**Module : CCNA Automation and programmability**

1. With Network Automation, **your network cost will decrease**. Because you can do many network activity automatically and fastly. This will reduce the job complexity ...
2. Unlike SDN, traditional networks use routers, switches and other hardware and physical infrastructure to generate connections and run the networks. SDN controllers use a northbound interface that communicates with APIs, allowing application developers to program the network.
3. Virtualization creates a simulated, or virtual, computing environment as opposed to a physical environment. Virtualization often includes computer-generated versions of hardware, operating systems, storage devices, and more.
4. Client-Server Architecture. RESTful APIs are built with a client-server architecture, meaning that the client sends a request to the server and the server sends back a response. ...

Statelessness. ...

Cacheability. ...

Layered System. ...

Code-On-Demand. ...

Uniform Interface.

1. It describes software and bots that are programmed to emulate and copy human actions to complete repetitive business tasks. RPA software robots can navigate systems, read and enter data, and perform a wide range of rule-based tasks.
2. 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.

1. a powerful network controller and management dashboard that lets you take charge of your network, optimize your Cisco investment, and lower your IT spending.
2. While SD-Access is used to change the architecture of LAN networks, SD-WAN creates next-generation wide area networks with significant automation capabilities instead of MPLS/VPLS

**Module :Ccna – Infrastructure And Wan Wan Tachnolozyies**

1. any type of malicious activity or attack that could potentially cause harm or damage to an organization, its data or its personnel.
2. Protecting an organization from the impact of risk events by using different techniques.
3. an attack meant to shut down a machine or network, making it inaccessible to its intended users.
4. a subclass of denial of service (DoS) attacks.
5. the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system.
6. A social engineering attack is a cybersecurity attack that relies on the psychological manipulation of human behavior to disclose sensitive data, share credentials, grant access to a personal device or otherwise compromise their digital security.
7. a form of cyberattack in which criminals exploiting weak web-based protocols insert themselves between entities in a communication channel to steal data.