Module 11 CCNA-Automation and Programmability

1. Compare Traditional Network with Controller-Based Networking

In traditional networking, each device (like routers and switches) is configured individually using the Command Line Interface (CLI). This means if you have 10 switches, you need to configure each one manually. It’s time-consuming and can lead to mistakes, especially in large networks. Also, troubleshooting can be hard because you have to check each device separately.

In controller-based networking, there’s a central controller that manages all the devices. Instead of configuring each device manually, you just tell the controller what you want, and it configures all the devices for you. This makes things faster, easier, and less prone to errors. For example, Cisco DNA Center is a controller that can manage many devices at once. It’s like having a boss who tells all the workers what to do, instead of each worker figuring it out on their own.

2. How Automation Impacts Network Management

Automation is like having a robot do repetitive tasks for you. In networking, automation helps in many ways:

- Saves Time: Instead of typing commands for every device, you can write a script or use a tool to do it automatically.

- Reduces Mistakes: Humans make errors, but automation follows the same steps every time, so there’s less chance of mistakes.

- Makes Scaling Easier: If you have a big network with hundreds of devices, automation helps you manage them all without extra effort.

- Improves Troubleshooting: Automated tools can quickly find problems and even fix them in some cases.

- Saves Money: By reducing manual work, companies can save on labor costs.

For example, instead of logging into 50 switches to update a setting, you can use a tool like Ansible to update all of them at once.

3. Explain Virtualization

Virtualization is like creating a “virtual” version of something physical. For example, instead of having 10 physical servers, you can have one powerful server running 10 virtual servers. This saves space, power, and money.

In networking, virtualization means creating virtual networks on top of physical hardware. For example:

- VLANs (Virtual LANs): You can split one physical network into multiple virtual networks.

- VPNs (Virtual Private Networks): You can create a secure virtual network over the internet.

- NFV (Network Functions Virtualization): Instead of using physical devices like firewalls, you can run them as software on a server.

Virtualization makes networks more flexible and efficient because you can easily change things without buying new hardware.

4. Describe Characteristics of REST-Based API

APIs (Application Programming Interfaces) are like messengers that let different software talk to each other. REST (Representational State Transfer) is a type of API that uses standard web protocols like HTTP.

Here are some key characteristics of REST-based APIs:

- Uses HTTP Methods: REST APIs use common HTTP methods like GET (to read data), POST (to create data), PUT (to update data), and DELETE (to remove data).

- Stateless: Each request is independent, and the server doesn’t need to remember previous requests.

- Resource-Based: Everything is treated as a resource, like a URL. For example, `https://api.example.com/devices` could represent a list of devices.

- Data Formats: REST APIs usually use JSON or XML to send and receive data.

- Scalable: Because it’s stateless, REST APIs can handle many requests easily.

For example, Cisco DNA Center has REST APIs that let you automate tasks like adding new devices or checking network health.

5. Explain Methods of Automation

Automation in networking can be done in many ways:

- Scripting: Writing scripts in languages like Python to automate tasks. For example, a script can log into a router and update its configuration.

- Ansible: A tool that automates configuration management. You write playbooks (like recipes) that tell Ansible what to do, and it does it for you.

- Puppet/Chef: Similar to Ansible, these tools help automate and manage configurations across many devices.

- SDN (Software-Defined Networking): A controller automates the entire network by managing devices centrally.

- Intent-Based Networking (IBN): You tell the network what you want (your intent), and it automatically configures itself to meet that goal.

For example, if you want to update the password on 100 routers, you can write a Python script or use Ansible to do it in minutes instead of doing it manually.

6. Explain SDN (Software-Defined Networking)

SDN is a new way of managing networks. In traditional networks, each device makes its own decisions (like how to route traffic). In SDN, there’s a central controller that makes all the decisions, and the devices just follow orders.

Here’s how it works:

- Controller: The brain of the network. It decides how traffic should flow.

- Southbound API: This is how the controller talks to the devices. A common example is OpenFlow.

- Northbound API: This is how applications talk to the controller. For example, a monitoring app might ask the controller for network stats.

SDN makes networks more flexible and easier to manage because you can change the entire network just by updating the controller.

7. Explain DNA Center

Cisco DNA Center is a tool that helps manage networks. It’s like a control center for your network. Here’s what it can do:

- Design: Helps you plan and design your network.

- Policy: Lets you create rules (policies) for how the network should behave.

- Provisioning: Automates the setup of new devices.

- Assurance: Monitors the network and helps you find and fix problems.

For example, if you add a new switch to your network, DNA Center can automatically configure it and make sure it follows your policies.

8. Explain SD-Access and SD-WAN

SD-Access (Software-Defined Access):

- This is for managing access to your network, especially in large organizations.

- It uses a fabric (a kind of virtual network) to connect devices and users.

- It makes it easy to set rules (like who can access what) and improves security by isolating different parts of the network.

SD-WAN (Software-Defined Wide Area Network):

- This is for managing connections between different locations, like branch offices.

- Instead of using expensive MPLS connections, SD-WAN can use cheaper internet connections.

- It makes it easy to manage and optimize traffic across all locations.

For example, if a company has offices in New York and London, SD-WAN can help them connect securely and efficiently without spending too much money.