**CCNA ASSIGMENT**

**MODULE 5**

1. Explain How Automation Impacts Network Management

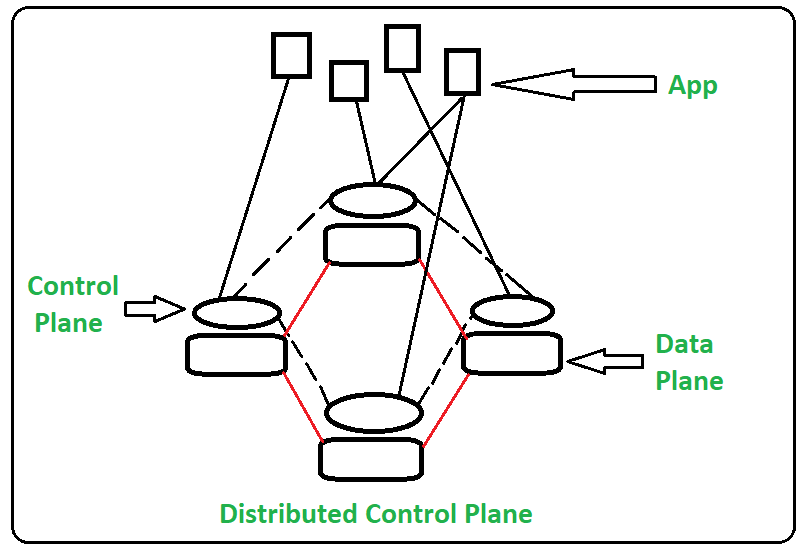
Network automation is the process of automating the configuring, managing, testing, deploying, and operating of physical and virtual devices within a network. With everyday network tasks and functions automated and repetitive processes controlled and managed automatically, network service availability improves.

Any type of network can use network automation. Hardware- and software-based solutions enable data centres, service providers, and enterprises to implement network automation to improve efficiency, reduce human error, and lower operating expenses.

1. Compare Traditional network with Controller based networking

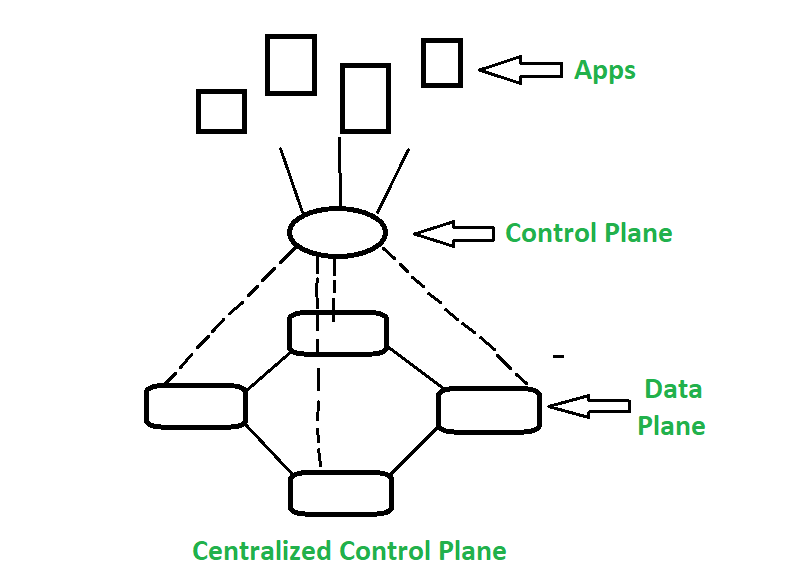
Traditional network refers to the old conventional way of networking which uses fixed and dedicated hardware devices such as routers and switches to control network traffic. Inability to scale and network security and Performance are the major concern now a days in the current growing business situation so that SDN is taking control to traditional network. Traditional network is static and based on hardware network appliances.

Traditional network architecture was used by many companies till recent years but now a days due to its drawbacks Software Defined Network has been developed and in coming years it will be used more.



SDN stands for Software Defined Network which is networking architecture approach. It enables the control and management of network using software applications. Through Software Defined Network (SDN) networking behavior of entire network and its devices are programmed in centrally controlled manner through software applications using open APIs.

Software Defined Network improves performance by network virtualization. In SDN software controlled applications or APIs work as basis of complete network management that may be directing traffic on network or to communicate with underlying hardware infrastructure. So in simple we can say SDN can create virtual network or it can control traditional network with the help of software.



1. Explain Virtualization

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as Host Machine and that virtual machine is referred as a Guest Machine

Types of Virtualization:

* Hardware Virtualization.
* Operating system Virtualization.
* Server Virtualization.
* Storage Virtualization.

1. Describe Characteristics of REST-based API

Representational State Transfer (REST) is an architectural style that defines a set of constraints to be used for creating web services. REST API is a way of accessing web services in a simple and flexible way without having any processing.

REST technology is generally preferred to the more robust Simple Object Access Protocol (SOAP) technology because REST uses less bandwidth, simple and flexible making it more suitable for internet usage. It’s used to fetch or give some information from a web service. All communication done via REST API uses only HTTP request.

Working: A request is sent from client to server in the form of a web URL as HTTP GET or POST or PUT or DELETE request. After that, a response comes back from the server in the form of a resource which can be anything like HTML, XML, Image, or JSON. But now JSON is the most popular format being used in Web Services.

1. Explain methods of Automation

Network automation is the process of using software to automate network and security provisioning and management in order to continuously maximize network efficiency and functionality. Network automation is often used in conjunction with network virtualization.

IT departments today seek speed, agility, and consistency in provisioning and managing both traditional and cloud-native applications. A modern network automation platform can achieve these goals by automating networking functions like resource provisioning, network mapping, and network testing.

Network Automation enables you to speed application deployment by automating network and security provisioning and management through the complete application lifecycles and across data center and cloud environments.

Automate Your IT: Take the next step in digital transformation by virtualizing and automating network and security operations – an area of infrastructure that’s traditionally been largely hardware-based and required manual provisioning and management.

Accelerate New App Development: Embrace new cloud-native applications and DevOps workflows with networking and security management that easily integrates into developer processes without requiring retooling.

See Clearly Across Environments: Exchange a traditionally limited view of network traffic and security dependencies for global visibility and effortless troubleshooting of your network and security policies.

Network automation software finds the most efficient way to map, configure, provision, and manage a network. API-based automation replaces manual, command-line instructions to configure each networking device. The APIs can be invoked directly or go through a programming language, for example Python, Java or Go. Scripts are only one aspect of network automation—a modern automation platform monitors network resources when provisioning and verifies that a network will be able to handle a configuration request before implementing it.

1. Explain SDN

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. SDN can create and control a virtual network – or control a traditional hardware – via software.

While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server.

Increased control with greater speed and flexibility: Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.

Customizable network infrastructure: With a software-defined network, administrators can configure network services and allocate virtual resources to change the network infrastructure in real time through one centralized location. This allows network administrators to optimize the flow of data through the network and prioritize applications that require more availability.

Robust security: A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

1. Explain DNA Centre

Cisco DNA is a controller-based architecture. Having Cisco DNA Centre at its core, Cisco DNA provides the policy, automation, and analytics required to adapt to change, simplify and scale operations, and protect against degradation and threats. It provides 360-degree open platform extensibility to vastly increase the network’s value by opening the way for new and innovative applications, processes, and solutions that are required today, and those that will be needed in the future.

Intent-based networking (IBN) built on Cisco DNA takes a software-delivered approach to automating and assuring services in your campus and branch networks and across your WAN. Cisco DNA can help you to streamline operations, analyse and resolve issues faster, and increase user productivity by optimizing application performance.

Automate, analyse, and optimize

Automate, analyse, and optimize

Translate business intent into network policies, and use automation and AI/ML analytics to help achieve business outcomes.

Detect, contain, and mitigate threats

Detect, contain, and mitigate threats

Get complete visibility into user activity, devices, things, and traffic to enforce zero-trust security.

Enterprise-grade services

Deliver the multi cloud world

Provide consistent and secure application delivery in today's highly distributed hybrid and multi cloud environment to optimize the user experience.

Centralize design and management

Centralize design and management

Take control of your network and orchestrate functions with onsite and cloud-based network controllers.

1. Explain SD-Access and SD-WAN

SD-Access as name suggested Software defined Access for changing the architecture of the LAN networks while SD-WAN as software defined WAN which can automate and may be next generation networks over the MPLS/VPLS. MPLS is still have a hold through the service provider end, but using the SD-WAN will get rid of the control from the service provider.

SD-Access

SD-Access has the components like DNA-Centre which acts as a controller for control plane and while data plane is still with the devices in the network. Make sure you understand the difference between the DNA and DNA-Centre.

DNA is an architecture while DNA-Centre is the controller in that architecture. The other main component is Cisco ISE. Cisco ISE as already discussed in my previous articles is used for authentication for the users in the network.

SD-WAN

Similarly for the SD-WAN Viptela architecture, there are three controllers which can be on the cloud or on-perm deployment and can have the control plane. All devices in the SD-WAN architecture works on the zero trust model and to maintain the trust between them they need to create the DTLS/TLS tunnels and exchange the certificates which are preloaded on the devices.

Make sure you understand the traffic routed to the controller which is in the cloud generally is only the control plane traffic. The End devices can be connected for the data plane traffic over the secured IPSEC/GRE tunnels.

SD-WAN is basically a application aware network and choose path on the based parameters like SLA, Jitter and so on. You can use VRRP protocol to switch the traffic flow from LAN to different SD-WAN routers and the IPSEC/GRE tunnel will originate from one SD-WAN to another SD-WAN router based upon the traffic flow which control instructs.