Module 11 CCNA -Automation and Programmability

1. **Explain How Automation Impacts Network Management**
    - Automation is changing network management by increasing efficiency, improving visibility, speeding up events, ensuring consistency and compliance, simplifying network configuration and orchestration, and leveraging advanced analytics for optimization. By leveraging automation, organizations can reduce operating costs and free up valuable human resources for initial ideas while building reliable, efficient and flexible networks.

2. **Compare Traditional network with Controller based networking**
    - Traditional communication systems rely on distributed management functions across a single client, causing problems with manual configuration, visibility, complex solutions, and scalability. The potential for automation is limited and network management becomes more cumbersome as network scale increases.
    - Controller-based networking provides a centralized approach to network management. The network controller is responsible for managing decisions, enabling automation and providing flexibility. Increases network visibility across traffic, operations, and security by providing effective troubleshooting and resolution.
    - Controller-based networking is a big possibility, allowing new services and policies to be easily integrated into the network. Centralized management facilitates and simplifies management by providing a good view of the network.
    - Controller-based networking is often associated with software-defined networking (SDN), which has additional benefits such as resource allocation and integration with cloud environments. Organizations can achieve better operational efficiency, faster planning, centralized management and network optimization by implementing a network manager. Minimizes manual work, minimizes configuration errors, and increases response time to network issues.Additionally, automation and analytics can provide better insights for decision making and optimization of network operations.

3. **Explain Virtualization**
    - Virtualization is the process of creating physical instances such as servers, storage devices, networks or processes. It involves using a software layer called a hypervisor to create and manage virtual machines (VMs) that can run their own operating systems and applications. Virtualization provides many benefits such as server consolidation, resource efficiency, isolation, security, flexibility, and easy migration of VMs. It enables organizations to better utilize hardware, reduce costs, improve security, and simplify the management and deployment of applications. Virtualization has become a core technology in the data center, enabling businesses to gain greater speed, efficiency and cost savings while improving their IT infrastructure.
4. **Describe Characteristics of REST-based API**
    - REST (Representational State) is a framework for building web applications and APIs (Application Programming Interfaces). A REST-based API follows a set of methods and properties that define its design and behavior. The main features of the REST based API are as follows:
    - **Stateless:** The REST based API is stateless, meaning every client-to-person request The server contains all the information needed by the server to understand and process the request. The server does not store specific information of the client on request, which adds to the convenience and convenience.
    - **Resource Oriented:** REST introduces the concept of resources and resources are defined by URIs (Uniform Resource Identifiers).Each resource must have a unique URI and the API endpoint is designed to interact with the resource. Resources can represent entities such as users, objects, or data.
    - **Uniform Interface:** A REST API based on the Uniform Interface that defines common functions for interacting with resources. An interaction usually uses HTTP methods (GET, POST, PUT, DELETE) to manage resources and HTTP event methods to indicate the result of a request (eg., 200 successes, 404 failures).
    - **Change of State:** REST based API that changes resources on behalf of clients and servers. The server provides a representation, such as a JSON or XML file, in response to the client's request. Customers may modify or apply these impressions as needed
    - **Client-Server Architecture:** The REST-based API follows the client-server architecture in which the client requests the server and the server processes and responds to requests.

- This isolation provides scalability and loose connectivity between client and server components.
- **Cacheable:** REST APIs can take advantage of caching mechanisms to improve performance and reduce the load on the server. Clients can cache responses from the server and reuse them for the same request, reducing network traffic and improving response time.
- **Layered Systems:** REST-based architectures can be built as layered systems that can have multiple agent layers (such as agents, gateways, or equivalent objects) of clients and servers. Each layer provides a specific function and the customer is not aware of the specific process while fulfilling his request.

5. Explain methods of Automation

- Automation involves the use of technology and software to perform tasks and processes with minimal human intervention. Depending on the nature of the work and technology, there are many methods and methods for automation. Some automation methods are:
- **Scripting and script-based automation:** Scripting involves writing code or scripts to automate certain tasks or tasks. These scripts can be written in various programming languages and run to perform repetitive tasks or simplify complex operations. Script-based automation is often used for tasks such as project management, data management, and application deployment.
- **Robotic Process Automation (RPA):** RPA uses software robots or "bots" to automate human interactions with computer systems. Robots can interact with user interfaces, enter data, perform calculations, and perform predefined tasks across multiple applications. RPA is often used to automate manual, code-based and repetitive tasks in business processes such as accessing data, generating reports and processing documents.
- **Workflow Automation:** Workflow automation involves automating all business processes or operations by defining steps and tasks. It often involves the integration of various systems, applications and data.Workflow automation tools provide a visual interface for creating, executing, and monitoring workflows, enabling organizations to simplify and streamline complex processes, approvals, and data flows.

- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML techniques can be used to work by training algorithms to perform tasks that normally require human intelligence. This includes tasks such as natural language processing, image recognition, fact checking, and decision making. AI and ML-based automation can be used in many areas such as customer support, data analytics, fraud detection and recommendations.
- **Application Programming Interface (API):** An API allows software systems to interact and exchange data.Automation can be achieved by integrating and orchestrating different systems using APIs. For example, data is synchronized between machines, allowing for real-time processing or updating of data. API-based automation provides integration across applications, services, and platforms.
- **Infrastructure as Code (IaC):** IaC involves managing and provisioning infrastructure resources through code. Infrastructure configurations such as servers, networking, and storage are defined and managed using scripts or manifest code.Tools such as Ansible, Chef, and Terraform are used to enable the integration and management of infrastructure resources, making it easy to deploy and scale applications and procedures.

6. Explain SDN

- SDN (Software Defined Networking) is a design method in network infrastructure that separates the control plane from the data plane. While the network equipment focuses on packet transmission in the data plane, it offers an SDN management system to control and manage the network. The SDN controller provides an overview of the network and programmable control of network behavior.
- SDN brings many benefits to network management. It supports centralized management and administration, allowing administrators to easily configure, monitor and troubleshoot the network from one place.
- Simplify network automation through programmability by simplifying tasks such as scheduling, switching, and policy management. SDN also supports dynamic network configurations, providing agility and adaptability to business changes.
- SDN is network virtualization, where multiple virtual networks can coexist on a shared physical network. This can provide better service, isolation and security for different applications or user groups. In addition, SDN provides better visibility

and analytics, allowing administrators to monitor network performance, identify problems, and improve network performance.

- SDN has applications in many areas, including data centers, wide area networks, campus networks, and service providers. It enables organizations to achieve greater efficiency, speed and cost savings by providing flexible and flexible solutions for managing today's networks.

7. Explain DNA Center

- Cisco DNA Center (Digital Network Architecture Center) is the central management system that provides integration. It functions as the command center of Cisco's digital network architecture, providing comprehensive tools and capabilities to manage and improve business networks.
- DNA Center simplifies network operations by providing a single interface to configure, monitor and troubleshoot your entire network infrastructure. It provides an overview of network devices, topology and their connections, allowing network administrators to simplify their tasks and increase efficiency. One of the most important resources of the
- DNA Center is Goal-Based Networking (IBN), which allows managers to use business management best principles to articulate their desired network results.
- These goals have been translated into network configuration and policies, reducing the complexity of network management. IBN allows administrators to set and enforce network-wide policies, achieve network integration, and maintain consistent security policies across the entire network.
- DNA Center also provides advanced analytics and validation, machine learning, and artificial intelligence to understand network activity, troubleshoot, and identify potential issues. Provides recommendations to optimize network performance and improve user experience.
- Security is a core component of DNA Center with features such as network isolation, security management, threat detection and threat response.Integrates with Cisco security solutions to provide network security management.

8. **Explain SD-Access and SD-WAN**

- SD-Access (Software Defined Access) and SD-WAN (Software Defined Wide Area Network) are two communication methods that use Software Defined Network (SDN) principles to transform and improve network connectivity.
- **SD-Access:**
- SD-Access is a design that simplifies network access and increases business network security. It combines policy-based automation, network segmentation, and integration of wired and wireless networks. The main features of SD-Access include:
    - Central Control: SD-Access uses a central control system to control and manage network policy, configuration and access control. This simplifies network management and allows network-wide policy enforcement.
    - Network Segmentation: SD-Access supports active network segmentation by dividing the network into multiple virtual networks or network segments. This increases security and provides better communication management by isolating different users or devices from each other.

    - Automated and policy-based provisioning: SD-Access automates network provisioning and configuration based on predefined policies. It enables dynamic addition of devices, automatic VLAN assignment, and simplified policy management.

    - Wired and wireless convergence: SD-Access integrates wired and wireless networks and provides unified management and policy.
    - This leads to conflicting and consistent user experience across different network access processes.

- **SD-WAN:**
    - SD-WAN is a technology that makes it easy to manage and improve the performance of wide area networks (WANs). It allows organizations to support multiple network connections such as MPLS, broadband or cellular and increase traffic on demand. Key features of SD-WAN include:

- Centralized Organization: SD-WAN provides a centralized management system for managing and configuring the entire WAN infrastructure. Managing the network is easy, providing a single interface for configuration, monitoring, and troubleshooting.
- Dynamic options: SD-WAN dynamically routes traffic between different WANs based on application requirements, network conditions, and policies. This ensures efficient use of bandwidth and improves application performance.

- Quality of Service (QoS) and Priority Actions: SD-WAN allows priority management of traffic and QoS requirements. It ensures that critical applications receive the necessary bandwidth and network resources to maintain performance.
- Security and Protection: SD-WAN includes security features such as VPN tunneling and encryption to protect data transferred over the WAN.
- It supports secure connections between different offices, data centers and cloud services.

- Application Insights and Management: SD-WAN provides visibility into application performance and network connectivity. Administrators can monitor application usage, troubleshoot performance issues, and enforce application-specific policies.