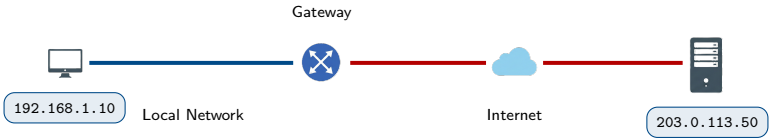
IPv4 and IPv6 Addressing

Intro to Networks Module 4.0

Brendan Shea, PhD

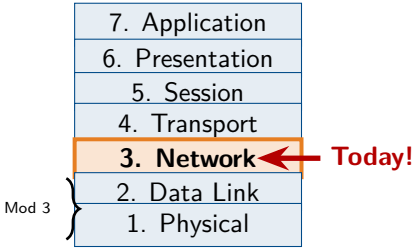
Rochester Community and Technical College
Intro to Networking



Outline I

Review: From Layer 2 to Layer 3

- Module 3 covered **switches** and **MAC addresses** (Layer 2).
- Today's question: How do we communicate *beyond* our local network?
- MAC addresses only work locally—switches don't forward to other networks.
- We need **IP addresses** (Layer 3) to route traffic across networks.



The Key Difference

MAC = local delivery (within your network)
IP = end-to-end delivery (across the internet)

Learning Outcomes I

After completing this module, you will be able to:

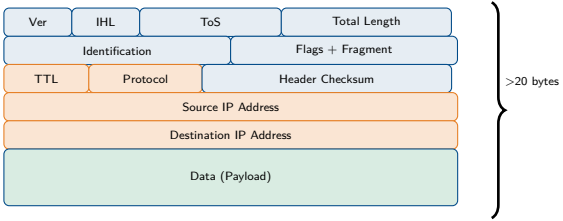
- Explain the role of **Layer 3 (IP) addressing** and how it differs from Layer 2 (MAC) addressing.
- Describe **ARP** (Address Resolution Protocol) and how it maps IP addresses to MAC addresses.
- Interpret **IPv4 addresses** in dotted decimal notation and understand the role of **subnet masks**.
- Calculate network addresses, broadcast addresses, and usable host ranges using **CIDR notation**.
- Apply **VLSM** (Variable Length Subnet Masking) to create subnets of different sizes.
- Identify **private IP ranges** (RFC 1918) and explain **NAT** (Network Address Translation).
- Configure IP addresses, subnet masks, and **default gateways** on network devices.

Learning Outcomes II

- Use troubleshooting tools including **ping**, **arp**, **ipconfig/ifconfig**, and **traceroute**.
- Compare **IPv4** and **IPv6** addressing formats and describe IPv6 adoption strategies.

The IPv4 Datagram Header

- IP wraps data in a **datagram** (like frames at Layer 2).
- Header contains addressing and control information.
- Key fields:
  - **Version**: 4 for IPv4
  - **TTL**: Time to Live (hop limit)
  - **Source IP**: Sender's address
  - **Destination IP**: Receiver's address
  - **Protocol**: What's inside (TCP, UDP)



TTL Prevents Loops

Each router decrements TTL by 1. When TTL reaches 0, the packet is discarded—prevents infinite loops!

Layer 2 vs Layer 3 Addressing

MAC Address (Layer 2)

- Hardware address burned into NIC
- Works only on **local network**
- **Changes** at each router hop
- Example: `00:1A:2B:3C:4D:5E`

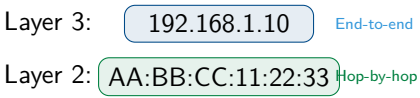
IP Address (Layer 3)

- Logical address assigned by admin
- Works **across networks**
- **Stays the same** end-to-end
- Example: `192.168.1.100`

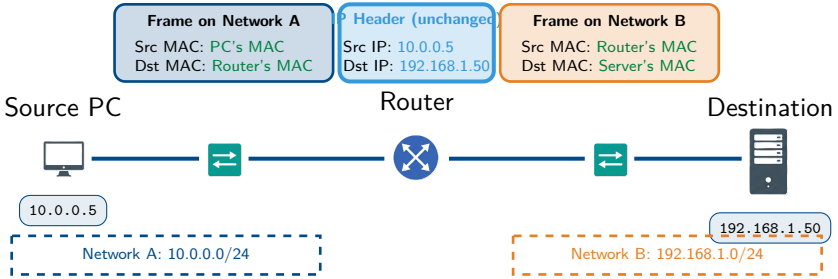
Mailing Analogy

IP address = Full mailing address (123 Main St, Springfield, USA)

MAC address = Apartment number (Apt 4B—only meaningful inside the building)



How Routers Use Both Addresses

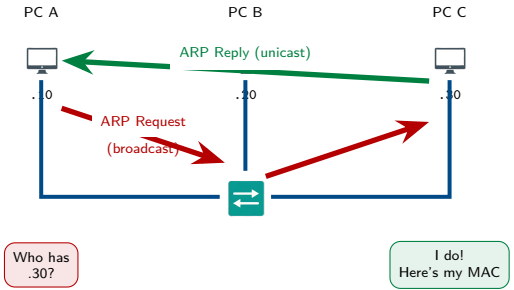


Key Insight

IP addresses stay the same from source to destination. **MAC addresses** change at every hop—the router creates a new frame for each network segment.

Address Resolution Protocol (ARP)

- Problem: You know the **destination IP**, but need the **MAC** to send a frame.
- Solution: **ARP** asks "Who has this IP?"
- ARP Request: Broadcast to all devices—"Who has 192.168.1.50?"
- ARP Reply: Target responds with its MAC address (unicast).
- Result is cached in the **ARP table**.



Security Note

ARP has no authentication. **ARP spoofing** attacks send fake replies to redirect traffic!

ARP Table and Cache

- ARP results are stored in the **ARP cache** (also called ARP table).
- Avoids broadcasting for every single packet.
- Entries expire after a timeout (typically 2–20 minutes).
- View with: `arp -a` (Windows/Linux/Mac)

Common ARP Commands

`arp -a` — Display all entries
`arp -d [IP]` — Delete an entry
`arp -s [IP] [MAC]` — Add static entry

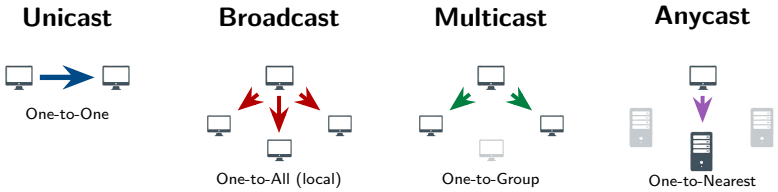
Sample ARP Table Output

IP Address	MAC Address
192.168.1.1	00:1a:2b:3c:4d:01
192.168.1.25	00:1a:2b:3c:4d:25
192.168.1.50	00:1a:2b:3c:4d:50

Troubleshooting Tip

Empty ARP table? No local communication is happening—check Layer 1 and 2 first!

Unicast, Broadcast, Multicast, and Anycast



Common Uses

Unicast: Most traffic (web, email)
Broadcast: ARP, DHCP discovery

Common Uses

Multicast: Video streaming, routing updates
Anycast: DNS, CDNs (find closest server)

Case Study: Homer's Home Network Mystery

▶ Case Study: Homer's Home Network Mystery

Homer Simpson just set up a new PC in his home office. He runs some tests:

- He can ping `127.0.0.1` (loopback) — Success!
- He can ping his own IP `192.168.1.50` — Success!
- He **cannot** ping Marge's laptop `192.168.1.51` — Fails!
- He **cannot** reach the internet — Fails!

Homer runs `arp -a` and sees an **empty ARP table**.

Review Questions

1. What does an empty ARP table suggest about network communication?
2. What Layer 1 or Layer 2 issue might cause this?
3. What should Homer check first?

Case Study Solution: Homer's Home Network Mystery

✓ Solution: Homer's Home Network Mystery

1. Empty ARP table means **no successful local communication**—ARP requests aren't being answered (or sent).
2. Likely Layer 1/2 causes:
   - Ethernet cable unplugged or damaged
   - NIC disabled in operating system
   - Switch port is dead or disabled
   - Wrong VLAN assignment on switch port
3. Homer should check (in order):
   - Cable connection at PC and switch
   - Link lights on NIC and switch port
   - NIC status in Windows (Network Connections)

Key Lesson

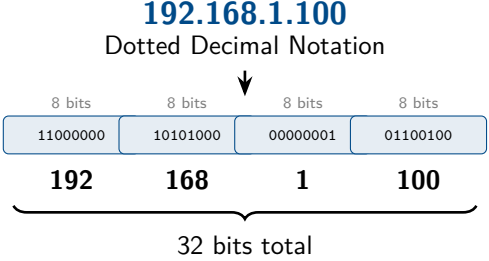
If the ARP table is empty, the problem is almost always **Layer 1 or Layer 2**—not the IP configuration. Check physical connectivity first!

IPv4 Address Format

- IPv4 addresses are **32 bits** long.
- Written as four **octets** in decimal, separated by dots.
- Each octet ranges from **0 to 255**.
- Total possible addresses: about 4.3 billion.
- Not enough for today's internet!

Why 0–255?

Each octet is 8 bits. $2^8 = 256$ possible values (0 through 255).

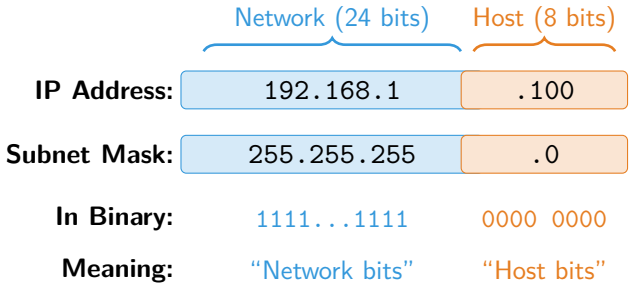


Network Masks Explained

- Every IP address has two parts:
  - **Network portion**: Which network?
  - **Host portion**: Which device?
- The **subnet mask** defines where to split.
- Mask uses **1s** for network bits, **0s** for host bits.

Analogy

Think of a phone number: area code (network) + local number (host).



Subnet Mask Examples

Subnet Mask	CIDR	Total Addresses	Usable Hosts
255.0.0.0	/8	16,777,216	16,777,214
255.255.0.0	/16	65,536	65,534
255.255.255.0	/24	256	254
255.255.255.128	/25	128	126
255.255.255.192	/26	64	62
255.255.255.224	/27	32	30
255.255.255.240	/28	16	14
255.255.255.248	/29	8	6
255.255.255.252	/30	4	2

Why "Usable" Is Less

Two addresses are always reserved:

- **Network address** – all 0s in host portion
- **Broadcast address** – all 1s in host portion

Formula

Usable hosts $= 2^n - 2$

where $n =$ number of host bits

Example: /24 has 8 host bits

$2^8 - 2 = 256 - 2 = 254$ hosts

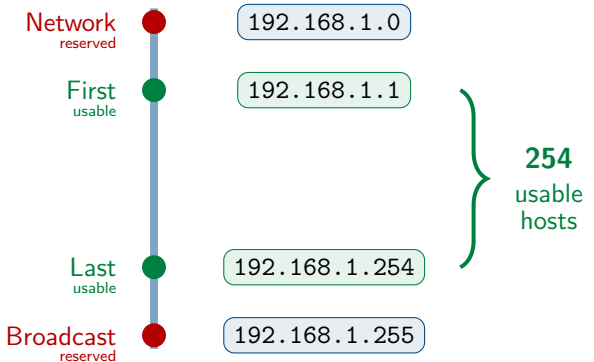
Calculating Host Address Ranges

Given Information

- Network: `192.168.1.0/24`
- Subnet Mask: `255.255.255.0`

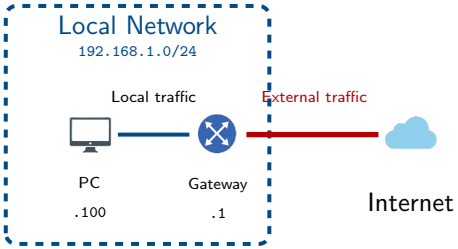
Step-by-Step Calculation

1. **Network Address**:
   `192.168.1.0` – host bits all 0
2. **First Usable Host**:
   `192.168.1.1` – network + 1
3. **Last Usable Host**:
   `192.168.1.254` – broadcast - 1
4. **Broadcast Address**:
   `192.168.1.255` – host bits all 1



Default Gateway

- The **default gateway** is the router that connects your network to other networks.
- If destination IP is NOT on your local subnet → send to the gateway.
- Gateway must be on the **same subnet** as the host.
- Typically the first or last usable address (e.g., `.1` or `.254`).



Common Mistake

If the gateway is on a different subnet than the host, the host cannot reach it—and cannot reach anything outside the local

PC Configuration

IP: `192.168.1.100`
Mask: `255.255.255.0`
Gateway: `192.168.1.1`

Case Study: Moe's Tavern Network Problem

▶ Case Study: Moe's Tavern Network Problem

Moe is setting up a new point-of-sale (POS) system at the tavern to track Duff Beer sales. The system is configured as follows:

Setting	Value
IP Address	`192.168.10.50`
Subnet Mask	`255.255.255.0`
Default Gateway	`192.168.20.1`

Barney's laptop (`192.168.10.25`) can ping the POS system just fine. However, the POS system **cannot** reach the internet or the beer distributor's ordering website.

Review Questions

1. What's wrong with this configuration?
2. Why can Barney reach the POS but the POS can't reach the internet?
3. What should the gateway address be?

Case Study Solution: Moe's Tavern Network Problem

✓ Solution: Moe's Tavern Network Problem

1. The gateway `192.168.20.1` is on a **different subnet** than the POS system (`192.168.10.x`).
2. Why Barney can reach POS but POS can't reach internet:
   - Barney and POS are on the **same subnet**—local traffic doesn't need the gateway
   - Internet traffic requires the gateway, which is **unreachable** (different subnet)
3. Gateway should be on the same subnet, such as `192.168.10.1`.

Key Lesson

The default gateway **must** be on the same subnet as the host. This is one of the most common misconfigurations!

Classful Addressing (Legacy)

- The original IP design divided addresses into **classes** based on the first octet.
- Each class had a fixed network/host boundary—no flexibility!

Class	First Octet	Default Mask	Networks	Hosts/Network
A	1–126	255.0.0.0 (/8)	126	16,777,214
B	128–191	255.255.0.0 (/16)	16,384	65,534
C	192–223	255.255.255.0 (/24)	2,097,152	254
D	224–239	(Multicast—not for hosts)		
E	240–255	(Experimental—reserved)		

The Problem

Very wasteful! A company needing 300 hosts had to get a Class B (65,534 addresses).

The Solution

CIDR (Classless Inter-Domain Routing) replaced classes with flexible prefix lengths.

Public vs Private Addressing

Public IP Addresses

- Routable on the internet
- Must be globally unique
- Assigned by ISPs (from IANA/RIRs)
- Limited supply (IPv4 exhaustion!)

Private IP Addresses

- For internal networks only
- **NOT** routable on internet
- Can be reused by any organization
- Free to use—no registration needed

Private Address Ranges

Range	CIDR
10.0.0.0 – 10.255.255.255	/8
172.16.0.0 – 172.31.255.255	/12
192.168.0.0 – 192.168.255.255	/16

NAT Makes It Work

NAT (Network Address Translation) converts private addresses to public at the router—this is how your home network reaches the internet!

Other Reserved Address Ranges

Address Range	Name	Purpose
127.0.0.0/8	Loopback	Test local TCP/IP stack
169.254.0.0/16	APIPA / Link-Local	Auto-config when DHCP fails
0.0.0.0	"This network"	Default route or unknown
255.255.255.255	Limited Broadcast	Broadcast to local segment

Loopback (127.0.0.1)

- Always refers to "yourself"
- Tests if TCP/IP is working
- Never leaves the device
- Also called `localhost`

APIPA (169.254.x.x)

If you see this address, the device **couldn't get a DHCP address**!

Troubleshoot:

- DHCP server down?
- Network cable unplugged?
- Wrong VLAN?

CIDR: Classless Inter-Domain Routing

- **CIDR** replaced classful addressing in 1993.
- Much more flexible—any prefix length allowed!
- Notation: IP address + slash + prefix length.
- Prefix = number of network bits.

CIDR	Addresses	Usable Hosts
/24	256	254
/25	128	126
/26	64	62
/27	32	30
/28	16	14
/29	8	6
/30	4	2

Reading CIDR Notation

`192.168.1.0/24`

- Network: `192.168.1.0`
- Prefix: 24 bits for network
- Remaining: 8 bits for hosts

Quick Math

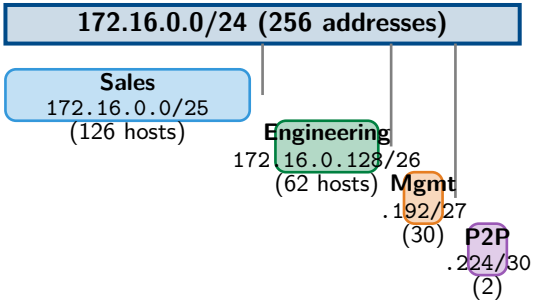
Addresses $= 2^{(32-\text{prefix})}$

Example: /26

$2^{(32-26)} = 2^6 = 64$ addresses

Variable Length Subnet Masks (VLSM)

- **VLSM** allows different subnet sizes within the same network.
- Assign subnets based on actual need—no wasted addresses!
- Always allocate **largest subnets first**.



Example Requirement

Company needs:
→ Sales: 100 hosts
→ Engineering: 50 hosts
→ Management: 25 hosts
→ Point-to-point link: 2 hosts

Result

Used 220 addresses for 177 hosts.
Without VLSM: would need 512+ addresses!

Case Study: Springfield Elementary Network Design

▶ Case Study: Springfield Elementary Network Design

Principal Skinner needs to design the school network with three segments. The district IT department has assigned him `172.16.50.0/24` (256 addresses).

Segment	Devices Needed	Description
Computer Lab	28	Student workstations
Admin Office	12	Staff computers, printers
Teacher's Lounge	6	Laptops, smart TV

Skinner wants to use VLSM to efficiently allocate addresses without waste.

Review Questions

1. What is the smallest subnet size that can fit 28 hosts?
2. List appropriate subnet assignments for each segment.
3. How many addresses will be "wasted" (unused or reserved)?

Case Study Solution: Springfield Elementary Network Design

✓ Solution: Springfield Elementary Network Design

1. 28 hosts needs at least 30 usable addresses → **/27** (32 addresses, 30 usable).
2. Subnet assignments (largest first):

Address Accounting

Used: $32 + 16 + 8 = 56$ addresses
For: $28 + 12 + 6 = 46$ devices
Reserved (net/bcast): 6 addresses
"Wasted": 4 addresses (headroom)

Key Lesson

VLSM lets you right-size subnets. Always assign **largest first**, then work down. Leave room for growth!

ipconfig (Windows)

Common Commands

`ipconfig`
Shows IP, mask, gateway

`ipconfig /all`
Adds MAC, DHCP server, DNS

`ipconfig /release`
Release current DHCP lease

`ipconfig /renew`
Request new DHCP lease

`ipconfig /flushdns`
Clear the DNS cache

Sample Output: ipconfig /all

```
Ethernet adapter Local Area Connection:
Description          Intel Ethernet
Physical Address     00-1A-2B-3C-4D-5E
DHCP Enabled         Yes
IPv4 Address         192.168.1.100
Subnet Mask          255.255.255.0
Default Gateway      192.168.1.1
DHCP Server          192.168.1.1
DNS Servers          8.8.8.8
```

Troubleshooting Tip

See `169.254.x.x`? DHCP failed!
See `0.0.0.0`? No IP assigned at all.

ifconfig and ip (Linux)

Legacy: ifconfig

`ifconfig`
Show all interface configuration

`ifconfig eth0`
Show specific interface

`ifconfig eth0 down`
Disable an interface

`ifconfig eth0 up`
Enable an interface

Modern: ip command

`ip addr` (or `ip a`)
Show IP addresses

`ip link`
Show interface status (up/down)

`ip route`
Show routing table and gateway

`ip neigh`
Show ARP cache (neighbors)

Note

`ifconfig` is deprecated on many modern Linux distributions. Use `ip` instead!

Sample: ip addr

```
2:  eth0:  <UP,BROADCAST>
  inet 192.168.1.50/24
  link/ether 00:1a:2b:3c:4d:5e
```

The arp Command

Common Commands

`arp -a`
Display entire ARP cache

`arp -a 192.168.1.1`
Display entry for specific IP

`arp -d 192.168.1.1`
Delete an entry from cache

`arp -s 192.168.1.1 00-1a-2b-3c-4d-5e`
Add a static entry manually

When to Use

- Verify local connectivity
- Troubleshoot duplicate IPs
- Check for ARP poisoning

Sample Output: arp -a

```
Interface:  192.168.1.100
Internet Addr      Physical Addr         Type
192.168.1.1        00-1a-2b-3c-4d-01     dynamic
192.168.1.25       00-1a-2b-3c-4d-25     dynamic
192.168.1.50       00-1a-2b-3c-4d-50     dynamic
192.168.1.254      00-1a-2b-3c-4d-fe     static
```

Dynamic vs Static

Dynamic: Learned via ARP, expires after timeout

Static: Manually configured, never expires

ping: The Essential Connectivity Test

- `ping` tests reachability using **ICMP** echo request/reply.
- Measures **round-trip time (RTT)** in milliseconds.
- **TTL** in response indicates hops traveled.
- Works on Windows, Linux, Mac.

Common Options

`ping 192.168.1.1`
Basic connectivity test

`ping -t 192.168.1.1`
Continuous ping – Windows

`ping -c 5 192.168.1.1`
Send 5 pings – Linux/Mac

Sample Output

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1:  bytes=32 time=2ms TTL=64
Reply from 192.168.1.1:  bytes=32 time=1ms TTL=64
Reply from 192.168.1.1:  bytes=32 time=1ms TTL=64
Reply from 192.168.1.1:  bytes=32 time=2ms TTL=64
```

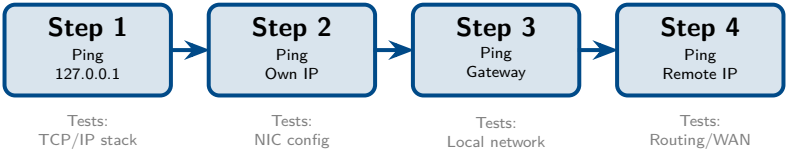
Common Results

Reply – Success! Host is reachable

Request timed out – No response received

Destination unreachable – Routing problem

Ping Troubleshooting Methodology



If Step 1 Fails

TCP/IP stack is broken. Reinstall network drivers or reset TCP/IP stack.

If Step 2 Fails

NIC is not configured properly. Check IP settings, cable, NIC driver.

If Step 3 Fails

Local network issue. Check cable, switch port, gateway address, ARP table.

If Step 4 Fails

Routing or remote issue. Check gateway config, ISP connection, firewall.

Why IPv6? The Problem with IPv4

- IPv4 has only about **4.3 billion** addresses.
- Already exhausted! IANA ran out in 2011.
- Workarounds like NAT and CIDR helped, but add complexity.
- **IPv6** provides a permanent solution.

IPv6 Address Space

$2^{128} = 340$ undecillion addresses

That's 340,282,366,920,938,463,463, 374,607,431,768,211,456 addresses!

IPv6 Benefits

- Virtually unlimited addresses
- Simpler header format
- Built-in IPsec support
- No need for NAT
- Auto-configuration – SLAAC
- Better multicast support

Perspective

IPv6 could assign a unique address to every atom on Earth's surface... and still have addresses left over!

IPv6 Address Format

- **128 bits** long – 4x longer than IPv4.
- Written as 8 groups of 4 hex digits.
- Groups separated by colons.
- Letters can be uppercase or lowercase.

Full Format

2001:0db8:85a3:0000:
0000:8a2e:0370:7334

Simplification Rules

Rule 1: Drop leading zeros in each group

2001:0db8:85a3:0000:0000:8a2e:0370:7334

↓

2001:db8:85a3:0:0:8a2e:370:7334

Rule 2: Replace ONE set of consecutive zero groups with ::

2001:db8:85a3:0:0:8a2e:370:7334

↓

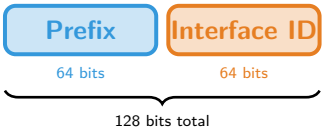
2001:db8:85a3::8a2e:370:7334

Important: Use :: Only Once!

You can only use :: once per address. Using it twice would make the address ambiguous – you wouldn't know how many zero groups each :: represents.

IPv6 Network Prefixes and Address Types

- IPv6 uses **prefix length** instead of subnet mask.
- Written with slash notation: /64
- Standard subnet prefix: **/64**
- First 64 bits = network, last 64 bits = interface ID.



Common IPv6 Address Types

Type	Prefix
Global Unicast	2000::/3
Link-Local	fe80::/10
Unique Local	fc00::/7
Multicast	ff00::/8
Loopback	::1/128
Unspecified	::/128

Example Address

`2001:db8:1234:5678::1/64`

Prefix: 2001:db8:1234:5678
Interface ID: ::1

IPv6 Address Types Explained

Global Unicast – GUA

- Public, routable addresses
- Equivalent to IPv4 public IPs
- Start with 2 or 3
- Assigned by ISPs

Unique Local – fc00::/7

- Private addresses
- Like IPv4 10.x.x.x or 192.168.x.x
- NOT routable on internet
- For internal use only

Link-Local – fe80::

- Auto-configured on every interface
- Only valid on local segment
- NOT routable
- Used for neighbor discovery

Multicast – ff00::/8

- One-to-many communication
- Replaces IPv4 broadcast
- ff02::1 = all nodes
- ff02::2 = all routers

Always Present

Every IPv6 interface has a link-local address, even without DHCP or manual config!

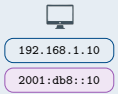
Loopback

::1 is the IPv6 loopback – equivalent to IPv4's 127.0.0.1

IPv4 to IPv6 Transition

Dual Stack

- Run IPv4 AND IPv6 simultaneously
- Most common transition method
- Devices have both addresses
- Gradual migration over time



Tunneling

- Encapsulate IPv6 inside IPv4
- Cross IPv4-only networks
- Types: 6to4, Teredo, ISATAP
- Adds overhead

Translation – NAT64

- Convert between protocols
- IPv6-only hosts reach IPv4 servers
- More complex to manage
- Last resort option

Recommendation

Dual stack is the preferred transition method. Run both protocols until IPv4 can be safely retired. Most modern operating systems support dual stack by default.

Module 4.0 Summary I

Key Concepts:

- **IP (Layer 3)** provides end-to-end addressing; **MAC (Layer 2)** provides local delivery. **ARP** resolves IP to MAC.
- **IPv4 addresses**: 32-bit dotted decimal (e.g., 192.168.1.100). **Subnet mask** divides network and host portions.
- **CIDR notation** (e.g., /24) replaced classful addressing. Usable hosts $= 2^n - 2$ (subtract network and broadcast addresses).
- **VLSM** (Variable Length Subnet Masking) allows subnets of different sizes for efficient IP allocation.
- **Private IP ranges**: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 (RFC 1918). Use **NAT** for internet access.
- Address types: **Unicast** (one-to-one), **Broadcast** (one-to-all on subnet), **Multicast** (one-to-group), **Anycast** (one-to-nearest).

Module 4.0 Summary II

- **Default gateway** must be on the same subnet as the host. **TTL** (Time to Live) prevents routing loops.

Module 4.0 Summary III

Troubleshooting & IPv6:

- Tools: **ipconfig/ifconfig** (view config), **ping** (test connectivity), **arp** (view MAC mappings), **traceroute** (show path).
- Methodology: Ping loopback (127.0.0.1) $\rightarrow$ local gateway $\rightarrow$ remote host to isolate problems.
- **169.254.x.x** = APIPA (DHCP failure). Empty ARP table indicates Layer 1/2 problem.
- **IPv6**: 128-bit addresses in hex notation (e.g., 2001:db8::1). Use :: to compress zeros.
- IPv6 types: **Link-local** (fe80::/10, auto-configured), **Global unicast** (2000::/3), **Unique local** (fc00::/7).
- **Dual stack**: Run IPv4 and IPv6 simultaneously during transition period.