.

- Multicast addresses
  It represents a group of IP devices and can only be used as the destination of a datagram.

- Anycast addresses
  It is assigned to a set of interfaces that typically belong to different nodes.

10) How would you Discuss Advantages and Disadvantages of IPv6

Advantages of IPv6

- Reliability
- Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- Stringer Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

Disadvantages of IPv6

- Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- Communication: IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

11) How would you Describe IPv6 tunneling over IPv4 Configuration

Since IPv4 and IPv6 are not compatible with each other we need some migration strategies. One technique that we can use is tunneling. Basically it means that we encapsulate IPv6 packets into IPv4 packets (or the other way around) so that it can be routed.

To configure IPv6 static tunneling over an IPv4 network, there are two methods:

- Manual tunnels
- GRE (Generic Routing Encapsulation) tunnels

Both tunnel types are very similar with just minor differences. Both support IPv6 IGPs through the tunnel interface and forwarding of multicast traffic. The manual tunnels refer to RFC 4213 which defines how to encapsulate IPv6 packets in IPv4. GRE is a generic encapsulation type that rides on top of IPv4 and isn't only for IPv6. It can carry many different protocols and if you ever configured an IPSEC VPN with IGPs running through it you had to use GRE.

12) How would you Define GRE?

GRE is a generic encapsulation type that rides on top of IPv4 and isn't only for IPv6. It can carry many different protocols and if you ever configured an IPSEC VPN with IGPs running through it you had to use GRE.

Unit 4

1) How would you elaborate Campus Network? Explain

A campus network is generally the portion of the enterprise network infrastructure that provides access to network communication services and resources to end users and devices that are spread over a single geographic location. It may be a single building or a group of buildings spread over an extended geographic area. Normally, the enterprise that owns the campus network usually owns the physical wires deployed in the campus.

Therefore, network designers typically tend to design the campus portion of the enterprise network to be optimized for the fastest functional architecture that runs on high speed physical infrastructure (1/10/40/100 Gbps). Moreover, enterprises can also have more than one campus block within the same geographic location, depending on the number of users within the location, business goals, and business nature.

When possible, the design of modern converged enterprise campus networks should leverage the following common set of engineering and architectural principles:

- Hierarchy
- Modularity
- Resiliency

2) What is Enterprise campus: Hierarchical design models.

The hierarchical network design model breaks the complex flat network into multiple smaller and more manageable networks. Each level or tier in the hierarchy is focused on a specific set of roles. This design approach offers network designers a high degree of flexibility to optimize and select the right network hardware, software, and features to perform specific roles for the different network layers.

A typical hierarchical enterprise campus network design includes the following three layers:

- Core layer: Provides optimal transport between sites and high-performance routing. Due the criticality of the core layer, the design principles of the core should provide an appropriate level of resilience that offers the ability to recover quickly and smoothly after any network failure event with the core block.
- Distribution layer: Provides policy-based connectivity and boundary control between the access and core layers.

- Access layer: Provides workgroup/user access to the network. The two primary and common hierarchical design architectures of enterprise campus networks are the three-tier and two-tier layers models.

Three-tier model is typically used in large enterprise campus networks, which are constructed of multiple functional distribution layer blocks.

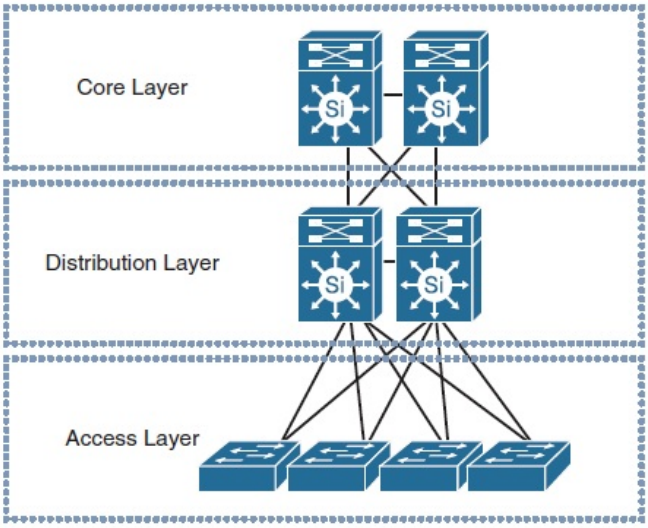


Figure 3-1 *Three-Tier Network Design Model*

3) How would you elaborate IPSec and SSL.

IPSec

- IPSec is suite of protocols to provides security services during communications between networks. It supports network level peer authentication, data origin authentication, data integrity, data encrytion and data decryption. It is often used to create a VPN.

SSL

- SSL is a networking protocol to provide a secure connection between a client and server over the internet. It works at transport layer. It is often used to secure communication between web browser and web server.

4) How would Differentiate IPSec and SSL.

- Concept: IPSec, Internet Protocol Security, is a suite of protocols to provide security for internet protocol. SSL, is a secure protocol to send information securely over internet.

- Layer: IPSec works in internet layer of OSI model. SSL works in transport and application layer of OSI model.
- Configuration: IPSec is complex to configure. SSL is simple to configure.
- Usage: IPSec is used to secure VPN, Virtual Private Network. SSL is used to secure web based communications/ transactions.
- Installation: Installation of IPSec is vendor neutral. Installation of SSL is vendor specific.
- Changes in OS: IPSec require changes to OS during implementation. SSL require No changes to OS during implementation.
- Changes to Application: IPSec require no changes required to Application during implementation. SSL require changes to Application during implementation.
- Location: IPSec is present in OS space. SSL is present in User space.

5) How would you Elaborate Developing an Optimum Design for Layer 3

To achieve high availability and fast convergence in the Cisco enterprise campus network, the designer needs to manage multiple objectives, including the following:

- Managing oversubscription and bandwidth
- Supporting link load balancing
- Routing protocol design
- FHRPs

Design models and recommended practices for high availability and fast convergence in Layer 3 of the Cisco enterprise campus network.

Managing Oversubscription and Bandwidth

Typical campus networks are designed with oversubscription. The rule-of-thumb recommendation for data oversubscription is 20:1 for access ports on the access-to-distribution uplink. The recommendation is 4:1 for the distribution-to-core links. When you use these oversubscription ratios, congestion may occur infrequently on the uplinks. QoS is needed for these occasions. If congestion is frequently occurring, the design does not have sufficient uplink bandwidth.

As access layer bandwidth capacity increases to 1 Gb/s, multiples of 1 Gb/s, and even 10 Gb/s, the bandwidth aggregation on the distribution-to-core uplinks might be supported on many Gigabit Ethernet EtherChannels, on 10 Gigabit Ethernet links, and on 10 Gigabit EtherChannels.

6) How would you describe Bandwidth Management with EtherChannel

As bandwidth from the distribution layer to the core increases, oversubscription to the access layer must be managed, and some design decisions must be made. Just adding more uplinks between the distribution and core layers leads to more peer relationships, with an increase in associated overhead. EtherChannels can reduce the number of peers by creating single logical interface. However, you must consider some issues about how routing protocols will react to single link failure:

- OSPF running on a Cisco IOS Software-based switch will notice a failed link, and will increase the link cost. Traffic is rerouted, and this design leads to a convergence event.
- OSPF running on a Cisco Hybrid-based switch will not change link cost. Because it will continue to use the EtherChannel, this may lead to an overload in the remaining links in the bundle as OSPF continues to divide traffic equally across channels with different bandwidths.
- EIGRP might not change link cost, because the protocol looks at the end-to-end cost. This design might also overload remaining links.

7) Explain the concept of Link Load Balancing

Many equal-cost, redundant paths are provided in the recommended network topology from one access switch to the other across the distribution and core switches. From the perspective of the access layer, there are at least three sets of equal-cost, redundant links to cross to reach another building block, such as the data center.

Cisco Express Forwarding (CEF) is a deterministic algorithm. When packets traverse the network that all use the same input value to the CEF hash, a "go to the right" or "go to the left" decision is made for each redundant path. When this results in some redundant links that are ignored or underutilized, the network is said to be experiencing CEF polarization.

To avoid CEF polarization, you can tune the input into the CEF algorithm across the layers in the network. The default input hash value is Layer 3 for source and destination. If you change this input value to Layer 3 plus Layer 4, the output hash value also changes.

8) How would Define WAN?

To many network professionals the term WAN doesn't refer to the Internet but refers exclusively to enterprise WAN services such as Frame Relay, ATM or MPLS. The distinction is that enterprise WAN services were designed primarily to connect a given enterprise's branch offices and data centers while the Internet provides connectivity to a huge range of resources with myriad owners. That is an arbitrary distinction that is quickly losing relevance and as a result throughout this e-book the term WAN refers to any combination of the Internet and enterprise

9) How would you discuss WAN Evolution

The modern WAN got its start in 1969 with the deployment of the ARPANET which was the precursor to today's Internet. The technology used to build the Internet began to be commercialized in the early 1970s with the development of X.25 based packet switched networks.

In addition to the continued evolution of the Internet, the twenty-year period that began around 1984 saw the deployment of four distinct generations of enterprise WAN technologies. For example, in the mid to late 1980s, it became common for enterprise IT organizations to deploy integrated TDM-based WANs to carry both voice and data traffic. In the early 1990s, IT organizations began to deploy Frame Relay-based WANs. In the mid to late 1990s, some IT organizations replaced their Frame Relay-based WANs with WANs based on ATM (Asynchronous Transfer Mode) technology. In the 2000s, many IT organizations replaced their Frame Relay or ATM-based WANs with WANs based on MPLS. Cost savings was the primary factor that drove the adoption of each of the four generations of WAN technologies.

10) How would you describe Traditional WAN Design

The traditional approach to designing a branch office WAN is to have T1 access to a service provider's MPLS network at each branch office and to have one or more higher speed links at each data center. In this design, it is common to have all or some of a company's Internet traffic be backhauled to a data center before being handed off to the Internet. One of the limitations of this

design is that since the Internet traffic transits the MPLS link this adds both cost and delay. One alternative to the traditional approach to designing a branch office WAN is to supplement the T1 access link in a branch office with direct Internet access and to also leverage technology such as Policy Based Routing (PBR). PBR allows network administrators to create routing policies to allow or deny paths based on factors such as the identity of a particular end system, the protocol or the application.

One advantage of this alternative design is that it enables network administrators to take Internet traffic off the relatively expensive MPLS link and put it on the relatively inexpensive Internet link. One disadvantage of this approach is that configuring PBR is complex, time consuming and error prone. Another limitation of this approach it that it creates a static allocation of traffic to multiple links which means that it isn't possible to reallocate the traffic when the quality of one of the links degrades.

11) What is "NeedToChange" Policy for WAN?

Cisco was given the description of a hypothetical company, referred to as NeedToChange, that has a traditional WAN and they were asked to provide their insight into how the company should evolve its WAN.

Within the context of a traditional WAN there is a wide breadth of options relative to a company's WAN topology, services, applications and goals. As a result of this breadth, it wasn't feasible to cover all possible options in a reasonably sized description of NeedToChange's WAN. In order to limit the size of the description of NeedToChange's WAN and yet still bring out some important WAN options, Cisco was allowed to embellish the description of NeedToChange's WAN. They could, for example, add additional data centers or key applications; vary the amount of traffic that was backhauled; prioritize the factors impacting NeedToChange's WAN or identify business drivers such as the need to support mergers and acquisitions.

12) What are the factors of "NeedToChange" Internet access, Regulations and Visibility

- Internet Access

  NeedToChange currently backhauls over half of its Internet traffic to its data center in Salt Lake City. The company is looking to enable direct Internet access from their branch offices

but they are concerned about security. NeedToChange is also concerned that it is supporting non-business related Internet traffic that is negatively impacting business traffic.

- Regulations

NeedToChange is subject to PCI compliance. As such, NeedToChange needs a network infrastructure that provides robust security.

- Visibility

In the majority of instances in which the performance of one of NeedToChange's business critical applications begins to degrade, the degradation is noticed first by the end users.

13) How would you elaborate different WAN Services

As discussed in The 2014 State of the WAN Report, network organizations currently make relatively little use of WAN services other than MPLS and the Internet and the use they do make of those other services is decreasing somewhat rapidly. That report also identified the concerns that network organizations have with those two services. Those concerns are shown in Table 1 in descending order of importance.

Unit 5

1) How would you define VPN Design

A VPN is connectivity deployed on a shared infrastructure with the same policies, security, and performance as a private network, but typically with lower total cost of ownership.

The infrastructure used can be the Internet, an IP infrastructure, or any WAN infrastructure, such as a Frame Relay network or an ATM WAN.

VPNs can be grouped according to their applications

Refer to (What are the different types of VPN? Explain)

2) What are the different types of VPN? Explain

VPNs can be grouped according to their applications:

- Access VPN

  Access VPNs provide access to a corporate intranet (or extranet) over a shared infrastructure and have the same policies as a private network. Remote-access connectivity is through dial up, ISDN, DSL, wireless, or cable technologies. Access VPNs enable businesses to outsource their dial or other broadband remote access connections without compromising their security policy.

  The two access VPN architectures are client-initiated and Network Access Server (NAS)-initiated connections. With client-initiated VPNs, users establish an encrypted IP tunnel from their PCs across an SP's shared network to their corporate network. With NAS-initiated VPNs, the tunnel is initiated from the NAS; in this scenario, remote users dial into the local SP point of presence (POP), and the SP initiates a secure, encrypted tunnel to the corporate network.

- Intranet VPN

  Intranet VPNs link remote offices by extending the corporate network across a shared infrastructure. The intranet VPN services are typically based on extending the basic remote-access VPN to other corporate offices across the Internet or across the SP's IP backbone. Note that there are no performance guarantees with VPNs across the Internet—no one organization is responsible for the performance of the Internet. The main benefits of intranet VPNs are reduced WAN infrastructure needs,

which result in lower ongoing leasedline, Frame Relay, or other WAN charges, and operational savings.

- Extranet VPN

  Extranet VPNs extend the connectivity to business partners, suppliers, and customers across the Internet or an SP's network. The security policy becomes very important at this point; for example, the company does not want a hacker to spoof any orders from a business partner. The main benefits of an extranet VPN are the ease of securely connecting a business partner as needed, and the ease of severing the connection with the business partner (partner today, competitor tomorrow), which becomes as simple as shutting down the VPN tunnel. Very granular rules can be created for what traffic is shared with the peer network in the extranet.

3) Explain Overlay VPNs in detail.

With overlay VPNs, the provider's infrastructure provides virtual point-to-point links between customer sites. Overlay VPNs are implemented with a number of technologies, including traditional Layer 1 and Layer 2 technologies (such as ISDN, SONET/SDH, Frame Relay, and ATM) overlaid with modern Layer 3 IP-based solutions (such as Generic Routing Encapsulation [GRE] and IPsec).

From the Layer 3 perspective, the provider network is invisible: The customer routers are linked with emulated point-to-point links. The routing protocol runs directly between routers that establish routing adjacencies and exchange routing information. The provider is not aware of customer routing and does not have any information about customer routes. The provider's only responsibility is the point-to-point data transport between customer sites. Although they are well known and easy to implement, overlay VPNs are more difficult to operate and have higher maintenance costs for the following reasons:

- Every individual virtual circuit must be provisioned.
- Optimum routing between customer sites requires a full mesh of virtual circuits between sites.
- Bandwidth must be provisioned on a site-to-site basis.

The concept of VPNs was introduced early in the emergence of data communications with technologies such as X.25 and Frame Relay. These technologies use virtual circuits to establish the

end-to-end connection over a shared SP infrastructure. In the case of overlay VPNs, emulated point-to-point links replace the dedicated links, and the provider infrastructure is statistically shared. Overlay VPNs enable the provider to offer the connectivity for a lower price and result in lower operational costs.

4) How would you elaborate Enterprise Data Center

An Enterprise Data Center consists of multiple data centers, each with a targeted focus on sustaining key functions. These data centers can be classified into three types: internet, extranet and intranet.

Internet data centers are a category of enterprise data centers that support servers and devices necessary for e-commerce web applications. In some cases, web servers are completely isolated from the rest of the network at the physical level. These servers have no physical path to any other part of the network, with the exception of a direct connection to the intranet data center using a separate set of non-routable links.

Extranet data centers provide support for business-to-business transactions in the enterprise network. These services are generally accessed over secure VPN connections or private WAN links.

5) How would you describe Data Center Access Layer

The Data Center Access layer provides Layer 2, Layer 3, and mainframe connectivity. The design of the Data Center Access layer varies depending on whether Layer 2 or Layer 3 access switches are used; it is typically built with high-performance, low-latency Layer 2 switches, allowing better sharing of service devices across multiple servers and allowing the use of Layer 2 clustering, which requires the servers to be Layer 2-adjacent. With Layer 2 access switches, the default gateway for the servers can be configured at the access or aggregation layer.

Servers can be single- or dual-attached; with dual-attached NICs in the servers, a VLAN or trunk is required between the two redundant access layer switches to support having a single IP address on the two server links to two separate switches. The default gateway is implemented at the access layer.

A mix of both Layer 2 and Layer 3 access switches using one rack unit (1RU) and modular platforms results in a flexible solution and allows application environments to be optimally positioned.

6) How would you elaborate Data Center Core Layer

Implementing a Data Center Core layer is a best practice for large data centers. The following should be taken into consideration when determining whether a core is appropriate:

- 10-Gigabit Ethernet density: Without a Data Center Core, will there be enough 10-Gigabit Ethernet ports on the Campus Core switch pair to support both the campus Building Distribution layer and the Data Center Aggregation layer?
- Administrative domains and policies: Separate campus and data center cores help isolate the campus Building Distribution layers from Data Center Aggregation layers for troubleshooting, maintenance, administration, and implementation of policies (using QoS and ACLs).
- Anticipation of future development: The impact that could result from implementing a separate Data Center Core layer at a later date might make it worthwhile to install it at the beginning.

The data center typically connects to the Campus Core using Layer 3 links. The data center network addresses are summarized into the Campus Core, and the Campus Core injects a default route into the data center network. Key Data Center Core layer characteristics include the following:

- A distributed forwarding architecture
- Low-latency switching
- 10-Gigabit Ethernet scalability
- Scalable IP multicast support

7) What are the Key considerations in developing a storage area network design

The best storage area network design for your customers will take into consideration a number of critical issues: uptime needs, scalability, security and disaster recovery. Find out how each of these factors will influence storage area network design choices.

Storage area networks (SANs) let several servers share storage resources and are often used in situations that require high performance or shared storage with block-level access, like virtualized servers and clustered databases. Although SANs started out as a high-end technology used only in large enterprises, cheaper SANs are now affordable even for small and medium-sized businesses (SMBs).

8) Explain the term Security with respect to storage area network

With several servers able to share the same physical hardware, it should be no surprise that security plays an important role in a storage area network design. Your client will want to know that servers can only access data if they're specifically allowed to. If your client is using iSCSI, which runs on a standard Ethernet network, it's also crucial to make sure outside parties won't be able to hack into the network and have raw access to the SAN.

Most of this security work is done at the SAN's switch level, Franco said. Zoning allows you to give only specific servers access to certain LUNs, much as a firewall allows communication on specific ports for a given IP address. If any outward-facing application needs to access the SAN, like a website, you should configure the switch so that only that server's IP address can access it, Franco said.

If your client is using virtual servers, the storage area network design will also need to make sure that each virtual machine (VM) has access only to its LUNs, Schulz said. Virtualization complicates SAN security because you cannot limit access to LUNs by physical controllers anymore -- a given controller on a physical server may now be working for several VMs, each with its own permissions. To restrict each server to only its LUNs, set up a virtual adapter for each virtual server. This will let your physical adapter present itself as a different adapter for each VM, with access to only those LUNs that the virtualized server should see.