Module 11 CCNA -Automation and Programmability

(Network Troubleshooting)

1.Explain How Automation Impacts Network Management.

Ans: Network automation involves using software, scripts, or tools to perform repeatable operations such as configuring, managing, and troubleshooting network devices without requiring manual intervention. It automates the device provisioning, IP allocation, vlan setup, routing updates, traffic monitoring, etc, for all of the device at once. Automation speeds up network management, keeps configurations uniform, and is highly scalable particularly in large-enterprise networks which amount to endless two-day long configuration of every device. It enhances equipment efficiency, decreases operational costs, and allows for better real-time monitoring and troubleshooting. For instance, instead of setting 100 hundred switches one at a time, an automation script or a tool can configure all devices at once, minutes after all traffic is redirected and see what happens and it can revert all changes instantly.

2. Compare Traditional network with Controller based networking.

Ans:

Feature	Traditional Networking	Controller-Based Networking
Control Plane	Distributed → Each device manages its own control logic	Centralized → A controller manages the entire network
Configuration	Manual, device-by-device via CLI	Centralized automation via controller GUI/API
Scalability	Hard to scale in large networks	Highly scalable and efficient
Management	Complex, time-consuming	Simplified and centralized
Example	Configuring routers & switches separately	Using Cisco DNA Center or SDN controllers

3. Explain Virtualization.

Ans: Virtualization is the ability to run multiple virtual environments on a single physical unit. It stands up virtual machines (VMs), virtual networks or virtual storage using software such as VMware, VirtualBox or Hyper-V. Such technology cuts cost for organizations by eliminating the requirement for several physical devices as well as improving resource utilization. There are several different forms of virtualization, such as server virtualization, which enables several virtual machines to run on the same server, network virtualization, that isolates virtual networks on physical infrastructure, and storage virtualization, which groups several storage systems together to make them function as a single storage entity. For instance, instead of purchasing ten physical servers for ten applications, a corporation could host the ten applications as ten virtual machines on.

4. Describe Characteristics of REST-based API.

Ans: REST (Representational State Transfer) is an architectural style used to design web APIs that allow different systems and applications to communicate with each other. REST-based APIs are stateless, meaning each request from a client to a server is independent and contains all the necessary information for processing. They follow a client-server model, where the client requests resources and the server provides responses. REST APIs use standard HTTP methods such as GET for retrieving data, POST for creating data, PUT/PATCH for updating data, and DELETE for removing data. They are resource-based, meaning resources are represented using unique URLs, and they usually exchange data in lightweight formats such as JSON or XML. For example, using a REST API, a request like GET https://api.example.com/devices could fetch a list of all connected network devices

5. Methods of Automation

Network automation can be implemented using different methods depending on the complexity and requirements of the network. The first method is scripting-based automation, where administrators use programming languages such as Python, Bash, or PowerShell to create scripts for configuring and managing devices. The second method is API-based automation, where REST APIs are used to interact directly with network devices or controllers for performing tasks such as creating VLANs, updating firmware, or monitoring traffic. The third method is configuration management tools such as Ansible, Puppet, and Chef, which are designed to automate device configurations at scale. Finally, orchestration platforms are used to manage multiple automation tools and workflows together, especially in large data centers and cloud environments. These methods improve efficiency, reduce manual errors, and make network management faster.

6. Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is a modern networking approach that separates the control plane from the data plane and centralizes network management using an SDN controller. In traditional networks, each device independently manages routing, switching, and security policies, which makes configuration difficult and time-consuming. With SDN, a centralized controller manages all the network devices, making it easier to configure, monitor, and troubleshoot the network from a single interface. SDN uses APIs to communicate with switches, routers, and firewalls, making the network programmable and highly flexible. It improves scalability, enhances security, and supports automation. For example, instead of logging into multiple switches to configure VLANs, an administrator can use the SDN controller to deploy the configuration across the entire network at once.

7. Cisco DNA Center

Cisco DNA Center is a powerful network automation and management platform based on SDN principles. It provides a centralized dashboard for configuring, monitoring, and troubleshooting network devices. DNA Center simplifies network operations by automating tasks such as device provisioning, firmware upgrades, policy enforcement, and real-time monitoring. It also provides analytics powered by AI and machine learning to optimize network performance and detect issues proactively. The platform uses REST APIs for integration with third-party applications and supports solutions like SD-Access and SD-WAN. For example, an administrator can use DNA Center to configure VLANs, deploy security policies, and monitor network health across hundreds of switches and routers from a single interface, saving time and improving consistency.

8. SD-Access And SD-WAN

Ans:

SD-Access is a Cisco solution managed by DNA Center that automates network access control in campus and enterprise networks. It simplifies the process of creating VLANs, assigning policies, and segmenting users and devices within the network. SD-Access ensures better security by automatically assigning users to the correct network segments based on their roles and identities. It also provides end-to-end automation, making it easy to deploy large networks without complex manual configurations. For example, in a university, SD-Access can automatically place students in the student network, faculty in the faculty network, and administrative staff in the admin network, ensuring proper access control and security without additional manual work,SD-WAN is a networking technology that simplifies the management and operation of wide-area networks by using software to control the connectivity between remote sites, branch offices, and data centers. Unlike traditional WANs that rely on expensive MPLS circuits, SD-WAN uses a combination of broadband internet, 4G/5G, and MPLS to provide cost-effective and high-performance connectivity. It centralizes network management, allowing administrators to control multiple branch networks from a single dashboard. SD-WAN improves application performance by dynamically selecting the best available path for traffic and provides built-in encryption for secure communications. For example, a company with offices in multiple cities can use SD-WAN to connect all branches securely over the internet without investing in costly private leased lines.