CCNA – Ağ Uzmanlığı

Öngereksinimler: Bilgisayar Kullanımı

Kurs Tanımı:

CCNA eğitimi ağ yapılarının temellerinin kavranması, giriş seviyede router ve switch konfigürasyonu yapılmasını ve sorun giderimi aşamalarını öğretmeyi hedefler. Eğitim, ICND1, ICND2 kurları olmak üzere iki ayrı kurdan oluşmaktadır. Katılımcılarımız bu kurların sınavlarına ayrı ayrı girebilecekleri gibi eğitim sonunda tek bir sınava da girebilmektedirler.

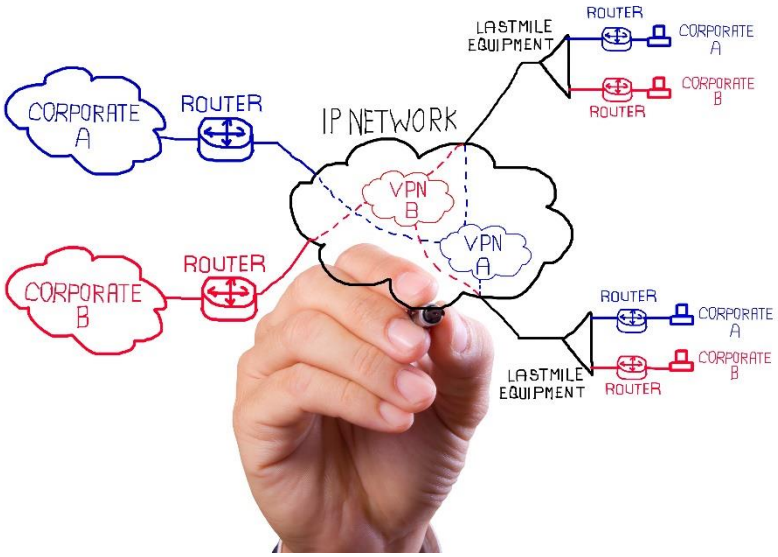
CCNA – Cisco Certified Network Associate (200-120)

ICND-1 – Interconnecting Cisco Network Devices Part 1 (100-101)

- Operation of IP Data Networks
- LAN Switching Technologies
- IP addressing (IPv4 / IPv6)
- IP Routing Technologies
- IP Services
- Network Device Security
- Troubleshooting

ICND-2 – Interconnecting Cisco Network Devices Part 2 (200-101)

- LAN Switching Technologies
- IP Routing Technologies
- IP Services
- Troubleshooting
- WAN Technology



CCNA
Cisco Certified Network Associate
(200-120)

1. **Operation of IP Data Networks**
   - 1.1. Recognize the purpose and functions of various network devices such as Routers, Switches, Bridges and Hubs
   - 1.2. Select the components required to meet a given network specification
   - 1.3. Identify common applications and their impact on the network
   - 1.4. Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models
   - 1.5. Predict the data flow between two hosts across a network
   - 1.6. Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN
2. **LAN Switching Technologies**
   - 2.1. Determine the technology and media access control method for Ethernet networks
   - 2.2. Identify basic switching concepts and the operation of Cisco switches.
     - 2.2.1. Collision Domains
     - 2.2.2. Broadcast Domains
     - 2.2.3. Ways to switch
       - 2.2.3.1. Store
       - 2.2.3.2. Forward
       - 2.2.3.3. Cut through
       - 2.2.3.4. CAM table
   - 2.3. Configure and verify initial switch configuration including remote access management
     - 2.3.1. Hostname
     - 2.3.2. Management IP address
     - 2.3.3. IP default-gateway
     - 2.3.4. Local user and password
     - 2.3.5. Enable secret password
     - 2.3.6. Console and VTY logins
     - 2.3.7. exec-timeout
     - 2.3.8. Service password encryption
     - 2.3.9. copy run start

2.4. Verify network status and switch operation using basic utilities
  2.4.1. Ping
  2.4.2. telnet
  2.4.3. SSH
2.5. Describe how VLANs create logically separate networks and the need for routing between them
  2.5.1. Explain network segmentation and basic traffic management concepts
2.6. Configure and verify VLANs
2.7. Configure and verify trunking on Cisco switches
  2.7.1. DTP (topic)
  2.7.2. Auto-negotiation
2.8. Identify enhanced switching technologies
  2.8.1. RSTP
  2.8.2. PVSTP
  2.8.3. EtherChannels
2.9. Configure and verify PVSTP operation
  2.9.1. Describe root bridge election
  2.9.2. Spanning tree mode

3. IP Addressing (IPv4/IPv6)

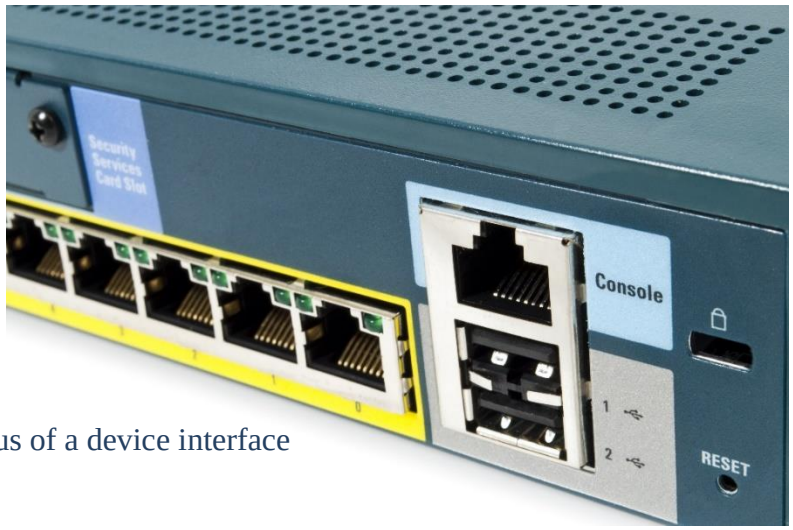
3.1. Describe the operation and necessity of using private and public IP addresses for IPv4 addressing
3.2. Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment
3.3. Identify the appropriate IPv4 addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment
3.4. Describe the technological requirements for running IPv6 in conjunction with IPv4
    3.4.1.1. Dual Stack
3.5. Describe IPv6 addresses
  3.5.1. Global unicast
  3.5.2. Multicast
  3.5.3. Link local
  3.5.4. Unique local
  3.5.5. EUI 64
  3.5.6. Auto-configuration

4. IP Routing Technologies

4.1. Describe basic routing concepts
  4.1.1. Packet forwarding

4.1.2. Router lookup process
4.1.3. Process Switching/Fast Switching/CEF

4.2. Configure and verify utilizing the CLI to set basic router configuration
4.2.1. Hostname
4.2.2. Local user and password
4.2.3. Enable secret password
4.2.4. Console and VTY logins
4.2.5. exec-timeout
4.2.6. Service password encryption
4.2.7. Interface IP Address
4.2.7.1. Loopback
4.2.8. banner
4.2.9. MOTD
4.2.10. copy run start



4.3. Configure and verify operation status of a device interface
4.3.1. Serial
4.3.2. Ethernet

4.4. Verify router configuration and network connectivity using
4.4.1. Ping
4.4.1.1. Extended ping
4.4.2. Traceroute
4.4.3. telnet
4.4.4. SSH
4.4.5. Show cdp neighbors

4.5. Configure and verify routing configuration for a static or default route given specific routing requirements

4.6. Differentiate methods of routing and routing protocols
4.6.1. Static vs. dynamic
4.6.2. Link state vs. distance vector
4.6.3. next hop
4.6.4. IP routing table
4.6.5. Passive Interfaces (how they work)
4.6.6. Administrative distance
4.6.7. split horizon
4.6.8. metric

4.7. Configure and verify OSPF
4.7.1. Benefit of single area

- 4.7.2. Configure OSPv2
- 4.7.3. Configure OSPv3
- 4.7.4. Router ID
- 4.7.5. Passive Interface
- 4.7.6. Discuss multi-area OSPF
- 4.7.7. Understand LSA types and purpose

4.8. Configure and verify interVLAN routing (Router on a stick)

- 4.8.1. Sub interfaces
- 4.8.2. Upstream routing
- 4.8.3. Encapsulation

4.9. Configure SVI interfaces

4.10. Manage Cisco IOS Files

- 4.10.1. Boot Preferences
- 4.10.2. Cisco IOS Images (15)
- 4.10.3. Licensing
  - 4.10.3.1. Show license
  - 4.10.3.2. Change license

4.11. Configure and verify EIGRP (single AS)

- 4.11.1. Feasible Distance/Feasible Successors/Administrative distance
- 4.11.2. Feasibility condition
- 4.11.3. Metric composition
- 4.11.4. Router ID
- 4.11.5. Auto summary
- 4.11.6. Path Selection
- 4.11.7. Load Balancing
  - 4.11.7.1. Unequal
  - 4.11.7.2. Equal

5. IP Services

5.1. Configure and verify DHCP (IOS Router)

- 5.1.1. Configuring router interfaces to use DHCP
- 5.1.2. DHCP options (Basic overview and functionality)
- 5.1.3. Excluded addresses
- 5.1.4. Lease time

5.2. Describe the types, features, and applications of ACLs

- 5.2.1. Standard (editing and sequence numbers)
- 5.2.2. Extended
- 5.2.3. Named

5.2.4. Numbered
5.2.5. Log option
5.3. Configure and verify ACLs in a network environment
5.3.1. Named
5.3.2. Numbered
5.3.3. Log option
5.4. Identify the basic operation of NAT
5.4.1. Purpose
5.4.2. Pool
5.4.3. Static
5.4.4. 1 to 1
5.4.5. Overloading
5.4.6. Source addressing
5.4.7. One-way NAT

5.5. Configure and verify NAT for given network requirements
5.6. Configure and verify NTP as a client
5.7. Recognize High availability (FHRP)
5.7.1. VRRP
5.7.2. HSRP
5.7.3. GLBP
5.8. Configure and verify syslog
5.8.1. Utilize syslog output
5.9. Describe SNMP v2 and v3

6. Network Device Security

6.1. Configure and verify network device security features
6.1.1. Device password security
6.1.2. Enable secret vs enable
6.1.3. Transport
6.1.3.1. Disable telnet
6.1.3.2. SSH
6.1.4. VTYs
6.1.5. Physical security
6.1.6. Service password
6.1.7. Describe external authentication methods
6.2. Configure and verify switch port security
6.2.1. Sticky MAC
6.2.2. MAC address limitation

- 6.2.3. Static/dynamic
- 6.2.4. Violation modes
  - 6.2.4.1. errDisable
  - 6.2.4.2. shutdown
  - 6.2.4.3. protect restrict
- 6.2.5. Shutdown unused ports
- 6.2.6. errDisable recovery
- 6.2.7. Assign unused ports to an unused VLAN
- 6.2.8. Putting native VLAN to other than VLAN 1

6.3. Configure and verify ACLs to filter network traffic

6.4. Configure and verify an ACLs to limit telnet and SSH access to the router

7. Troubleshooting

7.1. Troubleshoot and correct common problems associated with IP addressing and host configurations

7.2. Troubleshoot and resolve VLAN problems

- 7.2.1. Identify that VLANs are configured
- 7.2.2. Verify port membership correct
- 7.2.3. Correct IP address is configured

7.3. Troubleshoot and resolve trunking problems on Cisco switches

- 7.3.1. Verify correct trunk states
- 7.3.2. Verify correct encapsulation id configured
- 7.3.3. Correct VLANs allowed

7.4. Troubleshoot and resolve ACL issues

- 7.4.1. Verify statistics
- 7.4.2. Verify permitted networks
- 7.4.3. Verify direction
  - 7.4.3.1. Interface

7.5. Troubleshoot and resolve Layer 1 problems

- 7.5.1. Framing
- 7.5.2. CRC
- 7.5.3. Runts
- 7.5.4. Giants
- 7.5.5. Dropped packets
- 7.5.6. Late collisions
- 7.5.7. Input/output errors

7.6. Identify and correct common network problems

7.7. Troubleshoot and resolve spanning tree operation issues

7.7.1. Verify root switch
7.7.2. Verify priority
7.7.3. Verify mode is correct
7.7.4. Verify port states

7.8. Troubleshoot and resolve routing issues
7.8.1. Verify routing is enabled (SHIP protocols)
7.8.2. Verify routing table is correct
7.8.3. Verify correct path selection

7.9. Troubleshoot and resolve OSPF problems
7.9.1. Verify neighbor adjacencies
7.9.2. Verify hello and dead timers
7.9.3. Verify OSPF area
7.9.4. Verify interface MTU
7.9.5. Verify network types
7.9.6. Verify neighbor states
7.9.7. Review OSPF topology table

7.10. Troubleshoot and resolve EIGRP problems
7.10.1. Verify neighbor adjacencies
7.10.2. Verify AS number
7.10.3. Verify load balancing
7.10.4. Split horizon

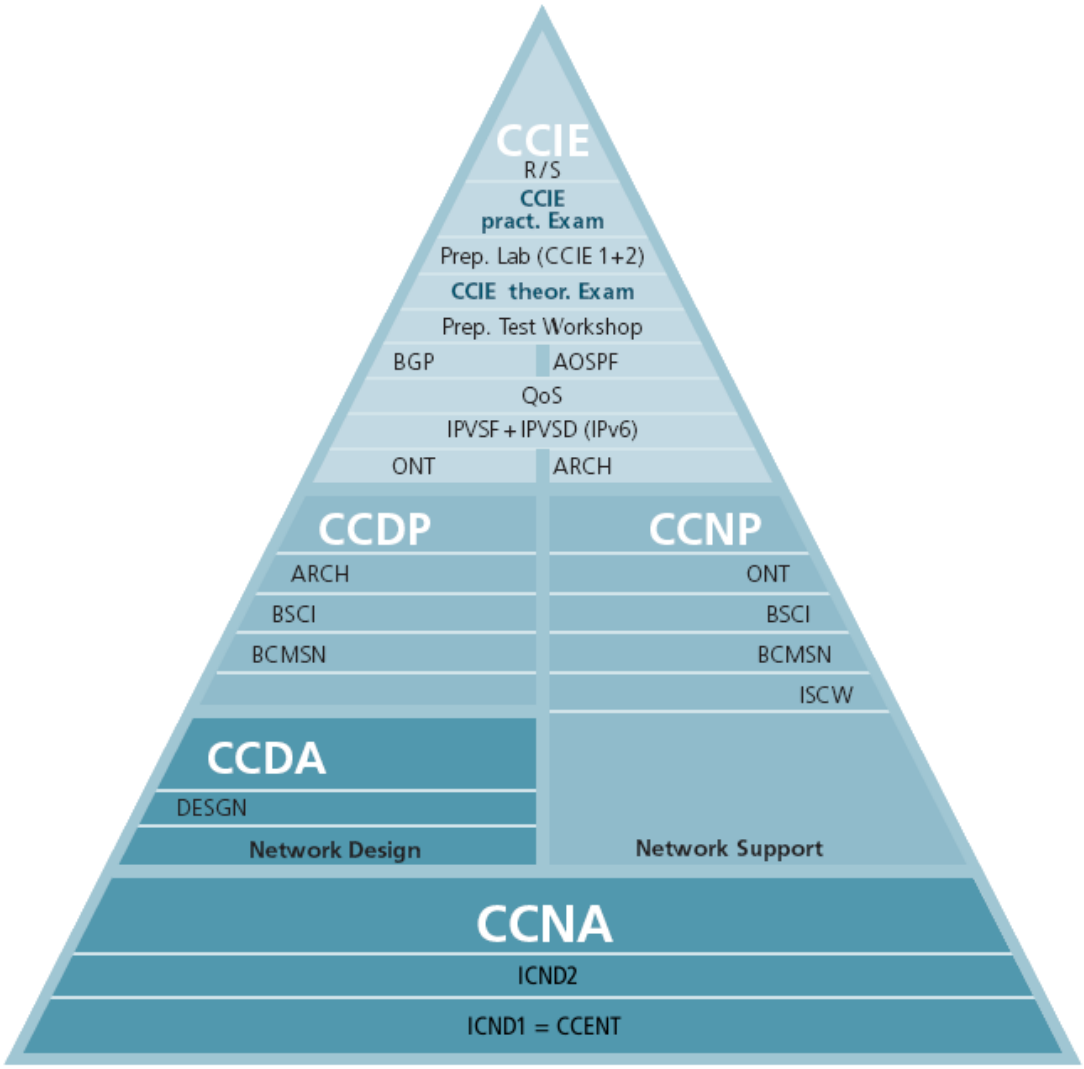
7.11. Troubleshoot and resolve interVLAN routing problems
7.11.1. Verify connectivity
7.11.2. Verify encapsulation
7.11.3. Verify subnet
7.11.4. Verify native VLAN
7.11.5. Port mode trunk status

7.12. Troubleshoot and resolve WAN implementation issues
7.12.1. Serial interfaces
7.12.2. Frame relay
7.12.3. PPP

7.13. Monitor NetFlow statistics
7.14. Troubleshoot EtherChannel problems

8. WAN Technologies

8.1. Identify different WAN Technologies
8.1.1. Metro Ethernet
8.1.2. VSAT

8.1.3. Cellular 3G/4G
8.1.4. MPLS
8.1.5. T1/E1
8.1.6. ISDN
8.1.7. DSL
8.1.8. Frame relay
8.1.9. Cable
8.1.10. VPN

8.2. Configure and verify a basic WAN serial connection
8.3. Configure and verify a PPP connection between Cisco routers
8.4. Configure and verify frame relay on Cisco routers
8.5. Implement and troubleshoot PPPoE