**MODULE : CCNA Automation and Programmability**

**Que 1** **: Explain** **How Automation impacts Network Management**

**Ans :** Network management includes two aspects: configuration management and operational management.

**Configuration management** refers to any feature or function that changes device configuration. **Operational management** includes reporting, monitoring, gathering operational data, and alerting administrators to possible issues.

* Automation provides the following benefits.

**Reduce the network cost**

It reduces the network cost by automating the many tasks that technicians would traditionally need to perform by visiting each device. With automation, they do not need to visit every device to configure and manage it. They can create automation procedures and scripts on a controller device and the controller device will configure and manage devices. Since most of the tasks are performed by a controller device, a company needs fewer technicians.

**Reduce the time to complete projects**

Traditional networking requires administrators to visit each device to apply configuration. It consumes too much time. Automation saves this time by remotely applying changes.

**Provide consistent configuration**

Automation provides consistency in configurations. With automation, administrators create scripts and then instruct the controller to deploy them to the devices; each device receives the same configuration. Since administrators are not required to type the same configuration commands over and over on each device, it causes fewer configuration errors.

**Make network management easier**

In traditional networking, administrators manage each device individually. It makes device management complex and tedious. With automation, they can manage all devices from a central location. It makes device management easy and fast.

**Simplify network operations**

Automation simplifies network operations by using scripts. Without automation, administrators have to monitor all devices manually. With automation, they can create a script and deploy it on the controller device. The controller device monitors all devices and notifies the administrator when an event occurs.

**Que 2 : Compare Traditional network with Controller based networking**

**Ans:** There are two types of networking environments: traditional networking environments and controller-based networking environments. In this tutorial, we will compare both and understand the main differences between them.

## Traditional networking environments

In traditional networking environments, we individually configure and manage each network device. For example, if we have 10 routers in our network, we need to configure and manage them separately.

Configuring and managing each network device is a tedious task. Since we configure each device manually by entering commands, there is also a possibility of mistakes.

With traditional networking environments, we take the following actions for each network device over the lifetime of the device:

* We install the network device (such as a router or a switch) into the network.
* We make the initial configuration of the device. The initial configuration allows the device to perform its functions in the network.
* We monitor the overall performance of the device and events that occur on the device. For this, we can use network management protocols such as SNMP (Simple Network Management Protocol) and NetFlow.
* Over time, we modify and update the configuration as per the requirements of the network.
* We upgrade the operating system on the device as needed.

### Key points:-

* Administrators manage all devices independently. To manage them, they have to establish a new connection each time. They also have to terminate the connection after making the changes.
* Administrators manually make all changes. Manual configuration is prone to configuration errors.
* It uses the blacklisting security model. In this model, everything is allowed unless you disallow it.

## Controller-based networking environments

Controller-based networking uses automation technologies to apply configuration changes to multiple devices at the same time. It uses the controller software or device that automates configuration changes on the network and manages the deployment of configuration changes to multiple devices simultaneously. It actively monitors the network for changes. When we add a new device to the network, it automatically applies the initial configuration to the device, without needing our intervention.

### Key points: -

Administrators manage all devices collectively. To manage them, they use the controller software or appliance.

Administrators only need to configure the controller software or appliance. The controller software or appliance manages all devices automatically based on their configuration.

Since the controller configures all devices, the chances of configuration errors are zero unless the administrator configures the controller device incorrectly.

It uses the whitelisting security model. In this model, everything is blocked unless you allow it. It enhances the network's security.

**Que 3 : Explain Virtualization**

**Ans :** Virtualization is technology that you can use to create virtual representations of servers, storage, networks, and other physical machines. Virtual software mimics the functions of physical hardware to run multiple virtual machines simultaneously on a single physical machine.

* It reduces network costs. Since the maximum work is done by the controller software or appliance and a company needs only one or two administrators to manage the controllers, it does not need to hire many administrators.

**Que 4 : Explain method of Automation**

**Ans :** Automation includes the use of various equipment and control systems such as machinery, processes in factories, boilers, and heat-treating ovens, switching on telephone networks, steering, stabilization of ships, aircraft and other applications and vehicles with reduced human intervention.

**Que 5 : Explain SDN**

**Ans : Software defined networking (SDN)** is an approach to network management that enables dynamic, programmatically efficient network configuration to improve network performance and monitoring.It is a new way of managing computer networks that makes them easier and more flexible to control.

In traditional networks, the hardware (like routers and switches) decides how data moves through the network, but SDN changes this by moving the decision-making to a central software system. This is done by separating the **control plane** (which decides where traffic is sent) from the **data plane** (which moves packets to the selected destination). In this article, we will discuss Software-Defined Networking in detail, including its workings, different models, and architecture.

**Que 6 : Explain DNS Center**

## Ans : DNS Definition

The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. Every device connected to the internet has its own IP address, which is used by other devices to locate the device. DNS servers make it possible for people to input normal words into their browsers, such as Fortinet.com, without having to keep track of the IP address for every website.

## What Is A DNS Server?

A DNS server is a computer with a database containing the public IP addresses associated with the names of the websites an IP address brings a user to. DNS acts like a phonebook for the internet. Whenever people type domain names, like Fortinet.com or Yahoo.com, into the address bar of web browsers, the DNS finds the right IP address. The site’s IP address is what directs the device to go to the correct place to access the site’s data.

Once the DNS server finds the correct IP address, browsers take the address and use it to send data to content delivery network (CDN) edge servers or origin servers. Once this is done, the information on the website can be accessed by the user. The DNS server starts the process by finding the corresponding IP address for a website’s uniform resource locator .

## How Does DNS Work?

In a usual DNS query, the URL typed in by the user has to go through four servers for the IP address to be provided. The four servers work with each other to get the correct IP address to the client, and they include:

1. **DNS recursor**: The DNS recursor, which is also referred to as a DNS resolver, receives the query from the DNS client. Then it communicates with other DNS servers to find the right IP address. After the resolver retrieves the request from the client, the resolver acts like a client itself. As it does this, it makes queries that get sent to the other three DNS servers: root nameservers, top-level domain (TLD) nameservers, and authoritative nameservers.
2. **Root nameservers**: The root nameserver is designated for the internet's DNS root zone. Its job is to answer requests sent to it for records in the root zone. It answers requests by sending back a list of the authoritative nameservers that go with the correct TLD.
3. **TLD nameservers**: A TLD nameserver keeps the IP address of the second-level domain contained within the TLD name. It then releases the website’s IP address and sends the query to the domain’s nameserver.
4. **Authoritative nameservers**: An authoritative nameserver is what gives you the real answer to your DNS query. There are two types of authoritative nameservers: a master server or primary nameserver and a slave server or secondary nameserver. The master server keeps the original copies of the zone records, while the slave server is an exact copy of the master server. It shares the DNS server load and acts as a backup if the master server fails.

**Que 7 : Explain SD-A CCESS and SD-WAN**

**Ans :** SD-WAN and SD-Access are ways to approach software-defined networking terminology. While SD-Access is used to change the architecture of LAN networks, SD-WAN creates next-generation wide area networks with significant automation capabilities instead of MPLS/VPLS.