CCNA 200-301 v1.1

MODULE 1 — NETWORK FUNDAMENTALS

Complete Hands-on Training Labs

Topology • Sequential Device Configuration • Verification Output • Troubleshooting

NETWORK GUIDE ACADEMY

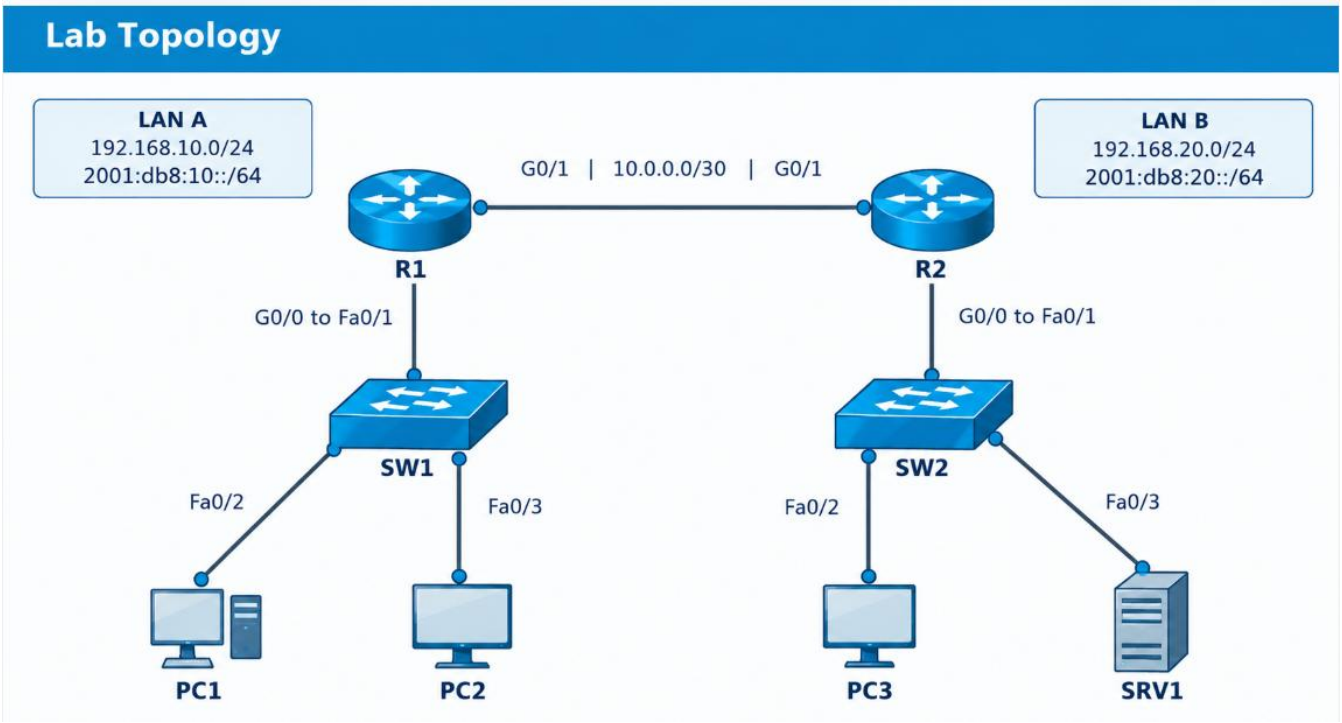
Instructor / Student Lab Guide

Scope: CCNA v1.1 Module 1 — Network Fundamentals objectives 1.1 through 1.7. The labs intentionally use one configuration path per device and then move forward to verification and troubleshooting

Lab sequence

1. Identify network components, physical links and interface health
2. Configure the reference topology, IPv4 addresses and routing
3. Verify IPv4 subnetting, ARP, MAC learning, forwarding and flooding
4. Add IPv6 addressing, types, neighbor discovery and dual-stack tests
5. Observe TCP versus UDP, client IP parameters and application flows
6. Investigate cabling faults and duplex/speed mismatches
7. Wireless, virtualization and architecture observation exercises

Reference topology and equipment



Equipment: two routers (R1/R2), two Layer 2 switches (SW1/SW2), three PCs (PC1–PC3), one server (SRV1), copper Ethernet cables. Use Packet Tracer or equivalent. Routers G0/0 toward LAN and G0/1 toward WAN; switches FastEthernet ports as shown.

Addressing and interface plan

Node	Port / NIC	IPv4 / mask	IPv6 /64 or role
R1	G0/0	192.168.10.1 /24	2001:db8:10::1/64
R1	G0/1	10.0.0.1 /30	2001:db8:12::1/64
R2	G0/0	192.168.20.1 /24	2001:db8:20::1/64
R2	G0/1	10.0.0.2 /30	2001:db8:12::2/64
SW1	VLAN 1	192.168.10.2 /24	management only
SW2	VLAN 1	192.168.20.2 /24	management only

PC1	Fa0	192.168.10.11 /24	2001:db8:10::11/64
PC2	Fa0	192.168.10.12 /24	2001:db8:10::12/64
PC3	Fa0	192.168.20.11 /24	2001:db8:20::11/64
SRV1	Fa0	192.168.20.10 /24	2001:db8:20::10/64

Default gateways: LAN A clients 192.168.10.1 / 2001:db8:10::1; LAN B clients 192.168.20.1 / 2001:db8:20::1. PC and server Ethernet interfaces use static addresses to keep output reproducible.

Lab 1 — Inventory, topology and physical interfaces

CCNA objectives: 1.1, 1.2, 1.3

Objective: Recognize router, Layer 2 switch, hosts/server, LAN/WAN links and cable types.

Connection map: R1 G0/0 ↔ SW1 Fa0/1; SW1 Fa0/2 ↔ PC1; SW1 Fa0/3 ↔ PC2; R1 G0/1 ↔ R2 G0/1; R2 G0/0 ↔ SW2 Fa0/1; SW2 Fa0/2 ↔ PC3; SW2 Fa0/3 ↔ SRV1.

Device discovery commands (read-only; run on each router and switch before configuration):

```
show version
show inventory
show interfaces status          ! switch platforms supporting this syntax
show ip interface brief
show interfaces description
```

VERIFY — Model and interface count match inventory; interface LEDs and link states correspond to each cable.

VERIFY — Router separates IP networks; Layer 2 switch bridges hosts in a LAN; SRV1 provides services; endpoint initiates traffic.

VERIFY — Copper cables connect Ethernet endpoints; recognize that fiber and optics are alternatives depending on range and interface.

Lab 2 — Complete baseline configuration — IPv4 connectivity

CCNA objectives: 1.6, 1.7, 1.10

Objective: Build the topology once with per-device configurations and verified routed reachability.

Step 1 — R1: baseline and IPv4

```
enable
configure terminal
hostname R1
no ip domain-lookup
interface GigabitEthernet0/0
 description LAN-A-to-SW1-Fa0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
exit
interface GigabitEthernet0/1
 description WAN-to-R2-G0/1
 ip address 10.0.0.1 255.255.255.252
 no shutdown
exit
ip route 192.168.20.0 255.255.255.0 10.0.0.2
end
copy running-config startup-config
```

Step 2 — R2: baseline and IPv4

```
enable
configure terminal
hostname R2
no ip domain-lookup
interface GigabitEthernet0/0
 description LAN-B-to-SW2-Fa0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
exit
interface GigabitEthernet0/1
 description WAN-to-R1-G0/1
 ip address 10.0.0.2 255.255.255.252
 no shutdown
exit
ip route 192.168.10.0 255.255.255.0 10.0.0.1
end
copy running-config startup-config
```

Step 3 — SW1: baseline, management and ports

```
enable
configure terminal
hostname SW1
no ip domain-lookup
interface FastEthernet0/1
 description UPLINK-to-R1-G0/0
 switchport mode access
 no shutdown
exit
interface FastEthernet0/2
 description PC1
 switchport mode access
 no shutdown
exit
interface FastEthernet0/3
 description PC2
 switchport mode access
 no shutdown
exit
interface Vlan1
 ip address 192.168.10.2 255.255.255.0
 no shutdown
exit
ip default-gateway 192.168.10.1
end
copy running-config startup-config
```

Step 4 — SW2: baseline, management and ports

```
enable
configure terminal
hostname SW2
no ip domain-lookup
interface FastEthernet0/1
 description UPLINK-to-R2-G0/0
 switchport mode access
 no shutdown
exit
interface FastEthernet0/2
 description PC3
```

```
 switchport mode access
 no shutdown
exit
interface FastEthernet0/3
 description SRV1
 switchport mode access
 no shutdown
exit
interface Vlan1
 ip address 192.168.20.2 255.255.255.0
 no shutdown
exit
ip default-gateway 192.168.20.1
end
copy running-config startup-config
```

Step 5 — PCs and server: host NIC settings

In Packet Tracer: Desktop → IP Configuration (PC) or Config → FastEthernet (server). Set addresses in the plan; add subnet mask 255.255.255.0 and the correct IPv4 gateway. Enable HTTP and DNS on SRV1 using Services where supported. DNS record: www.lab.local → 192.168.20.10 (lab-only name). DNS server on PC1/PC2/PC3: 192.168.20.10.

Step 6 — Verify immediately after configuration

```
R1# show ip interface brief
GigabitEthernet0/0    192.168.10.1    YES manual up     up
GigabitEthernet0/1    10.0.0.1        YES manual up     up

R1# show ip route static
S 192.168.20.0/24 [1/0] via 10.0.0.2

R1# ping 10.0.0.2
Success rate is 100 percent (5/5)

PC1> ping 192.168.20.10
Reply from 192.168.20.10: bytes=32 ...
```

VERIFY — Both interfaces on R1/R2 are up/up and have the correct IP/mask.

VERIFY — Both routers have one static route to the remote LAN (shown as S); connected networks are present as C.

VERIFY — PC1→PC2 succeeds within the LAN; PC1→SRV1 succeeds across R1–R2.

VERIFY — SW1/SW2 VLAN 1 SVI is up only after VLAN 1 has at least one active member port and is operational.

VERIFY — A first ping can time out during ARP resolution; repeat it before troubleshooting.

Lab 3 — IPv4 subnetting, ARP and Layer 2 MAC forwarding

CCNA objectives: 1.6, 1.7, 1.13

Objective: Prove how hosts discover MACs, how switches learn source MACs and how routers separate broadcast domains.

Step 1 — Examine subnets (no new configuration)

192.168.10.0/24: network 192.168.10.0, usable .1–.254, broadcast .255. 192.168.20.0/24: another LAN. 10.0.0.0/30: usable 10.0.0.1 and 10.0.0.2, broadcast 10.0.0.3. All 192.168.x.x and 10.x.x.x examples are RFC 1918 private addressing.

Step 2 — Trigger a frame and observe learning

```
SW1# show mac address-table dynamic
PC1> ping 192.168.10.12
SW1# show mac address-table dynamic
```

```
R1# show ip arp
PC1> arp -a
PC1> ping 192.168.20.10
SW1# show mac address-table dynamic
```

Expected: SW1 learns PC1 source MAC on Fa0/2 and PC2 on Fa0/3; router MAC is learned on Fa0/1. Exact MAC values vary. In simulation mode send a first unknown-unicast or ARP request to inspect flooding: ARP broadcast is flooded to other ports in VLAN 1, while a subsequent known unicast is forwarded on a single learned port.

VERIFY — MAC table maps each learned MAC to the correct physical port and VLAN 1.

VERIFY — ARP maps IPv4 neighbors to Ethernet MAC addresses; remote SRV1 IP is not ARPed directly by PC1 — the default gateway is.

VERIFY — Unknown-destination and broadcast frames can flood within VLAN 1; known unicast uses MAC-table lookup.

VERIFY — The R1–R2 routed link prevents propagation of LAN ARP broadcasts.

VERIFY — Aging: wait for MAC aging or use a carefully scoped clear in an isolated lab; verify relearning after new traffic.

Lab 4 — IPv6 address configuration and neighbor discovery

CCNA objectives: 1.8, 1.9

Objective: Extend the same physical topology to dual-stack IPv6 and demonstrate link-local/global unicast and NDP.

Step 1 — Add IPv6 to R1 only (keep prior IPv4)

```
R1# configure terminal
ipv6 unicast-routing
interface GigabitEthernet0/0
 ipv6 address 2001:DB8:10::1/64
exit
interface GigabitEthernet0/1
 ipv6 address 2001:DB8:12::1/64
exit
ipv6 route 2001:DB8:20::/64 2001:DB8:12::2
end
copy running-config startup-config
```

Step 2 — Add IPv6 to R2 only

```
R2# configure terminal
ipv6 unicast-routing
interface GigabitEthernet0/0
 ipv6 address 2001:DB8:20::1/64
exit
interface GigabitEthernet0/1
 ipv6 address 2001:DB8:12::2/64
exit
ipv6 route 2001:DB8:10::/64 2001:DB8:12::1
end
copy running-config startup-config
```

Step 3 — Configure clients

Assign the static IPv6 addresses in the addressing table to PC1/PC2/PC3/SRV1; set corresponding IPv6 default gateway on each client. On Packet Tracer, use Desktop → IP Configuration → IPv6 Configuration; where router advertisements are enabled, gateways may appear automatically.

Step 4 — IPv6 verification

```
R1# show ipv6 interface brief
R1# show ipv6 route static
R1# show ipv6 neighbors
R1# ping 2001:DB8:12::2
PC1> ping 2001:DB8:20::10
R2# show ipv6 route 2001:DB8:10::/64
```

VERIFY — GUA 2001:db8:... addresses are configured, and each enabled interface also has a fe80:: link-local address.

VERIFY — R1 has an IPv6 static route to LAN B and R2 to LAN A.

VERIFY — IPv6 neighbor table contains link-layer mappings learned via NDP (ICMPv6), not ARP.

VERIFY — 2001:db8::/32 is reserved for documentation; these lab addresses are not routed on the public Internet.

VERIFY — Identify IPv6 multicast ff00::/8, link-local fe80::/10, and unique-local fc00::/7; anycast and EUI-64 are conceptual observation items.

Lab 5 — TCP, UDP, OSI mapping and host IP parameters

CCNA objectives: 1.5, 1.10

Objective: Observe transport differences and validate endpoint addressing and application access.

Step 1 — Enable services on existing SRV1

Packet Tracer SRV1: Services → HTTP → On. Services → DNS → On; add www.lab.local / A / 192.168.20.10. Optionally Services → FTP → On with a test user in the isolated lab. PC1 DNS server must be 192.168.20.10.

Step 2 — Test application flows from PC1

```
PC1> ipconfig /all
PC1> ping 192.168.20.10
PC1> nslookup www.lab.local
PC1> tracert 192.168.20.10
PC1> netstat -an
```

Open PC1 Web Browser → http://www.lab.local or http://192.168.20.10. Use Packet Tracer Simulation Mode: filter DNS, TCP, HTTP and ICMP; run lookup and reload the page. DNS queries commonly use UDP/53, with TCP/53 also possible; HTTP uses TCP/80 in this lab. ICMP is not TCP or UDP. OSI mapping: Ethernet L2, IP L3, TCP/UDP L4, HTTP/DNS L7.

VERIFY — PC1 has the expected IPv4, mask, gateway, DNS, and (after Lab 4) IPv6 address.

VERIFY — DNS resolution returns 192.168.20.10; HTTP connects over TCP following the handshake.

VERIFY — Observe TCP SYN → SYN/ACK → ACK, retransmission/reliability concepts, and contrast connectionless UDP.

VERIFY — Traceroute shows the routed path and may vary across simulated hosts; it is not proof of application success.

Lab 6 — Interface errors, cabling and duplex troubleshooting

CCNA objectives: 1.3, 1.4

Objective: Diagnose physical connectivity and interpret CRC/errors and speed/duplex indicators.

Carry out each fault only on the specified lab link, restore it immediately, and do not make disruptive changes on production devices.

Fault A — shut down SW1 Fa0/2

```
SW1# configure terminal
interface FastEthernet0/2
 shutdown
end
SW1# show interfaces FastEthernet0/2
SW1# show interfaces status

! Recovery
SW1# configure terminal
interface FastEthernet0/2
 no shutdown
end
```

VERIFY — During failure PC1 loses its link and pings fail; after recovery link returns and the ping succeeds.

VERIFY — The interface operational status reflects the administratively shut state.

Fault B — check speed, duplex and counters (read only)

```
SW1# show interfaces FastEthernet0/1
SW1# show interfaces FastEthernet0/2
SW1# show interfaces counters errors
R1# show interfaces GigabitEthernet0/0
```

Expected: normal lab links should negotiate correctly and have no steadily increasing CRC/input errors. A mismatched duplex can cause poor performance and late collisions on half-duplex sides (platform-dependent). Do not force speed/duplex across mismatched interfaces merely to reproduce a fault; emulate it only if the simulator supports it and restore auto-negotiation afterward.

VERIFY — Distinguish administratively down, physical down, and protocol down; detect wrong port or disconnected cable.

VERIFY — Identify input errors, CRC, collisions, drops and negotiation state; counters can be zero on a healthy idle lab.

Lab 7 — Wireless, virtualization and architecture observation

CCNA objectives: 1.1, 1.2, 1.11, 1.12

Objective: Relate foundational architecture and services to the built topology without introducing Module 2 WLAN-controller or switching configurations.

A — Wireless extension (separate optional observation)

Optional: connect a standalone access point by Ethernet to an unused SW1 access port in VLAN 1; configure SSID NGA-LAB, WPA2-PSK/AES and a lab-only passphrase in the AP GUI. Give the wireless client 192.168.10.30/24, gateway 192.168.10.1 and DNS 192.168.20.10. Confirm association, IP settings, PC1 ping and server HTTP. This is an optional extension: hardware/AP GUI settings vary, so no IOS AP CLI is presumed.

VERIFY — Correct SSID, security type, passphrase, client association and IP configuration.

VERIFY — For 2.4 GHz, recognize non-overlapping 20 MHz channels 1/6/11 in common regulatory domains; actual allowed channels depend on locale.

B — Virtualization/VRFs observation (no change to baseline)

In a supported virtual environment, inspect a VM and a container: distinguish their operating-system isolation and network adapter/bridge. On a VRF-capable router, run the following read-only command; VRFs are separate Layer 3 routing tables, not VLANs.

```
show vrf
show ip route
```

VERIFY — Name hypervisor, VM, container and their different isolation models.

VERIFY — Describe a VRF as a separate routing instance; if show vrf lists no tenant VRFs, that is acceptable for the base lab.

C — Topology architectures observation

The reference network is a small routed two-site topology (LAN–WAN–LAN), not a complete two-tier campus, three-tier campus or spine–leaf fabric. Sketch where access/distribution/core tiers would be, where a spine and a leaf would attach, and distinguish on-premises endpoints from cloud-hosted services. No extra device configuration required.

VERIFY — Explain two-tier collapsed core, three-tier, spine–leaf, SOHO, WAN and on-premises/cloud in design terms.

VERIFY — Identify router, L2/L3 switch, NGFW/IPS, AP, WLAN controller, endpoints, servers and PoE as component roles; not all need deployment in this baseline.

Final end-to-end acceptance checklist

Test	Execution point	Pass criterion
IPv4 local subnet	PC1 → 192.168.10.12	Replies from PC2
IPv4 remote subnet	PC1 → 192.168.20.10	Replies from SRV1
WAN IPv4	R1 → 10.0.0.2	Successful ping
Routing	R1/R2 show ip route	Correct connected and static networks
MAC learning	SW1 show mac address-table	PCs and router learned on proper ports
IPv6 routed reachability	PC1 → 2001:db8:20::10	Replies from SRV1
NDP	R1 show ipv6 neighbors	Neighbor entries after traffic
DNS + HTTP	PC1 web browser	Name resolves and home page loads
Interface health	All routers / switches	Ports up/up, no increasing faults
Persistence	All Cisco devices	Startup configuration saved

Troubleshooting workflow

1. Physical: verify power/cable/port LEDs, show interfaces status and show ip interface brief.
2. Addressing: inspect PC NIC IP/mask/gateway; validate router G0/0/G0/1 assignments.
3. Local: ping gateway and same-subnet peer; compare ARP and MAC table with physical port map.
4. Routed: ping 10.0.0.1↔10.0.0.2; check each static route and return path.
5. IPv6: verify ipv6 unicast-routing, each /64, static IPv6 routes and NDP entries.
6. Application: verify SRV1 HTTP/DNS enabled, DNS A record and client DNS settings.
7. Configuration: show running-config interface <name>, then save corrected changes.

Knowledge check and instructor notes

- Why does PC1 ARP for R1 instead of SRV1 when reaching a remote network?
- What does the switch do before and after the destination MAC is learned?
- How many usable IPv4 host addresses exist in /24 and /30 networks?
- Why do both R1 and R2 need a route to the opposite LAN?
- How does IPv6 NDP differ from IPv4 ARP?
- How do DNS over UDP and HTTP over TCP differ?
- Which physical counter would suggest corruption on a copper link?
- How are VLANs, VRFs, containers and virtual machines different?