सूक्ष्म, लघु एवं मध्यम उद्यम मंत्रालय
DEVELOPMENT COMMISSIONER
MINISTRY OF MICRO, SMALL & MEDIUM ENTERPRISES
MSME TECHNOLOGY CENTRE

MODEL CURRICULUM

Qualification Name:

CISCO CERTIFIED NETWORK ASSOCIATE (CCNA)

Qualification Code: MSME / CCNA/ 73

Version: 2.0

NSQF Level: 4

Model Curriculum Version: 2.0

Submitted By:

MSME TECHNOLOGY CENTRE
O/o DC MSME, Ministry of Micro, Small and Medium Enterprises
Govt. of India
A-Wing, 7th Floor, Nirman Bhawan, Maulana Azad road
New Delhi-110108
Contact No. +91-674-2654700
Email-msmetcab@gmail.com

COURSES / MODULE TEMPLATE

NOS /Module: Introduction to Network

NOS /Module Code: MSME/CCNA/01

Outcomes:-

After completion of course Student should be able to:

- Understand the concept of Networking.
- Knowledge about networking devices.
- Working principle of Network Topologies.
- Understand the function of networking devices and procedure to troubleshoot the common issues.
- Identify various communication Medias and cabling technique.
- Understand the responsibilities of each layers of OSI model.
- Understand the working principle of Transport layer.
- Understand the TCP and UDP protocol
- Setup different network and share the resources.

Theory Hours: 30 **Practical Hours: - 90** **Theory Marks:** **Practical Marks: -100**

Unit No.	Unit Name	Unit Level Outcomes	Contents (Chapters/Topics)	TH & PR Hours	PR Marks
UNIT-I	**Basic networking concept**	After completion of unit Student should be able to – • Understand the concept of Networking. • Understand the advantages of networking. • Working principle of Network Topologies. • Knowledge about OSI Model & various protocols • Identify various communication Medias. • Able to understand crimping & punching technology. • Understand the concept of number system.	Introduction about networking Types of networking LAN,MAN,WAN Network Trends End Device Configuration Protocols and OSI Models Concept of TCP/IP Model Number Systems	**30**	**25**

UNIT-II	**IP Address concept**	After completion of unit Student should be able to – • Configure routers to enable end-to-end connectivity between remote devices. • Understand the responsibilities of each layers of OSI model. • Understand the working principle of Transport layer. • Understand the TCP and UDP protocol. • Calculation of IPV4 Addressing. • Understand the IPV6 Addressing. • Sub netting of IP Address Using FLSM & VLSM for Sub netting.	Introduction of IP Address Public vs private IP Address IPv4 Addressing IPv6 Addressing IP Subnetting(FLSM,VLSM) Internet Control Message Protocols (ICMPs) Ethernet Switching Network Layer Address Resolution	**30**	**25**
UNIT-III	**Basic Router Configuration**	After completion of unit Student should be able to – • Understand about router • Understand the needs and benefits of Router. • Understand the working process of Router • Configuration of Router. • Configuration of IPv4/IPv6 addresses on router. • Assigning Passwords to router. • Perform Telnet function. • Configure routers to enable end-to-end connectivity between remote devices. • Assigning Passwords to router. • Perform Telnet function. • Configure a small network with security best practices. • Troubleshoot connectivity in a small network.	Router and it's booting process TELNET & SSH Basic Router Command and Router Modes Router Port & IP initialization Router Connectivity and Physical Device Security. Transport Layer Application Layer	**30**	**25**
UNIT-IV	**Basic Switch and End Device Configuration**	After completion of unit Student should be able to – • Knowledge about network Switch • Types of switch and its uses. • Configure switches and end devices to provide access to local and remote network resources. • Explain how physical and data link layer protocols support the operation of Ethernet in a switched network.	Configure network switch Basic switch Command and switch Modes Network Security Fundamentals Topology Management & Building Network Architecture. Build a Small Network	**30**	**25**

COURSES / MODULE TEMPLATE

NOS /Module: Switching, Routing, and Wireless Essentials
NOS /Module Code: MSME/CCNA/02

Outcomes:

After completion of course Student should be able to:-

- Configure Router with IPv4 & IPv6 Addressing.
- Configure the VLANs, VTP, SSH and other services in Switch.
- Configure Static and Default Routes.
- Understand the Dynamic Routing Protocols.
- Resetting of password in Routers and Switches.
- Able to Load IOS of Router.
- Understand the concept of DHCP & configure in device.
- Able to configure Ether Channel.
- Configure Wireless Router.
- Identify the different Public Internet Network (DSL, Cable Modems and Wi-max).
- Configuration of Virtual Private Network (VPN).
- Understand the concept and technical detail of Frame Relay switch.
- Tunneling of IPv6 over IPv4 Packets.
- Understand the WAN encapsulation protocols.
- Configure ACLs in the network.

THEORY HOURS: - 30 PRACTICAL HOURS: -120 THEORY MARKS: -NA PRACTICAL MARKS:-100

Unit No.	**Unit Name**	**Unit level outcomes**	**Contents (chapters/topics)**	**TH & PR hours**	**PR Marks**
UNIT-I	Switching Technology & VLAN Management	After completion of unit Student should be able to- • Understand about switching technology. • Able to Configure the network switch • Knowledge about VLAN technology • Able to communicate between different network devices • Explain about inter-VLAN Routing • Able to understand the concept of Spanning Tree Protocol • Configure the ether channel in different switch • Able to Configure DHCP both in IPV4 & IPV6	Introduction about switching technology Basic Device Configuration Switching Concepts VLANs Inter-VLAN Routing Ether Channel DHCPv4 SLAAC and DHCPv6	**50**	**40**
UNIT-II	LAN & Switch Security Configuration	After completion of unit Student should be able to- • Explain how to use endpoint security to mitigate attacks. • Able to configure AAA and 802.1X are used to authenticate LAN endpoints and devices. • Identify Layer 2 vulnerabilities. • Explain how a MAC address table attack	LAN Security Concepts, Switch Security Configuration	**50**	**30**

		compromises LAN security. • Explain how LAN attacks compromise LAN security. • Implement port security to mitigate MAC address table attacks. • Explain how to configure DTP and native VLAN to mitigate VLAN attacks. • Able to configure DHCP attacks. • Explain how to configure ARP inspection to mitigate ARP attacks. • Explain how to configure Port Fast and BPDU Guard to mitigate STP attacks.			
UNIT-III	WLAN Concepts & Routing Configuration	After completion of unit Student should be able to- • Describe WLAN technology and standards. • Knowledge about the components of a WLAN infrastructure. • Explain how wireless technology enables WLAN operation. • Understand how a WLC uses CAPWAP to manage multiple APs. • Describe channel management in a WLAN. • Describe WLAN security mechanisms & threats. • Explain how routers determine the best path. • Explain how routers forward packets to the destination. • Able to configure basic settings on a router. • Describe the structure of a routing table. Static and Dynamic Routing • Describe the command syntax for static routes. • Able to Configure IPv4 and IPv6 static routes. • Explain how a router processes packets when a static route is configured. • Able to manage the Troubleshoot common static and default route configuration issues.	WLAN Concepts & Configuration, Routing Concepts & IP Static Routing , Troubleshoot Static and Default Routes	**50**	**30**

COURSES / MODULE TEMPLATE

NOS /Module: Enterprise Networking, Security, and Automation

NOS /Module Code: MSME/CCNA/03

Outcomes:

After completion of course Student should be able to:-

- Configure single-area OSPFv2 in both point-to-point and multi-access networks.
- Explain how to mitigate threats and enhance network security using access control lists and security best practices. Implement standard IPv4 ACLs to filter traffic and secure administrative access.
- Configure NAT & VPN services on the edge router to provide IPv4 address scalability.
- Explain techniques to provide address scalability and secure remote access for WANs.
- Explain how to optimize, monitor, and troubleshoot scalable network architectures.
- Explain how networking devices implement QoS.
- Implement protocols to manage the network.
- Explain and implement the network technology devices perform such as virtualization, software defined networking (SDN), and automation affect evolving networks.

THEORY HOURS: -30 PRACTICAL HOURS: 90 THEORY MARKS: -NA PRACTICAL MARKS: 100

Unit No.	Unit Name	Unit Level Outcomes	Contents (Chapters/Topics)	PR hours	PR Marks
UNIT -I	**OSPF Concepts & Implement Different Area.**	After completion of unit Student should be able to – • Explain the difference between static routing and dynamic routing protocols • Identify common interior and exterior routing protocols • Describe the benefits of equal-cost multipath routing (ECMP) • Describe route redistribution and route filtering • Explain the main characteristics of link state routing protocols • Explain the messages, adjacency states, and link state advertisements of OSPF • Able to configure OSPF for IPv4 and IPv6 IP Address. • Configure OSPF as required for single area or multi/different area.	Introduction of OSPF Concepts Single-Area OSPFv2 Concepts Single-Area OSPFv2 Configuration	40	30
UNIT - II	**Network Security & Manage ACL, VPN, QoS, WAN**	After completion of unit Student should be able to – • Understand the concept of ACL network security. • Explain how ACLs are used to secure a medium-size Enterprise branch office network. • Configure standard ACLs in a medium-size Enterprise branch office network. • Configure extended ACLs in a medium-size Enterprise branch office network. • Describe the purpose and operation of Virtual	Network Security Concepts ACL Concepts & ACLs for IPv4 Configuration NAT for IPv4 WAN Concepts VPN and IPsec Concepts QoS Concepts Network Management Network Design Network Troubleshooting	40	40

		Private Network (VPN) types. • Identify the business and personal uses of VPNs. • Differentiate between a transport-mode VPN and a tunnel-mode VPN. • Identify the importance of encryption, authentication, and authorization. • Configure a site-to-site Internet Protocol Security (IP Sec) VPN. • Configure a Remote Access VPN. • Identify the components and protocols utilized in a wide area network. • Describe the different OSI model layers and their roles. • Demonstrate how to install and configure a WAN for optimal performance and security. • Explain how to secure network data as well as physically securing a network. • Discuss troubleshooting and support techniques, specific to wide area networks. • Able to manage network troubleshooting & network infrastructure.			
UNIT - III	**Network Virtualization & Automation**	After completion of unit Student should be able to – • Explain the importance of cloud computing & virtualization. • Describe the virtualization of network devices, services & SDN. • Describe controllers used in network programming. • Describe automation • Able to configure management tools & Compare JSON, YAML, and XML data formats. • Able to manage Cisco DNA center enables intent-based networking.	Network Virtualization Network Automation	**40**	**30**

COURSES / MODULE TEMPLATE

NOS /Module: Employability Skill

NOS /Module Code: MSME/ES&E/01

THEORY HOURS: 30 PRACTICAL HOURS: - THEORY MARKS: 100 PRACTICAL MARKS: -

Refer Standard Curriculum developed by NCVET. (https://nqr.gov.in/downloads/pdfs/30-hours_MC_Employability_Skills.pdf)