# CCNP ENCOR Cram Notes

## I. Architecture

Network architecture refers to the design and structure of a computer network. It includes the hardware components, software components, protocols, and communication channels that are used to connect different devices and enable them to communicate and exchange data.

Network architecture defines the way in which the components of the network are organized and how they interact with each other. It is responsible for ensuring that the network is reliable, scalable, and secure, and that it can support the applications and services that run on top of it.

There are many different types of network architectures, including client-server architecture, peer-to-peer architecture, and cloud-based architecture. Each type of architecture has its own strengths and weaknesses, and the choice of architecture will depend on the specific needs of the network and the applications that will be running on it.

Network architecture is an important consideration for network engineers and architects, as it can have a significant impact on the performance, reliability, and security of the network. It is also an important consideration for businesses and organizations, as the choice of network architecture can have a significant impact on their ability to compete and innovate in the marketplace.

### 1. Explain the different design principles used in an enterprise network

#### 1.1. Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning.

**Spine-leaf:**With the increased focus on massive data transfers and instantaneous data travel in the network, the aging three-tier design within a data center is being replaced with what is being called the Leaf-Spine design. It is also referred to as leaf and spine topology, in this design there are switches found at the top of each rack that connect to the servers in the rack,with a server connecting into each switch for redundancy. People refer to this as a top-of-rack (ToR) design because the switches physically reside at the top of the rack.

The Leaf layer consists of access switches that connect to devices like servers, firewalls, load balancers, and edge routers. The Spine layer (made up of switches that perform routing) is the backbone of the network, where every Leaf switch is interconnected with each and every Spine switch.

**SOHO:** Means small office,home office, and is a small network connecting a user or small handful of users to the internet and office resources such as servers and printers. Usually just one router and a switch, or two, plus a firewall.

**Tier 2 Design:** This is a hierarchical design that includes access and distribution layers. The access layer connects end devices, such as PCs and printers, while the distribution layer aggregates traffic from the access layer and connects to the core layer. This design provides a scalable and modular network that is easy to manage. It's also known as collapsed core design because it's only 2 layers. In this the distribution layer is merged with the core layer.

**Tier 3 Design:** This is a hierarchical design that includes access, distribution, and core layers. The access layer connects end devices, the distribution layer aggregates traffic from the access layer, and the core layer provides high-speed switching and routing for the distribution layer. This design is used in large enterprise networks and provides a high level of scalability, reliability, and performance. In this cisco defines 3 layers of hierarchy, the core,distribution, and access each with specific function and it's referred to as a 3-tier network architecture.

**Fabric Design:** This is a modern design that uses software-defined networking (SDN) to create a single, unified network fabric. The fabric design provides a flexible, scalable, and automated network that can adapt to changing business needs.

**Capacity Planning:** This involves estimating the future growth of the network and planning for the necessary capacity to support it. Capacity planning includes analyzing traffic patterns, predicting future traffic growth, and designing the network to accommodate the anticipated traffic.

A core is called collapsed when you move the role of the core switches to the distribution switches, merging the core- and distribution layer. We do this by directly connecting the distribution switches to each other, instead of through a core switch.

**Common features of most NGFWs:**

**1. Standard firewall features:** These include the traditional (first-generation) firewall functionalities such as stateful port/protocol inspection, Network Address Translation (NAT), and Virtual Private Network (VPN).

**2. Application identification and filtering:** This is the chief characteristic of NGFWs. This feature identifies and filters traffic based upon the specific applications, rather than just opening ports for all kinds of traffic. This prevents malicious applications and activity from using non-standard ports to avoid the firewall.

**3. SSL and SSH inspection:** NGFWs can even inspect SSL and SSH encrypted traffic. This feature decrypts traffic, makes sure the applications are allowed, checks other policies, and then re-encrypts the traffic. This provides additional protection from malicious applications and activity that tries to hide itself by using encryption to avoid the firewall.

**4. Intrusion prevention:** These are more intelligent capabilities and provide deeper traffic inspection to perform intrusion detection and prevention. Some of the NGFWs have built-in IPS functionality so that a stand-alone IPS might not be needed.

**5. Directory integration:** Most NGFWs include directory support (such as, Active Directory). For instance, they manage authorized applications based upon users and user groups.

**6. Malware filtering:** NGFWs can also provide reputation-based filtering to block applications that have a bad reputation. This functionality can check for phishing, viruses, and other malware sites and applications

A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.

A next-generation firewall (NGFW) does this, and so much more. In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to Gartner's definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Threat intelligence sources
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

In summary, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

## 1.2. High availability techniques such as redundancy, FHRP, and SSO

High availability techniques are used to ensure that network services are always available, even in the event of hardware or software failures. Some of the high availability techniques used in enterprise networks include:

Redundancy: This involves using multiple components, such as switches or routers, to provide

backup in case of failure. Redundancy can be achieved through device-level redundancy, link-level redundancy, or path-level redundancy.

First Hop Redundancy Protocols (FHRP): This is a protocol used to provide redundancy for IP default gateways. FHRP allows multiple routers to share the same IP address and provide redundancy in case of failure.

Stateful Switchover (SSO): This is a feature used to provide redundancy for network devices, such as switches or routers. SSO allows the active device to synchronize its state with the standby device, so that if the active device fails, the standby device can take over without interruption.

**First-hop router (FHR):** A router that is directly attached to the source, also known as a root router. It is responsible for sending register messages to the RP. A Rendezvous Point (RP) is a router in a multicast network domain that acts as a shared root for a multicast shared tree.

**Multicast Routing Information Base (MRIB):** A topology table that is also known as the multicast route table (mroute), which derives from the unicast routing table and PIM. MRIB contains the source S,group G, incoming interfaces (IIF), outgoing interfaces (OIFs), and RPF neighbor information for each multicast route as well as other multicast-related information.

**Multicast Forwarding Information Base (MFIB):** A forwarding table that uses the MRIB to program multicast forwarding information in hardware for faster forwarding.

**Last-hop router (LHR):** A router that is directly attached to the receivers, also known as a leaf router. It is responsible for sending PIM joins upstream toward the RP or to the source.

**Outgoing interface (OIF):** Any interface that is used to forward multicast traffic down the tree, also known as the downstream interface.

## 2. Analyze design principles of a WLAN deployment

### 2.1 Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)

There are different wireless deployment models that can be used in WLAN design, including:

**Centralized:** This model uses a centralized controller to manage and control the wireless access points (APs). All the configuration and management tasks are performed by the controller, which communicates with the APs over the wired network.

**Distributed:** This model distributes the control and management functions among the APs. Each AP acts as a controller for the nearby APs, and all the APs work together to provide a seamless wireless network.

**Controller-less:** This model eliminates the need for a central controller. Each AP operates independently and makes its own decisions about channel selection, power levels, and other network settings.

**Controller-based:** This model uses a central controller to manage and control the APs. The controller communicates with the APs over the wired network and provides centralized management and control of the wireless network.

**Cloud:** This model uses a cloud-based controller to manage and control the wireless network. The controller is hosted in the cloud and can be accessed from anywhere using a web browser.

**Remote Branch:** This model is designed for remote branch offices or small businesses. It uses a small, all-in-one device that combines the functions of a router, switch, and wireless access point.

Note that the connectivity was slow or intermittent. If there were any mode/SSID mismatch, there wouldn't be any communication at all. It is also likely that the wireless phones, filing cabinets, and antenna mismatch errors are adding to the problem.

A trunk link can be negotiated between two switches only if both switches belong to the same VLAN Trunking Protocol (VTP) management domain or, if one or both switches have not defined their VTP domain (that is, the NULL domain). If the two switches are in different VTP domains and trunking is desired between them, you must set the trunk links to ON mode or no-negotiate mode. This setting forces the trunk to be established.

A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master", also called as "zombie". It is from the zombie that the intruder identifies and communicates with other systems that can be compromised. The intruder loads hacking tools on the compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. This causes Distributed Denial of Service (DDoS) attack on the target computer.

The SSID needs to be consistent for a wireless client to roam between LWAPs that are managed by the same WLC. However, if the LAPs are managed by different WLCs, then the Mobility group must be same on the WLCs. A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC loading information, and can also forward data traffic among them, which enables inter-





 

controller wireless LAN roaming and controller redundancy. Note that the WLCs may be in the same or different IP subnet or VLAN. WLCs use what is known as Ether-IPtunnel to transfer User traffic from one WLC to another.
Assuming that a User (or Client) originally joined the WLAN on WLC1, WLC1 will always refer to itself as the User's anchor point. Any controller that is serving the User from a different subnet is known as a foreign agent. As the client continues to roam, the anchor WLC will follow its movement by shifting the Ether-IP tunnel to connect with the User's foreign WLC.

In order for a wireless client to seamlessly roam between mobility group members (WLCs), WLAN's SSID and security configuration must be configured identically across all WLCs comprising the mobility group.

**Intruder Prevention System (IPS):** IPS analyses network traffic, can report and take corrective action on traffic that it deems malicious or harmful. This can be implemented as an appliance, as a blade, or as a module in an ASA or IOS router. The primary method for identifying problem traffic is through signature matching.

**Cisco Security Manager (CSM):** This is an enterprise-level configuration tool that you can use to manage most security devices.

**Cisco Security Intelligence Operations (SIO) Service:** The SIO researches and analyses threats and provides real-time updates on these threats. There is also an application for smart phones.

**Location Services in a WLAN Design:**

Location services are used to track the physical location of wireless clients and devices in a WLAN. This can be useful for a variety of applications, such as asset tracking, security, and location-based services. There are different location services that can be used in a WLAN design, including:

Radio Frequency Identification (RFID): This technology uses radio waves to identify and track objects that have an RFID tag attached to them. RFID can be used to track assets or inventory in a warehouse or to locate people in a large building.

Wireless LAN Context-Aware Services (WLCS): This technology uses wireless access points to detect the location of wireless devices based on their signal strength and other factors. WLCS can be used to track the location of people or devices in a building or to provide location-based services.

Global Positioning System (GPS): This technology uses satellite signals to determine the location of a device. GPS can be used to track the location of vehicles or assets that are moving outdoors.

Bluetooth Low Energy (BLE): This technology uses low-power Bluetooth signals to detect the location of nearby devices. BLE can be used to track the location of people or assets in a building or to provide location-based services.

## 2.2 Differentiate between on-premises and cloud infrastructure deployments

On-premises and cloud infrastructure deployments are two different approaches to IT infrastructure deployment, each with its own advantages and disadvantages. Here are the differences between the two:

**1. Deployment Location:** On-premises infrastructure is deployed on-site within an organization's own physical data center, while cloud infrastructure is deployed off-site in a third-party data center managed by a cloud service provider.

**2. Control:** With on-premises infrastructure, the organization has complete control over the infrastructure, including hardware, software, and networking. In contrast, with cloud infrastructure, the organization has limited control over the infrastructure, as the cloud service provider manages the underlying infrastructure.

**3. Scalability:** On-premises infrastructure requires organizations to purchase, install, and configure hardware and software as they grow. This can be expensive and time-consuming. Cloud infrastructure, on the other hand, provides organizations with the ability to scale up or down quickly and easily, without the need for additional hardware or software.

**4. Cost:** On-premises infrastructure requires organizations to purchase and maintain their own hardware and software, which can be expensive. Cloud infrastructure, on the other hand, is typically offered on a subscription basis, which can be more cost-effective for organizations that do not have the resources to maintain their own infrastructure.

**5. Maintenance:** With on-premises infrastructure, organizations are responsible for maintaining and upgrading their own hardware and software. This can be time-consuming and costly. With cloud infrastructure, the cloud service provider is responsible for maintaining and upgrading the underlying infrastructure, freeing up time

and resources for the organization.

**6. Security:** On-premises infrastructure provides organizations with more control over security, as they can implement their own security policies and procedures. With cloud infrastructure, the organization must rely on the cloud service provider to implement and enforce security policies.

In summary, the choice between on-premises and cloud infrastructure deployments depends on the organization's specific needs, resources, and priorities. On-premises infrastructure provides more control, while cloud infrastructure provides scalability and cost-efficiency.