Assignment :- Module 11 CCNA - Automation and Programmability

1. Explain How Automation Impacts Network Management

Answer:-Automation simplifies network management by reducing manual tasks, minimizing human errors, and increasing efficiency. It allows for faster deployment, configuration, and troubleshooting of network devices. With automation tools like Ansible, Python scripting, and APIs, network administrators can manage complex networks with ease, ensuring better performance, security, and scalability.

2. Compare Traditional Network with Controller-Based Networking

Answer:-

Traditional Network:

1. Manual Configuration – Each device needs to be configured separately by hand.
2. Difficult to Scale – Adding and managing new devices is complex.
3. CLI-Based Management – Network admins must use the command-line interface (CLI) for changes.
4. High Chance of Errors – Manual configurations can lead to mistakes, causing network issues.
5. Security Challenges – Managing security across multiple devices is difficult and time-consuming.

Controller-Based Networking:

1. Centralized Control – A network controller manages all devices from one place.
2. Easy to Scale – Adding new devices is quick and automated.
3. Automation & APIs – Uses software tools to configure and manage networks efficiently.
4. Consistent Performance – Reduces errors and ensures smooth network operation.
5. 5. Better Security – Security policies are applied automatically across the network.

3. Explain Virtualization

Answer:-Virtualization is a technology that allows multiple virtual instances of servers, networks, and storage to run on a single physical hardware. In networking, virtualization enables multiple virtual networks to operate independently on shared infrastructure. It improves resource utilization, enhances security, and simplifies network management.

4. Describe Characteristics of REST-based API

Answer:-REST (Representational State Transfer) API follows certain principles:

Stateless – Each request from a client to the server must contain all the necessary information.

Client-Server Architecture – The client and server are independent of each other.

Cacheable – Responses can be cached to improve performance.

Uniform Interface – Uses standard HTTP methods like GET, POST, PUT, and DELETE.

Scalability – Supports a large number of interactions efficiently.

5. Explain Methods of Automation

Answer:-There are several methods used for network automation:

Python Scripting – Automates network configurations and monitoring.

Ansible – A configuration management tool that automates deployment.

REST APIs – Allows communication between network devices and applications.

NETCONF & YANG – Protocols used for programmatic network configuration.

SDN (Software-Defined Networking) – Centralized control of network devices.

6. Explain SDN (Software-Defined Networking)

Answer:-SDN is a network architecture that separates the control plane from the data plane, allowing centralized control through software controllers. This improves flexibility, scalability, and automation in networking. SDN enables dynamic traffic management and enhances security through centralized policies.

7. Explain Cisco DNA Center

Answer:- Cisco DNA (Digital Network Architecture) Center is a centralized network management platform that helps automate, monitor, and secure networks. It provides network administrators with a graphical user interface (GUI) and APIs to easily configure and troubleshoot network devices.

Key Features of Cisco DNA Center:

1. Intent-Based Networking – Ensures network changes align with business goals.

2. AI-Driven Insights – Uses artificial intelligence to analyze network performance and detect issues.

3. Security Policy Enforcement – Applies security policies consistently across the network.

4. Automated Network Provisioning – Reduces manual work by automating device configurations and deployments.

8. Explain SD-Access and SD-WAN

Answer:- SD-Access (Software-Defined Access) – It is a Cisco solution that provides automated end-to-end segmentation to improve security and policy enforcement across wired and wireless networks.

SD-WAN (Software-Defined Wide Area Network) – It optimizes WAN connectivity by dynamically routing traffic based on network conditions, improving performance and reducing costs compared to traditional MPLS-based WANs.