LAN Network Design

Company Floor Network Setup

Complete Network Analysis Report

Network Type:	Small Business LAN
Devices:	10 total (Router, 2 Switches, 4 PCs, 1 Printer, 1 AP, 2 Wireless)
Address Scheme:	192.168.10.0/24 with subnetting
Date:	February 3, 2026

Network Overview

Network Components:

• 1 Router (with internet access and NAT capability)

• 2 Layer 2 Switches (for network segmentation)

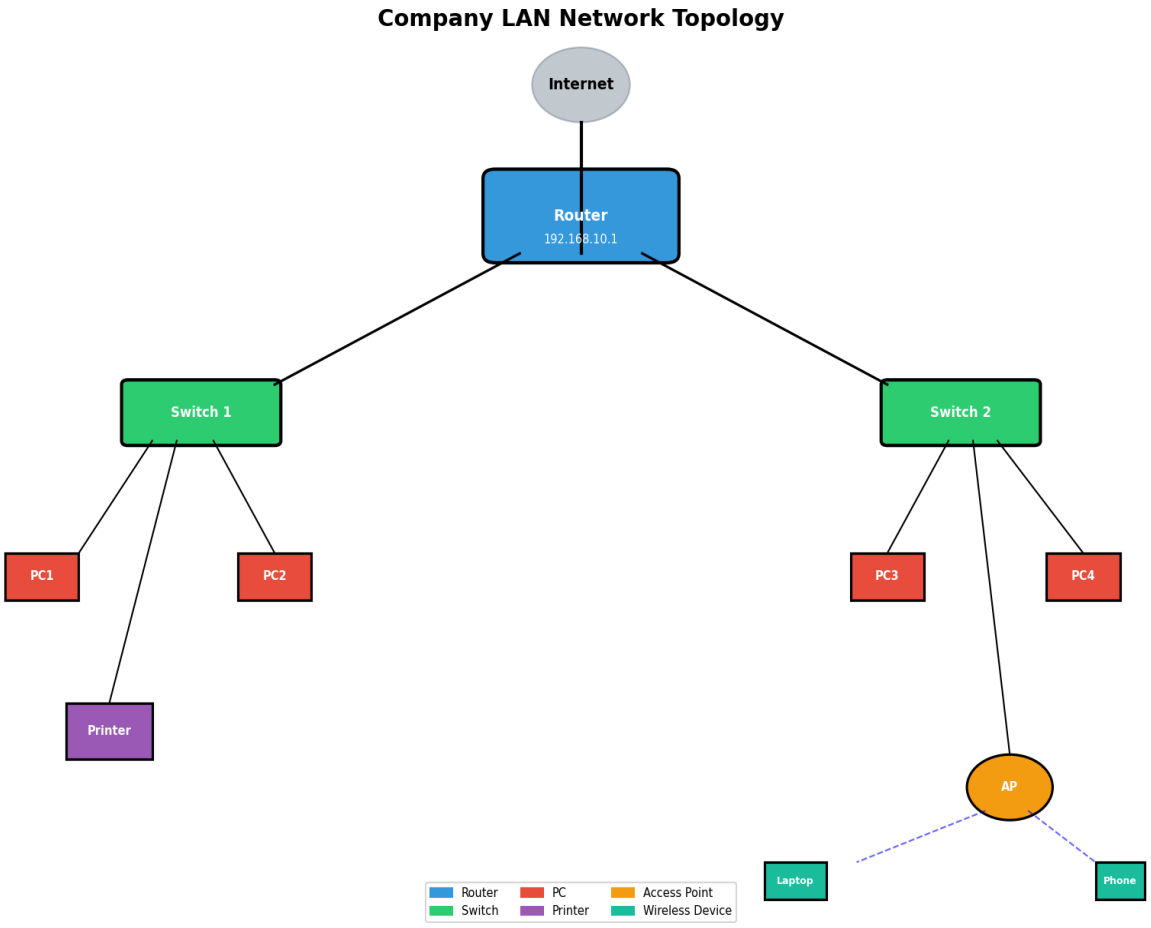
• 4 Employee PCs (wired connections)

• 1 Network Printer (shared resource)

• 1 Wi-Fi Access Point (802.11ac)

• 2 Wireless Devices (laptop and smartphone)

Network Topology Diagram:



Part 1: MAC Addressing & Frame Handling

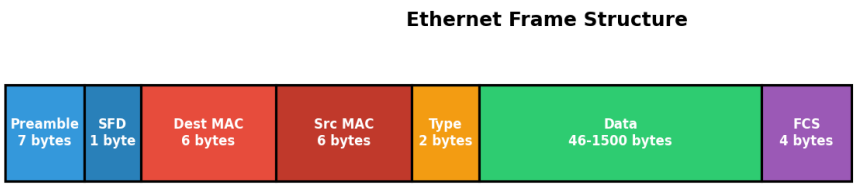
1.1 MAC Address Assignment

Each network interface has a unique 48-bit MAC address (6 bytes, written in hexadecimal):

Device	Interface	MAC Address	Vendor Prefix
Router	LAN Port	00:1A:2B:3C:4D:01	00:1A:2B (Cisco)
Switch 1	Uplink	00:1B:3C:5D:6E:11	00:1B:3C (Dell)
Switch 2	Uplink	00:1B:3C:5D:6E:12	00:1B:3C (Dell)
PC1	NIC	00:50:56:A1:B2:01	00:50:56 (Intel)
PC2	NIC	00:50:56:A1:B2:02	00:50:56 (Intel)
PC3	NIC	00:50:56:A1:B2:03	00:50:56 (Intel)
PC4	NIC	00:50:56:A1:B2:04	00:50:56 (Intel)
Printer	NIC	A4:5E:60:C7:D8:21	A4:5E:60 (HP)
Access Point	Radio	B8:27:EB:F1:A2:33	B8:27:EB (Ubiquiti)
Laptop	Wi-Fi	DC:A6:32:1F:2E:44	DC:A6:32 (Apple)
Smartphone	Wi-Fi	88:66:5A:3B:4C:55	88:66:5A (Samsung)

1.2 Ethernet Frame Structure

When PC1 sends data to the Printer, an Ethernet frame is constructed:



Example Frame: PC1 → Printer

Field	Value	Description
Preamble	10101010... (7 bytes)	Synchronization pattern
SFD	10101011 (1 byte)	Start Frame Delimiter
Dest MAC	A4:5E:60:C7:D8:21	Printer MAC address

Source MAC	00:50:56:A1:B2:01	PC1 MAC address
Type/Length	0x0800 (2 bytes)	IPv4 packet
Data	IP packet + payload	46-1500 bytes of data
FCS	32-bit CRC (4 bytes)	Error detection checksum

1.3 Collision Handling

Ethernet (Wired - CSMA/CD):

Modern switched Ethernet eliminates collisions through:

• **Full-duplex mode:** Separate transmit and receive paths

• **Switching:** Each port is its own collision domain

• **Buffering:** Switches store frames temporarily

Legacy CSMA/CD (half-duplex) would:

1. Listen before transmitting (Carrier Sense)

2. Detect collision if multiple devices transmit simultaneously

3. Stop transmission, send jam signal

4. Wait random backoff time, retry

Wi-Fi (Wireless - CSMA/CA):

Cannot detect collisions, so prevents them:

• **Listen before transmit:** Check if channel is idle

• **RTS/CTS (optional):** Request To Send / Clear To Send handshake

• **ACK frames:** Receiver acknowledges successful reception

• **Exponential backoff:** Random wait time increases with retries

• **IFS (Interframe Spacing):** Mandatory gaps between frames

Part 2: IP Addressing & Subnetting

2.1 Network Address Scheme

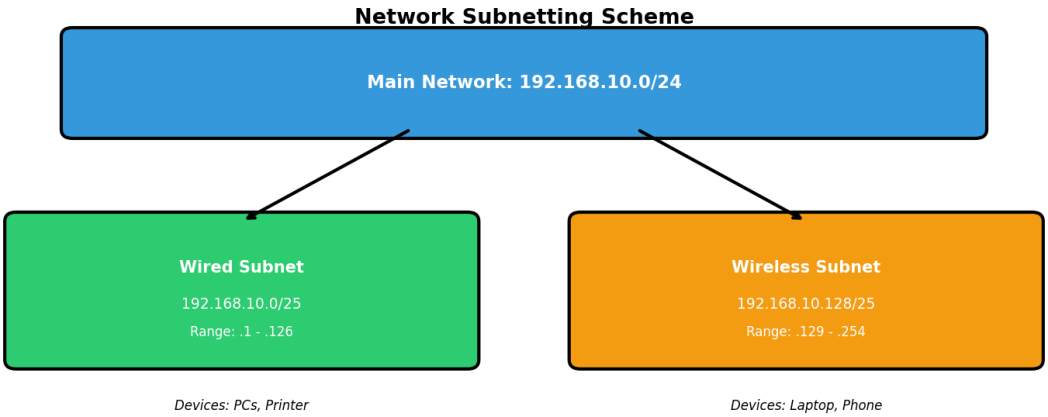
Base Network: 192.168.10.0/24 (Class C private address)

• **Subnet Mask:** 255.255.255.0

• **Available Hosts:** 254 (192.168.10.1 - 192.168.10.254)

2.2 Subnetting Strategy

The network is divided into two subnets for logical separation:



Subnet	Network Address	Subnet Mask	Host Range	Broadcast
Wired	192.168.10.0/25	255.255.255.128	.1 - .126	192.168.10.127
Wireless	192.168.10.128/25	255.255.255.128	.129 - .254	192.168.10.255

2.3 IP Address Assignments

Device	IP Address	Subnet	Default Gateway	Assignment
Router (LAN)	192.168.10.1	Both	N/A (Gateway itself)	Static
PC1	192.168.10.10	Wired	192.168.10.1	DHCP/Static
PC2	192.168.10.11	Wired	192.168.10.1	DHCP/Static
PC3	192.168.10.12	Wired	192.168.10.1	DHCP/Static
PC4	192.168.10.13	Wired	192.168.10.1	DHCP/Static

Printer	192.168.10.20	Wired	192.168.10.1	Static
Access Point	192.168.10.30	Wired	192.168.10.1	Static
Laptop	192.168.10.50	Wireless	192.168.10.1	DHCP
Smartphone	192.168.10.51	Wireless	192.168.10.1	DHCP

2.4 DHCP (Dynamic Host Configuration Protocol)

Role in the Network:

DHCP server (running on the router) automatically assigns IP addresses to devices, eliminating manual configuration.

DHCP Process (DORA):

1. **Discover:** Client broadcasts 'DHCP Discover' to find DHCP server
2. **Offer:** DHCP server responds with an available IP address offer
3. **Request:** Client requests the offered IP address
4. **Acknowledge:** Server confirms and provides IP, subnet mask, gateway, DNS, lease time

Configuration provided by DHCP:

• IP Address (e.g., 192.168.10.50)

• Subnet Mask (255.255.255.0)

• Default Gateway (192.168.10.1)

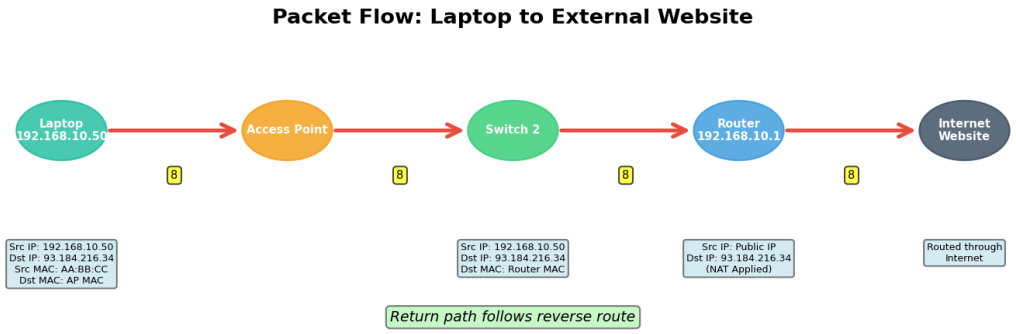
• DNS Server addresses

• Lease time (how long the IP is valid)

Part 3: Routing & Packet Forwarding

3.1 Scenario: Laptop Accessing External Website

When the wireless laptop (192.168.10.50) requests www.example.com (93.184.216.34):



3.2 Detailed Packet Journey

Step 1: Application Layer

• User enters www.example.com in browser

• DNS resolves domain to IP: 93.184.216.34

• HTTP request is prepared

Step 2: Transport Layer

• TCP segment created with:

- Source Port: 52341 (random high port)

- Destination Port: 80 (HTTP) or 443 (HTTPS)

Step 3: Network Layer (IP Packet)

• IP packet header contains:

Field	Value	Purpose

Version	4 (IPv4)	IP protocol version
Source IP	192.168.10.50	Laptop private IP
Dest IP	93.184.216.34	Website public IP
TTL	64	Hop limit (decremented by each router)
Protocol	6 (TCP)	Upper layer protocol
Header Checksum	Calculated	Error detection

Step 4: Data Link Layer (MAC Framing)

• Laptop checks routing table:

- Destination 93.184.216.34 is not on local network

- Must send to default gateway (192.168.10.1)

• ARP resolves gateway IP to MAC address

• Ethernet frame created:

- Source MAC: DC:A6:32:1F:2E:44 (Laptop)

- Dest MAC: 00:1A:2B:3C:4D:01 (Router)

Step 5: Physical Layer

• Wi-Fi radio transmits frame to Access Point

• AP forwards to Switch 2 via Ethernet cable

• Switch 2 forwards to Router based on MAC table

3.3 Router Processing

A. Receiving the Packet:

1. Router strips Ethernet frame (Layer 2)

2. Examines IP header (Layer 3)

3. Checks destination IP: 93.184.216.34

B. Routing Decision (How router decides next hop):

1. **Check Routing Table:**

Destination	Netmask	Gateway	Interface
192.168.10.0	255.255.255.0	0.0.0.0	LAN (eth0)
0.0.0.0	0.0.0.0	ISP Gateway	WAN (eth1)

2. **Longest Prefix Match:** Destination doesn't match 192.168.10.0/24

3. **Default Route:** Matches 0.0.0.0/0 (send to ISP)

4. **Decrements TTL:** Prevents routing loops

5. **Recalculates checksum:** Header modified

C. NAT (Network Address Translation):

Router performs NAT to allow private IPs to access internet:

Direction	Source IP	Source Port	Dest IP	Dest Port
Outbound	192.168.10.50	52341	93.184.216.34	80
After NAT	203.0.113.25	12345	93.184.216.34	80

NAT Table Entry Created:

Router stores: 192.168.10.50:52341 ↔ 203.0.113.25:12345

This mapping allows return traffic to find the laptop

D. Forwarding to Internet:

• New Ethernet frame created for WAN interface

• Source MAC: Router WAN interface

• Dest MAC: ISP gateway MAC (obtained via ARP)

• Packet sent to ISP, then routed through internet to destination

3.4 Return Path

When the website responds:

1. **Internet routing:** Packet reaches router's public IP (203.0.113.25)
2. **NAT lookup:** Router finds mapping: port 12345 → 192.168.10.50:52341
3. **Address translation:** Dest IP changed to 192.168.10.50
4. **Routing decision:** 192.168.10.50 is on LAN subnet
5. **ARP resolution:** Router finds laptop's MAC via ARP cache
6. **Frame forwarding:** Switch forwards to Access Point
7. **Wireless delivery:** AP transmits to laptop
8. **Laptop processes:** Removes headers, delivers data to browser

3.5 Key Routing Concepts

Concept	Description	Purpose
IP Header	Contains source/dest IPs, TTL, protocol	Enables routing between networks
Routing Table	Maps destinations to next hops	Determines packet forwarding path
Longest Prefix Match	Most specific route wins	Accurate routing decisions
Default Route	0.0.0.0/0 catches all unmatched	Internet gateway
TTL	Hop counter, decremented per router	Prevents infinite loops
NAT	Translates private to public IPs	Allows private networks internet access

Summary & Conclusion

Network Design Overview:

This LAN design demonstrates a complete small business network with:

• Proper segmentation via switches

• Logical subnetting for wired and wireless devices

• DHCP for automated configuration

• NAT for internet access with private addressing

• Collision avoidance through modern switching and Wi-Fi protocols

Key Takeaways:

• **Layer 2 (Data Link):** MAC addresses identify devices on local network. Switches use MAC tables for forwarding. Collisions handled by CSMA/CD (wired) and CSMA/CA (wireless).

• **Layer 3 (Network):** IP addresses enable inter-network communication. Routers use routing tables and longest prefix matching. NAT allows private networks to access internet.

• **DHCP:** Simplifies network administration by automatically assigning IP configurations to devices.

• **Packet Journey:** Data traverses multiple layers, with each layer adding/removing headers. Routers make forwarding decisions based on destination IP and routing table.

Network Configuration Summary:

Parameter	Value
Network Address	192.168.10.0/24
Total Devices	10 (4 PCs, 1 Printer, 1 Router, 2 Switches, 1 AP, 2 Wireless)
Subnets	2 (Wired: /25, Wireless: /25)
Gateway	192.168.10.1 (Router)
DHCP Range	192.168.10.50-100 (Wireless), 192.168.10.10-40 (Wired)
Collision Domain	Per switch port (wired), Shared (wireless)
Broadcast Domain	Entire LAN (all devices)
Internet Access	Via NAT on router