**1- List and explain five component architectures of a Network Architecture; their mechanisms and internal & external relationships.(Done)**

**Addressing and Routing Architecture:**

**Addressing** is applying identifiers (addresses) to devices at various protocol layers (e.g., data-link and network),

**Routing** is about learning the connectivity/reachability between/of networks and applying this connectivity/reachability

information to forward IP packets toward their destinations. It determines:

• How sources and sinks are virtually identified and located

• How the flows between sources and sinks are propagated throughout the network.

Mechanisms For addressing:

Subnetting: (using part of the device (host) address space to create another level of hierarchy)

variable-length subnetting (VLSM): where multiple variable length subnet masks (VLSM) are used, creating subnets of different sizes)

super-netting: (single IP network address and mask that can represent multiple subnets)

dynamic addressing (DHCP)

private addressing(not public so not routed on internet),

network address translation (NAT): It can bind private IPs to public IPs (one-to-one, many-to-one and port translation (PAT)).

Mechanisms For routing : Routing, default route propagation(the technique exchanging of routing information between ASs)

classless inter-domain routing (CIDR), multicasts, mobile IP

route filtering(technique of applying route filters to hide networks from the rest of an AS, or to add, delete, or modify routes in the routing table.)

peering, routing policies, confederations, and IGP and EGP selection/location.

Internal Relationships: Trade-offs between addressing and forwarding mechanisms, and trade-offs within addressing or within forwarding, Addressing and forwarding mechanisms influence the choice of routing protocols and where they are applied.They also form an addressing hierarchy upon which the routing hierarchy is overlaid

External Relationships:

Interactions between addressing/routing and network management: Addressing/routing can be used to configure boundaries for network management.

Interactions between addressing/routing and performance: MPLS, Differentiated and Integrated Services, and RSVP. » However, when routing protocol simplicity is a high priority, performance may be decoupled from addressing/ routing.

Interactions between addressing/routing and security: Security perimeters or zones can bound routing. » Network address translation (NAT) can be used to enhance security as well as provide private addressing space for a network. Also the use of dynamic addressing can create problems in tracing network events.

**Segmentation Architecture:** Communications within a network take place at OSI L3 and below.

– The boundaries that isolate the group is typically intangible. It is the netmask that sets the boundaries, an intangible 4 octets bit representation.

We identify a segment as a group of interconnected things (nodes)

– where a node claims presence with a MAC address in the group (for Ethernet segment).

– Communications within a segment take place at OSI L2 and below.

• Broadcast traffic is contained within a segment. Also referred to as broadcast domain.

– The boundaries that isolate the group are typically tangible.

• They are the nodes with L3 presence on participating NIC that determine the boundaries.

Any NIC (Network Interface Card) that has presence at L3 forms the boundary for the segment as such node does not forward broadcasts.

-Therefore a node with multiple NICs with L3 presence can be used to subdivide a segment into multiple segments.

-Subdivision of a segment, thus a broadcast domain, is called reducing the broadcast domain.

Best practice is to always contain a network within a segment.

**Network Management Architecture:** Network management provides functions to control, plan, allocate, deploy, coordinate, and monitor network resources

Mechanisms

• Monitoring: Obtaining values for end-to-end, per-link, and per-element network management characteristics

• Instrumentation: Determining the set of tools and utilities needed to monitor and probe the network for management data

• Configuration: Setting parameters in a network device for operation and control of that element

• FCAPS artifacts: The set of fault, configuration, accounting, performance, and security management artifacts.

Internal Relationships: The network architecture should include the potential locations for each component and/or management system, as well as the management data flows between components and/or management systems.

dependencies on capacity and reliability of the network for management data flows; dependence on the amount of data storage available for data.

Trade-offs in-band and out-band management.

Trade-offs in centralised management (which can act as a single point of failure; all management data flows are aggregated at the management system’s network interface, potentially causing congestion or failure) and (Distributed or hierarchical management can avoid central points of

failure and reduce congestion points )

External Relationships:

Between network management and addressing/routing

• Network management depends on the addressing/routing architecture for the proper routing of management data flows through the network.

Between network management and performance:

• How much network resources (e.g., capacity) network management requires, as this may impact the network’s ability to support various performance levels.

Between network management and security:

• Network management is dependent on some level of security in order to be used in most operational environments. This may be security at the protocol level (e.g., SNMP) And/or for securing access to network devices.

**Performance Architecture:** consists of the set of mechanisms used to configure, operate, manage, provision, and account for resources in the network that allocate performance to users, applications, and devices.

• Describes how network resources will be allocated to user and management traffic flows.

– Prioritising, scheduling, and conditioning traffic flows

• Includes capacity planning and traffic engineering.

often applies across multiple layers

Mechanisms Correlate user, application, and device requirements to traffic flows, as well as traffic engineering, access control,(QoS) , policies, and service-level agreements (SLAs).

Internal Relationships: trade off between :

-End-to-end and per-hop prioritization.

-Scheduling, and conditioning of traffic flows,

External Relationships:

Between performance and addressing/routing

• Performance can be closely coupled with routing through mechanisms such as MPLS, differentiated and integrated services, and RSVP.

• However, when routing protocol simplicity is a high priority, performance may be decoupled from forwarding.

Between performance and network management

• Performance depends on network management to configure, monitor, manage, verify performance levels throughout the network.

• Network management helps to couple QoS, SLAs, and policies by providing common communications paths and protocols for performance information

Between performance and security.

• As security is increased, by adding more mechanisms (and mechanisms that are more intrusive) to the network, performance is decreased.

• When security mechanisms interrupt or terminate and regenerate traffic flows, they seriously impact the

**Security and Privacy Architecture:** describes how system resources are to be protected from theft, damage, alteration, denial of service (DOS), or unauthorized access

Mechanisms:

Security threat analysis to determine which components of the system need to be protected and the types of security risks.

security policies and procedures to minimize exposure to security threats

physical security and awareness to protect devices from physical access, damage, and theft,

Protocol and application security:IPSec, SNMP security, and packet filtering.

Data Encryption, network perimeter: NAT and packet filtering with firewalls.

security and remote access security: traditional dial-in, point-to point sessions, and VPN connections

Internal Relationships: Some security mechanisms require the ability to look at, add to, or modify various information fields within the packet like NAT and information encrypting field.

External Relationships:

Between security and addressing/routing:

• When NAT is applied for security, it also impacts addressing for the network.

• In addition, dynamic addressing can interfere with address-specific protective measures making it hard to track hosts.

Between security and network management:

• Security depends on network management to configure, monitor, manage, and verify security levels throughout the network.

• In addition, there is a need for maintenance access even during attacks where in-band access to network devices is not available.

– For example, when devices are not at the same location, using dial-up for out-of-band access is a potential fall-back position to take.

Between security and performance:

• When security is a high priority, security mechanisms that impact traffic flows may restrict performance mechanisms to operate within security zones, or result in performance being minimized for that zone

• When performance is high priority, particularly when there is a need to provision end-to-end performance among select users, applications, or devices, performance mechanisms may preclude the use of intrusive security mechanisms in those areas of the network.

**2- Explain Hierarchy and Diversity and their benefits within the concept of Network Architecture. Give one example for each regarding how to establish hierarchy and how to establish diversity in a network. (Done)**

**Hierarchy** is the degree of concentration of networks or traffic flows at interconnection points within the network.

– Hierarchies provide separation and structure within the network

– They help us in determining the sizes of networks and break the broadcast domain . Example :

– Changing from a flat (bridged or layer 2 switched) structure to a routed structure.

– Adding routing to the network breaks a broadcast domain into a number of smaller broadcast domains.

**Diversity** balances the network structure by interconnecting the network at different levels in the design to provide greater performance through parts of the network

-Achieve performance within a hierarchical structure

– The dynamic between hierarchy and diversity is perhaps one of the most fundamental trade-offs in network architecture and design.

Example : Adding alternative paths for switching or routing or add CDN directly to the networks by passin hierarchy

**3- What is a Flow Model? List and explain four flow models.(done)**

**Flow model** is a group of flows that exhibit specific, consistent behaviour characteristics.

– Flow model helps describe the degrees of hierarchy and diversity of flows for applications.

– The flows within a flow model apply to a single application.

– Directionality, hierarchy, and diversity are the primary characteristics of flow model

– it shows where flows combine, where they can be grouped together, and where flows occur between peers, which are devices at the same level in the hierarchy

**Peer-to-peer model** is where the users and applications are fairly consistent in their flow behaviours throughout the network at the same level of hierarchy

– We cannot distinguish between flows in this model. Therefore, either all of the flows or none of the flows is critical

– Since the flows are equivalent, they can be described by a single specification (e.g., profile)

**Client-server model** Flows are bidirectional, between clients and the server, in the form of requests and responses

– Flows are asymmetric and hierarchically focused toward the client. Thus, requests tend to be small relative to responses

– Depending on the type of application, the flows may be considered almost unidirectional, from the server to the clients

**Hierarchical Client-server model**  Has the characteristics of a client–server flow model but also has multiple layers, or tiers, between servers.

– With the additional layer(s) of hierarchy in this model the servers can now be either data sources or sinks (or both).

**Distributed computing model** a distributed-computing flow model can have the inverse of the characteristics of the client–server flow model, or a hybrid of peer-to-peer and client–server flow models.

– Flows can be client–server but are reversed in symmetry

**4- Explain what a flow is and what the two common flow types are. List and explain common flow characteristics. (Done)**

**Flow** is sets of network traffic (application, protocol, and control information) that have common attributes, such as source/destination address, type of information, directionality, or other end-to-end information.

– Information within a flow is transmitted during a single session of an application.

– Flow is end-to-end, between source and destination applications/devices/users.

**Flow types:**

Individual Flows: An individual flow is the flow for a single session of an application.

– Is the basic unit of traffic flows.

– Are derived directly from the requirements specification, or are estimated from our best knowledge about the application, users, devices, and their locations.

Composite Flows: a combination of requirements from multiple applications, or of individual flows, that share a common link, path, or network.

-Most flows in a network are composite

Flow directionalities in the table could be: - Bidirectional / Unidirectional – Upstream , Downstream



**5- List and explain five addressing mechanisms. Give one example for each.(Done)**

Glassful Addressing: IETF provisioned the division of network part and the local (host) part of IP addresses under 3 forms (classes)



Subnetting: The next step in adding hierarchy to addressing is to allow a classful network address to be segmented into smaller.

– Subnetting is using part of the device (host) address space to create another level of hierarchy,

• Changing the address mask increases the number of bits allocated to the network, creating the subnet

Variable length subnetting (VLSM) is where multiple (VLSM) are used, creating subnets of different sizes.

– This allows the addressing to be more granular, wasting least amount of IP addresses possible.

Supernetting: is aggregating network addresses,

– By coming up with a new single IP network address and mask that can represent multiple subnets

• We come up with this new address by changing the address mask to decrease the number of bits recognized as the network.

– By decreasing the number of bits recognized as the network, we are in effect ignoring part of the network address, which results in aggregating network addresses.

• Supernetting reduces the number of advertisements in the Internet .

– Supernets give way to CIDR

Private Addressing and NAT: Optimizing the address space hierarchy (Subnetting, VLSM) was not helping the address depletion problem much.

– A more radical approach was to scoop a certain portion of the public IP range and make it non-public.

• So that organizations could use those addresses individually within their campus.

– No worries about address conflict with other organizations because they are not routed on Internet!

– Visit the RFC to get further information about what ranges were scooped as private addresses.

-NAT can bind priate IPs to public IPs

– It can be in a one-to-one, many-to-one and port translation (PAT)

**6- Explain what IGP and EGP is. Give two example protocols for IGP and one for EGP, elaborate on them in detail.(done)**

For dynamic routing or exchange reachability information on the network we use both:

**Interior gateway protocol IGP**: designed to manage reachability within an AS ,Where the requirements are fast convergence and not so large routing tables

– Examples:

RIP: Distance vector (DV) protocol, each router maintains “distance” (a metric to weight each hop, or connection between

routers) between itself and possible destinations, and a vector (distance and direction) is computed from distance information received from other participating routers on that network.

OSPF: Link-state (LS)protocol, each router learns about itself, its links to next-hop routers (its neighbours), and the state of each link. This information is communicated to other participating routers, and all routers build their routing information from the sum of these exchanged information.

**Exterior Gateway protocol EGP:** are designed to manage reachability throughout ASes , Fast convergence can pose a problem. Routing tables are typically

large, Examples: BGP: Path-Vector (PV) protocol, each router maintains, a path-vector algorithm is similar to a distance-vector algorithm,

such as that used in RIP. it operates on ASs or lists of ASs (paths) for constructing vectors.

**7- Within the concept of corresponding component architecture.(done)**

**a. Explain what an event is. How can event notification cations be monitored and what are the trade-offs? (Done)**

**Event** is something that occurs in the network that is noteworthy. (problem, failure in a network device or crosses a threshold value) across the

network. It may be noted in a log file, on a display, or by issuing an alarm

Real-time analysis usually requires short polling intervals (time periods between active probing of the network and network devices for management data)

-There is a trade-off between the number of characteristics and network devices polled for real-time analysis versus the amount of resources (capacity, CPU, memory, storage) needed to support such analysis.

– In some cases the amount of network data generated (and the resulting traffic) by the periodic polling of multiple characteristics on many network devices can impact the overall performance of the network.

**b. Explain and compare in-band and out-of-band management approaches. (Done)**

**In-band management** occurs when the traffic flows for network management follow the same network paths as the traffic flows for users and their applications.

– This simplifies the network management architecture, in that the same network paths can be used for both types of data, and a separate path (and possibly network) is not required. A trade-off with in-band management is if the very network link you are monitoring is down, you may not be able to communicate this with the EMS

**Out-of-band management** occurs when different paths are provided for network management data flows and user traffic flows.

– This type of management has the distinct advantage of allowing the management system to continue to monitor the network during most network events, even when such events disable the network.This allows you to effectively see into portions of the network that are unreachable through normal paths.

A trade-off with out-of-band management is the added expense and complexity of a separate network for network management

**c. What is MIB? Explain how it is structured and how the data on specic configuration/state fields of an equipment can be get/set via the protocol utilising an MIB. (Done)**

**MIB** is a formal description of a set of network objects that can be monitored and managed using the Simple Network Management Protocol (SNMP).

Objects can be part of the standard MIB , (MIB-II), other standard MIBs , remote monitoring , MIBs, or enterprise-specific MIBs, which have parameters specific to a particular vendor’s product. Each parameter has an object id (OID) to uniquely refer to. MIB structured in registered tree contains multiple levels the base is Root and the end are OIDs. We donate that by numbers. Vendors can have custom object trees and MIBs for example 1.3.6.1.4.1.9 Cisco and some OIDs used to monitor if there are trap interfaces or to set IP addresses for example.

**8- What is configuration? List and explain configuration mechanisms and protocols used. (Done)**

**Configuration** is setting parameters in a network device for operation and control of that element. Configuration mechanisms include

(Direct access to devices, Remote access to devices, Downloading configuration files)

**configuration mechanisms**

Direct Access

Devices have one port dedicated to management purposes only ( Console)

• The pinout of the port is generally proprietary, so you need a specific cable or DIY by finding out the pinouts (or via Software)

Once cabled in, you need a terminal software

• Putty, TerraTerm, HyperTerm, SecureCRT

• You need to set the port settings such as baud rate, for the specific model of device you are working on, Incorrect settings will cause gibberish text appear on console cli

Remote Access

– It is cumbersome to be have physical proximity to the device to manage.

– Remote access allows administrator/ NMS host to connect and manage the device remotely.

• Has to be configured via direct access first.

common *protocols* for remote access are

• SSH: Management traffic is encrypted via asymmetric encryption– CLI only

• WEB GUI: Typically SSL encryption – CLI & GUI

• TELNET: No encryption – CLI only

• SNMP: Decent encryption and authentication with v3 only – SNMP specific command language only

**9- Levels of performance are described by the performance characteristics. List and explain the performance characteristics. (Done)**

**Performance characteristics:**

• **Capacity** is used as a label for the class of characteristics that involves moving information from place to place,

– Bandwidth: Measure of electoronic setup of a medium

– Throughput: Measure of data along with L2-4 overhead

– Goodput: Measure of application layer data transmitted

• **Delay** is a measure of the time difference in the transmission of information across the system. E2E or RT

– Latency: Describes the response time of a network device, such as the latency through a switch or router.

– Jitter: Delay variation, which is the change in delay over time.

**• Reliaibility:**

– Statistical indicator of the frequency of failure of the network and its components and represents the unscheduled outages.

– When delivery times vary greatly, users lose confidence in the timely delivery of information. In this sense the term reliability can be coupled with confidence

**• Maintainability**:

– Statistical measure of the time to restore the system to fully operational status after it has experienced a fault. This is generally expressed as a mean-time-to-repair (MTTR).

**Availability**

– The relationship between the frequency of mission-critical failures and the time to restore service

– Defined as the mean time between failures divided by the sum of mean time to repair and mean time between failures.

**10- What is QoS and how is it useful? List and explain two standard types of/principal approaches to QoS; protocols used, their advantages and trade-offs.(Done)**

QoS in simplest sense; is determining, setting, and acting upon priority levels for data.

– So that the data needs a special treatment by QoS, it first needs to be identified.

– The two major operations for QoS treatment are

• Classification: Identify/classify the flows/data according to requirements.

• Marking: Mark/tag the identified data/flow with special codes/priority levels so that they can be recognized by QoS and treated according to the actions specified for that specific code/priority level.

– The most common layers that QoS treats data are L2 and L3

• At L2, Class of Service (CoS) field is used for marking.

• At L3, Type of Service (ToS) field is used for marking.

For L3 (IP-based) traffic, there are two standard types of QoS:

– Differentiated services (DiffServ, or DS)

• Approaches QoS from the perspective of treating traffic flows on a per-hop basis based on traffic behavior.

• Three traffic classes for DiffServ:

– Best-effort, assured forwarding (AF), and expedited forwarding (EF).

– Assured and expedited forwarding are the preferred traffic classes and are based on the types of performance they require.

– Expedited forwarding is usually targeted toward traffic that has delay requirements (e.g., real-time or interactive), while assured forwarding can be used for traffic with both delay and capacity requirements (e.g., multimedia or teleservices).

– Integrated services (IntServ, or IS)

• Approaches QoS from the perspective of supporting traffic flows on an individual, end-to-end basis.

• Defines values and mechanisms for allocating resources to flows across the end-to-end path of the flow.

– A signaling mechanism required to communicate flow requirements, as well as the setup and teardown of resource allocations across network devices in the end-to end path of a flow.

» Such signaling is usually provided by the resource reservation protocol (RSVP).

» Successful RSVP requests usually result in resources being reserved at each network device along this end-to-end path, along with state information about the requested service.



**11- List and explain five Security and Privacy mechanisms.(Done)**

**-Security threat analysis** to determine which components of the system need to be protected like

(Workstations/PCs, servers, switches, routers, services, data)and the types of security risks they should be protected from like (Unauthorized access or disclosure, DoS, theft or data corruption)

**-Security policies and procedures** to minimize exposure to security threats. define and document how the system can be used with minimal security risk. And clarify to users what the security threats are. high level can present an organization’s overall security philosophy ex: To deny specifics and accept everything else (open philosophy).

Or to accept specifics and deny everything else(closed philosophy). They should be:

• Straightforward to implement for your environment (keeping in mind who will be supporting them),

• Enforceable, and have clearly defined areas of responsibility.

Policies and procedures should include:

• Privacy statements (monitoring, logging, and access)

• Accountability statements (responsibilities, auditing)

• Authentication statements (password policies, remote access)

• Reporting violations (contact information, procedures)

**-Physical security and awareness** to protect devices (Server, router,…. Or software on taps CDs,…) from physical access, damage, and theft.

Ways to implement physical security include

• Access-controlled rooms (e.g., via card keys) for shared devices (servers) and specialized devices.

• Backup power sources and power conditioning

• Off-site storage and archival

• Alarm systems (e.g., fire and illegal entry alarms)

Security awareness entails getting users educated and involved with the day-to-day aspects of security in their network, and helping them to understand the potential risks of violating security policies and procedures.

**-Data Encryption- decryption :** is a security mechanism where cipher algorithms are applied together with a secret key to encrypt data so that they are unreadable if they are intercepted. Data are then decrypted at or near their destination.

Cryptography:

– Suite of mathematical functions and operations where data is rendered to different forms to provide confidentiality

– Cryptographic Encryption/Decryption

• Symmetric Cryptography

– Same key is used to ency/dec data

– Faster compared to Asym

– Key distribution is a concern

– Several examples are DES, 3DES, AES

• Asymmetric Cryptography

– Different keys of a keypair is used for ency/dec

– Can also achieve authentication

– Example; SSL certificates (RSA algorithm for TLS)

**Network Perimeter Security** For protecting the external interfaces between your network and external networks, NAT and packet filtering with firewalls are effective.

– As we have covered in earlier lecture, Network address translation, or NAT, is the mapping of IP addresses from one realm to another.

• Typically this is between public and private IP address space(RFC1918).

– Firewalls are combinations of one or more security mechanisms, implemented in network devices (routers) placed at strategic locations within a network.

• Firewalls can be filtering gateways, application proxies with filtering gateways, or devices running specialized “firewall” software

**12- explain three protocol application security mechanisms. Give one example for each demonstrating where each can be useful.**

**• IPSec** is a protocol for providing authentication and encryption/decryption between devices at the network layer.

– IPSec mechanisms consist of authentication header (AH) and encapsulating security payload (ESP).

– There are two modes that IPSec operates in:

• Transport: The IP payload is encrypted using ESP, while the IP header is left in the clear

• Tunnelling: IPSec can be used to encapsulate packets between two virtual private network (VPN) gateways (IPb and IPc in the figure).

The tunneling process consists of the following:

– IPSec tunnels are created between VPN gateways IPb and IPc IP packets are encrypted using ESP

» Tunnel can also be established between a VPN gateway and a user computer which typically has VPN client software

– These packets are then encapsulated within another IP packet, and addressed with the ends of the IPSec tunnel (IPb and IPc)

– At the end of the tunnel (the VPN gateway serving IPd), the original packet is unencapsulated and decrypted and sent to its destination IPd.

**Packet filtering** is a mechanism in network devices to explicitly deny or pass packets at strategic points within the network.

– It is often used to deny packets to or from particular IP addresses or ports (services).

Ex: allow source 192.168.2.1 port 80

**SNMPv3:** It protects against modification of information, masquerades, disclosure (eavesdropping), and message stream modification.

– SNMP Security provides the following security capabilities:

• SNMP message verification (data integrity), user identity verification (data origin authentication), and data confidentiality (via authProtocol, authKey, privProtocol, and privKey)

• Detects SNMP messages that have exceeded time thresholds (message timeliness/limited replay) (via snmpEngineID, snmpEngineBoots, and snmpEngineTime)

-SNMP security also includes authentication mechanisms (authProtocol) and encryption/decryption mechanisms (privProtocol):

• HMAC-MD5-96 (128-bit message digest algorithm (MD5) cryptographic hash-function, message authentication codes (HMAC) mode, truncated to 96 bits)

• HMAC-SHA-96 (Secure Hash Algorithm)

• CBC-DES (Cipher Block Chaining Mode Symmetric encryption/Decryption protocol

**13-Describe the network layout process. List and explain three products of network layout process.**

**Network layout** takes topology and technology choices; architecture and design decisions; vendor, equipment, and service-provider choices; and strategic locations; and from these develops various views of your planned network design, including:

– **logical diagrams:** show the connectivity and relationships among network devices. For example, you could have a logical diagram showing the routers in your network, or showing just the border routers, or just the interfaces to all external networks.

– **Physical blueprints**, describe detailed physical aspects of your network design:

– Locations of network devices, servers, cable plant, physical security, and secure locations;

– How devices are to be interconnected, their interface types and speeds; as well as device-specific and service-specific configuration information.

– There is significantly more detail in a blueprint than there is in a logical diagram.

• Developing network blueprints consists of:

– Mapping strategic locations of your network onto network templates; such locations found at external interfaces of the network, where your network connects to other networks, such as to other autonomous systems or to the Internet

– Applying topology and technology information: a topology consists of network devices (routers and/or switches), possibly co-located with security, monitoring, and/or performance devices and servers. Interconnectivity describes how the locations are connected.

– Adding your selections of network equipment and services: Here you should specify some or all of the following for each device:

• Equipment vendor• Equipment type/class• Device ID• Interface types and rates• Device hardware configuration• Device OS level/revision •Degrees of connection, power, internal (card, board, engine) diversity• Any appropriate vendor-specific information• Routing protocols used

– **Function-specific component plans**: Component plans build upon information you gathered in developing the network architecture and focuses on a specific function. common component plan focuses on security,

**14- Describe the benefits of Vendor, Equipment, and Service Provider Evaluations process. List and explain its phases and application.**

This process consists of using products fromnetwork analysis and architecture to develop an initial set of options.(iterative process.)

1- Seeding the Evaluation Process (generating an initial list of candidates for discussion by project manager or any..)

2- Conducting discussions to develop a complete set of candidate options, along with criteria to evaluate those options,

3- Gathering and developing data to apply to the evaluations: Common sources are:

– Discussions with internal and external groups to expand the amount of information

– Discussions with vendors and/or service providers (Providing value-added services, access to labs, testing and validation, and competitive pricing)

– Independent (third-party) assessments of vendors, equipment, and/orservice providers. provide a different prospective

– Modeling and simulation of all parts of network

– Information from risk assessments

4- Refining evaluation criteria and developing ratings; in gathering and developing data, we learn that there are some new criteria that should be added, removed or modified ;rating is done with a system of ratings. Ratings show how the candidates compare to one another. Ratings are applied with criteria (which you already have) and weights that show the relative importance of each criterion

5- Applying criteria and ratings to prioritize the candidate options; As in developing the first set of weights, this should be a group

effort that includes your best technical and executive decision makers. We need to agree on a scale for our ratings, Common ranges are 0 (candidate is least relevant for that criterion )-1(most relevant.) , 1–5 or 1–10

6- Modifying the set of candidate options, with the goal of selecting the optimal candidate. The result of the evaluation is a set of overall or summary ratings that combines the individual ratings for each candidate. We can remove the candidates with high delta or iterate the

process if there is a tie.

**15-Explain the concept of Software Defined Networking(SDN) and Network Function Virtualization(NFV). Describe the components of SDN and their relationship.**

**SDN** is an approach to network management that aims to make networks agile and flexible by enables efficient network configuration. The goal of SDN is to improve network control by enabling enterprises and service providers to respond quickly to changing business requirements. SDN technology focused on separation of the network [control plane](https://searchsdn.techtarget.com/definition/control-plane-CP) from the data plane. While the control plane makes decisions about how packets should flow through the network, the data plane actually moves packets from place to place.

In a classic SDN scenario, a packet arrives at a network switch, and rules built into the switch's proprietary firmware tell the switch where to forward the packet. These packet-handling rules are sent to the switch from the centralized controller.

**NFV** is a network concept that uses the technologies of IT [virtualization](https://en.wikipedia.org/wiki/Virtualization) to virtualize entire classes of [network node](https://en.wikipedia.org/wiki/Network_node) functions into building blocks that may connect, to create communication services. NFV architecture virtualizes network functions and eliminates specific hardware, network managers can add, move or change network functions at the server level in a simplified provisioning process.

NFV and [SDN](https://searchsdn.techtarget.com/definition/software-defined-networking-SDN) are complementary technologies but not dependent on each other. NFV can be implemented without a SDN being required, although the two concepts and solutions can be combined and potentially greater value accrued.

NFV moves services to a virtual environment but doesn't include policies to automate the environment. When SDN is combined with NFV infrastructure, however, SDN's centralized management function can forward data packets from one network device to another, while NFV allows routing control functions to run on a virtual machine located in a rack mount server, for example.

**16-Within the concept of corresponding component architecture**

**a. Explain Shaping and Policing within metering concept. Explain the difference and exemplify where each can be useful.**

**Shaping** In traffic conditioning, delaying traffic to change a performance characteristic. In order to shape non-conforming traffic, it may be sent to a shaper queue where delay is added before it is transmitted onto the network. By delaying traffic, a shaper queue changes the performance of that traffic flow.

**Policies** are formal or informal sets of high-level statements and rules about how network resources are to be allocated among users. They are used to create and manage one or more performance objectives. -Policies complete the framework of performance for a network by coupling the high-level view of how the network should perform, with mechanisms to implement performance at the network devices (QoS) and feedback loops with users (SLAs).

-Policies may describe what network, computing, storage, or other resources are available to users, when resources are available, or which users are permitted to access certain resources. In this sense these policies are similar to policies for security or routing.

-Policy information is often implemented, stored, and managed in policy databases kept on the network. Policy information is passed between databases and network devices using Common Open Policy Service (COPS) and LDAP.

**b. Explain Classiffication and Marking. At what layers of OSI model can those operations be performed and how?**

**Classification** The ability to identify traffic flows as part of traffic conditioning. The classifier looks at various parts of the IP packet, such as source and destination addresses, port numbers, or protocol types. Additionally, the classifier may look deeper into a packet for the necessary information. Once traffic flows have been classified, they may be metered to determine their performance levels.

**Marking** is Tagging an IP packet with a priority level, as part of traffic conditioning. Examples of marking included tagging packets with DiffServ Code Points. (DSCPs) for best-effort (BE), assured forwarding (AF), and expedited forwarding (EF) priority levels.

-Both of them work on layer 3 (Network layer)

**c. List and explain three algorithms/mechanisms that can be utilised to avoid congestion at a packet forwarding node in the network (not the**

**TCP flow control).**

**First in first out (FIFO)** is arguably the simplest queuing mechanism available. In FIFO queuing packets are stored in a single queue. For an output FIFO queue, packets are transmitted onto the network in the order that they were received (at the input queue).

**Class-based queuing (CBQ**) multiple queues with differing priorities are maintained. Priority levels are configurable in the network device and indicate the performance levels required for each traffic type. Packets of each priority level are placed in their respective queues. Higher-priority queues are processed before lower-priority queues, with the result that higher-priority traffic receives more network resources and thus greater performance.

**Weighted fair queuing (WFQ)** Like CBQ, weighted fair queuing (WFQ) assigns priorities (weights) to queues. Typically with this mechanism, high-priority traffic flows are processed first, and lower-priority traffic flows share the remaining resources.