

# CCNA Training Syllabus 30 Days Module Plan

## 1. Network Fundamentals

What is CCNA?

Why to acquire a CCNA certification?

Types of CCNA certification

Understanding the Need for Networking.

What is a Network?

What is OSI Model?

- Compare and contrast OSI and TCP/IP models
- Compare and contrast TCP and UDP protocols

Types of Network Devices.

- Switch
- Router
- Firewall

Describe the impact of infrastructure components in an enterprise network

## Firewalls

Access points

Wireless controllers

## Topology:

Star

Mesh

Hybrid

Select the appropriate cabling type based on implementation requirements

Types Of cables & Connectivity.

## Apply troubleshooting methodologies to resolve problems

Perform and document fault isolation

Resolve or escalate

Verify and monitor resolution

Configure, verify, and troubleshoot IPv4 addressing and subnetting

Compare and contrast IPv4 address types

- Unicast
- Broadcast
- Multicast
- Describe the need for private IPv4 addressing
- Classes of IPv4
- Subnetting.
- Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment
- Configure, verify, and troubleshoot IPv6 addressing
- Configure and verify IPv6 Stateless Address Auto Configuration
- Compare and contrast IPv6 address types

## 2. LAN Switching Technologies

Describe and verify switching concepts

- MAC learning and aging
  - Frame switching
  - Frame flooding
  - MAC address table
  - Interpret Ethernet frame format
  - Troubleshoot interface and cable issues (collisions, errors, duplex, speed)
  - Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches
1. Access ports (data and voice)
  2. Default VLAN
  3. Configure, verify, and troubleshoot interswitch connectivity
  
  4. Trunk ports
  5. Add and remove VLANs on a trunk
  6. DTP, VTP (v1&v2), and 802.1Q
  7. Native VLAN
  8. Configure, verify, and troubleshoot STP protocols
  
  9. STP mode (PVST+ and RPVST+)
  10. STP root bridge selection
  11. Configure, verify and troubleshoot STP related optional features
  
  12. PortFast
  13. BPDU guard
  14. Configure and verify Layer 2 protocols
  
  15. Cisco Discovery Protocol
  16. LLDP
  17. Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel

## 3. Routing Technologies

Describe the routing concepts

1. Packet handling along the path through a network
2. Forwarding decision based on route lookup
3. Frame rewrite
4. Interpret the components of a routing table
5. Prefix
6. Network mask
7. Next hop
8. Routing protocol code

## **Describe static routing and dynamic routing.**

1. Compare and contrast static routing and dynamic routing
2. Compare and contrast distance vector and link state routing protocols
3. Compare and contrast interior and exterior routing protocols
4. Configure, verify, and troubleshoot IPv4 and IPv6 static routing

### **Describe RIP**

Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

Troubleshoot basic Layer 3 end-to-end connectivity issues

### **Describe EIGRP**

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

### **Describe OSPF**

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

### **PRACTICAL : OSPF**

Describe BGP

Configure, verify, and troubleshoot BGP.

## **4. WAN Technologies**

1. Describe PPP, PPPoE & GRE tunnel.
2. PPP and MLPPP on WAN interfaces using local authentication
3. PPPoE client-side interfaces using local authentication
4. Describe WAN topology options
5. Point-to-point
6. Hub and spoke
7. Full mesh
8. Single vs dual-homed
9. Describe WAN access connectivity options

## **5. Infrastructure Services**

1. Describe DNS lookup operation
2. Troubleshoot client connectivity issues involving DNS
3. Configure and verify DHCP on a router (excluding static reservations)
4. Server, Relay, Client
5. TFTP, DNS, and gateway options
6. Troubleshoot client- and router-based DHCP connectivity issues
7. Configure, verify, and troubleshoot basic HSRP

## Infrastructure Security

1. Configure, verify, and troubleshoot port security
  2. Static
  3. Dynamic
  4. Sticky
  5. Max MAC addresses
  6. Violation actions
  7. Err-disable recovery
  8. Describe common access layer threat mitigation techniques
- Local authentication
  - Secure password
  - Access to device
  - [i] Source address
  - [ii] Telnet/SSH
  - Login banner
  - Describe device security using AAA with TACACS+ and RADIUS

## 7. Infrastructure Management / Device Monitoring Protocols.

### Configure and verify device-monitoring protocols

1. Backup and restore device configuration
  2. Using Cisco Discovery Protocol or LLDP for device discovery
  3. Licensing
  4. Logging
  5. Time zone
  6. Loopback
  7. Configure and verify initial device configuration
  8. Perform device maintenance
- Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)
  - Password recovery and configuration register
  - File system management
  - Use Cisco IOS tools to troubleshoot and resolve problems
  - Ping and traceroute with extended option
  - Terminal monitor
  - Log events
  - Local SPAN
  - Describe network programmability in enterprise network architecture
  - Function of a controller
  - Separation of control plane and data plane

## Real-time statistics on device CPU and Memory Utilization.

Up-to-the-second information on any performance metric of a device.

Real-time traffic/ Bandwidth utilization of an interface/ port.

Network performance monitoring

Factors that impact network performance.

- Availability
- CPU and memory
- Traffic
- Errors and discards
- WAN performance
- Proactive network device monitoring
- Network Uptime Monitor
- Packet Loss Monitoring
- Factors that can cause network packet loss


Packet loss can be caused by any or a combination of the following:

- Network Congestion
- Problems With Network Hardware
- Software Bugs
- Overloaded Devices
- Security Threats
- Faulty Configuration Changes
- Interface Monitoring
- Network Testing Tools
- What are network testing tools?
- Why are network testing tools important?


It is crucial to establish periodic network testing with reliable network testing tools to:

- Understand the network's state
- Ensure the configuration changes work as expected
- Detect crippling network attacks
- Provide a top-notch end-user experience

 What is Network Operations Center (NOC)?

 What is the purpose of a NOC?

 Network Operations Center Monitoring Tools -

 Practical demo on various tools Solar winds, HPSM, ManageEngine, WhatsUp Gold

 Challenges faced by an IT admin

## **Even in a relatively small networking environment:**

Monitor hardware such as servers, routers, switches, firewalls, VMs and storage devices and get real-time information on their status and availability.

1. Temperature
  2. Fan Speed
  3. Power Supply
  4. Processor Clock Speed
  5. Battery
  6. Disk Array
- The Need for FW.
  - FW Characteristics.
  - Types of FW
    - Packet Filtering
    - Stateful Packet Inspection
    - Application Level GW
    - Circuit Level GW

## **Load Balancing**

1. Basic Load Balancing Terminology.
2. Node, Host, Member & Server
3. Pool, Cluster & Farm
4. Virtual Server
5. Load Balancing Basics.
6. Load Balancing Decisions.
7. Load Balance or not to Load Balance.

## **PRACTICAL & Revision DAY**

System and tools requirement

Minimum System Requirements

1. FREE TOOLS Requirement.
2. CCNA Packet Tracer
3. GNS3
4. Cisco IOS
5. HPSM, Manage Engine, Solar wind--- Monitoring Tools.