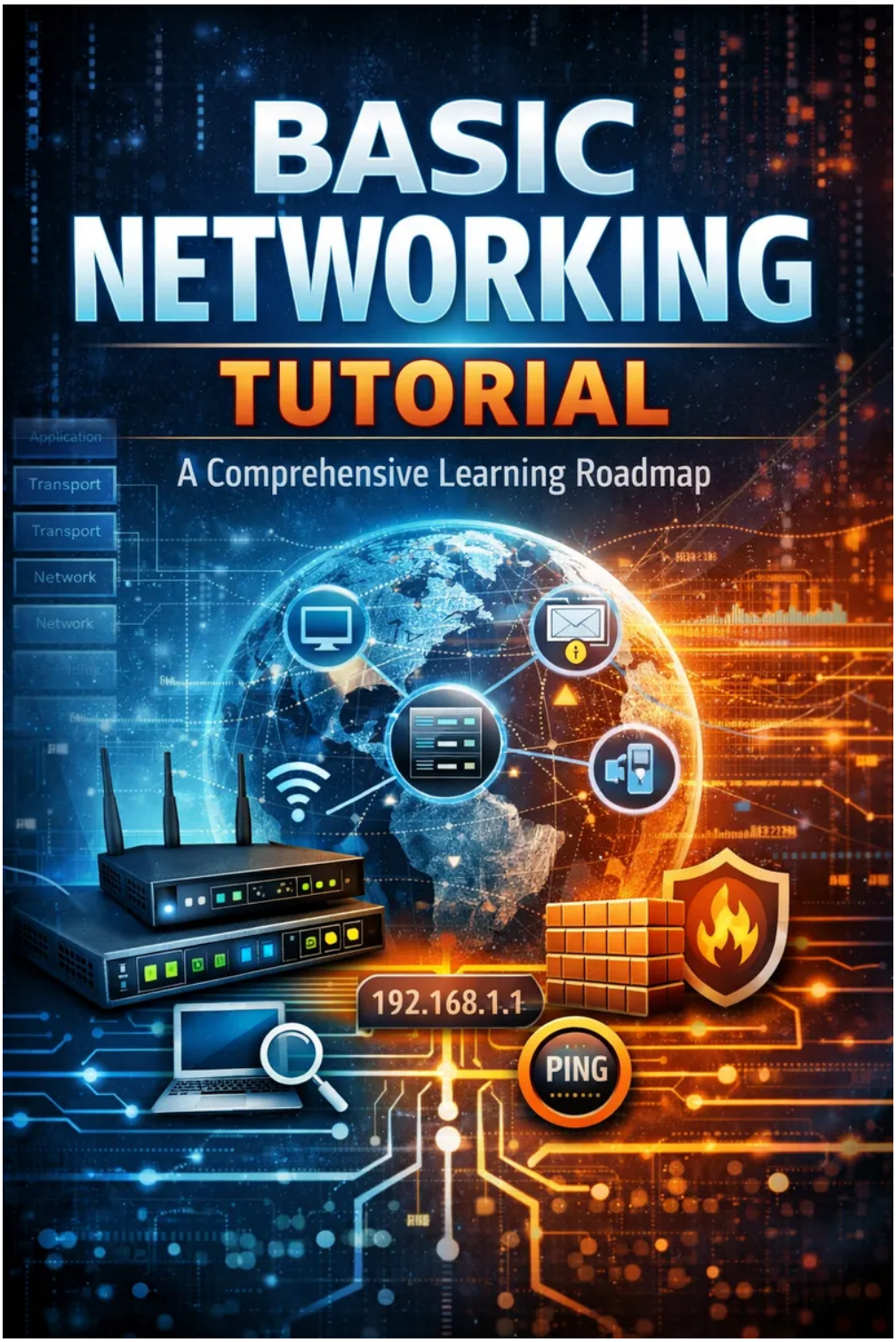
BASIC
NETWORKING
TUTORIAL
A Comprehensive Learning Roadmap
Application
Transport
Transport
Network
Network
192.168.1.1
PING

Basic Networking Tutorial

A Comprehensive Learning Roadmap

From Foundations to Troubleshooting

9 Stages • 50+ Key Concepts • Practical Skills

Basic Networking Tutorial

A Comprehensive Learning Roadmap

Cover Image
Cover Image

From Foundations to Troubleshooting

9 Stages • 50+ Key Concepts • Practical Skills

Networking Learning Roadmap - Table of Contents

Welcome to the Networking Learning Roadmap. This structured curriculum takes you from foundational concepts to practical troubleshooting skills.

Course Overview

Stage	Topic	Description
01	Core Concepts	OSI Model, TCP/IP Model, networking terminology
02	Addressing & Identity	IPv4, IPv6, subnetting, DHCP
03	Name Resolution & Access	DNS, ports, protocols, client-server model
04	Network Devices & Traffic Flow	Switches, routers, LAN vs WAN, NAT
05	Security Fundamentals	Firewalls, threats, best practices

Stage	Topic	Description
06	Troubleshooting Skills	Diagnostic tools and workflow

Appendix

Appendix	Topic
A	Dictionary of Terms
B	Quick Reference Card

How to Use This Roadmap

Recommended Learning Order

1. **Start with Stage 1** - Build your foundation with core concepts
2. **Progress sequentially** - Each stage builds on previous knowledge
3. **Complete each stage** before moving to the next
4. **Practice as you learn** - Use the troubleshooting tools in Stage 6

For Each Stage

- Read the theory and understand the concepts
- Review the tables and examples
- Complete the “Key Takeaways” section
- Move to the next stage when comfortable

Quick Reference

OSI 7 Layers (Bottom to Top)

Please **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

#	Layer
7	Application
6	Presentation

#	Layer
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Common Ports

Port	Service
22	SSH
80	HTTP
443	HTTPS
53	DNS
21	FTP

Troubleshooting Tools

Tool	Purpose
ping	Test connectivity
traceroute	Trace path
ipconfig/ifconfig	View config
nslookup	DNS lookup
netstat	View connections

For questions or corrections, refer to the appendix dictionary or revisit previous stages.

Stage 1: Core Concepts (Foundation)

Goal: Understand how networks are structured and how data moves.

The OSI Model (7 Layers)

The OSI (Open Systems Interconnection) model is a conceptual framework with 7 layers that explains how data moves through a network. Each layer has a specific responsibility.

The 7 Layers (Top to Bottom)

Layer	Name	What it does	Examples
7	Application	User interface, data format	HTTP, DNS, SMTP
6	Presentation	Data translation, encryption	SSL/TLS, JPEG, ASCII
5	Session	Manage connections, auth	NetBIOS, RPC
4	Transport	Reliable delivery, error correction	TCP, UDP
3	Network	Routing, logical addressing	IP, ICMP
2	Data Link	Physical addressing, frames	Ethernet, Wi-Fi
1	Physical	Raw bits on wire/ fiber	Cables, hubs

The 7 Layers (Bottom to Top)

Layer	Name	Mnemonic
1	Physical	Please
2	Data Link	Do
3	Network	Not
4	Transport	Throw
5	Session	Sausage
6	Presentation	Pizza
7	Application	Away

Why the OSI Model Matters

- **Troubleshooting:** Helps pinpoint where network problems occur

- **Vendor neutrality:** Common language for discussing networking
- **Understanding protocols:** Shows how different technologies fit together
- **Design:** Guides network architecture decisions

The TCP/IP Model (Real-World Standard)

While the OSI model is conceptual, the TCP/IP model is the actual protocol suite used on the internet. It has 4 layers:

TCP/IP Layers

Layer	OSI Layers	Protocols
Application	5, 6, 7	HTTP, DNS, FTP, SSH
Transport	4	TCP, UDP
Internet	3	IP, ICMP, ARP
Network Access	1, 2	Ethernet, Wi-Fi

Key Difference from OSI

- TCP/IP is practical and actually used
- OSI is a teaching framework
- TCP/IP combines some OSI layers for simplicity

How Data Flows

When you visit a website:

1. **Application:** Your browser sends an HTTP request
2. **Transport:** TCP breaks it into segments, adds port numbers
3. **Internet:** IP adds source/destination IP addresses
4. **Network Access:** Data is sent as frames over physical media

---

Basic Networking Terminology

Packets

The fundamental unit of data transmitted over a network. Contains: - **Header:** Source/destination info, protocol details - **Payload:** The actual data being sent - **Trailer:** Error-checking information

Frames

Packets wrapped with additional layer 2 (Data Link) information for local network delivery.

Bandwidth

The maximum amount of data that can be transmitted over a network connection in a given time. Measured in: - bps (bits per second) - Kbps (kilobits) - Mbps (megabits) - Gbps (gigabits)

Latency

The time it takes for data to travel from source to destination. Measured in milliseconds (ms). Factors affecting latency: - Physical distance - Network congestion - Number of routers/hops - Processing delays

Throughput

The actual amount of data successfully transferred over a network. Often lower than bandwidth due to: - Network congestion - Protocol overhead - Latency

Key Takeaways

- **Bandwidth** = capacity (pipe width)
- **Throughput** = actual flow (water in pipe)
- **Latency** = travel time (how long water takes)

Key Takeaways

1. The **OSI model** has 7 layers, each with specific responsibilities

2. The **TCP/IP model** is the real-world standard with 4 layers
3. Understanding layers helps with **troubleshooting** and **design**
4. **Packets** are the basic unit of network communication
5. **Bandwidth** is capacity, **latency** is delay, **throughput** is actual speed
6. Data flows down the OSI stack on send, up on receive

Exercises

Review Questions

1. List all 7 OSI layers in order (bottom to top).
2. Which layer handles routing? Which layer handles MAC addresses?
3. What is the difference between bandwidth and throughput?
4. Explain why TCP/IP is used more than OSI in practice.

Hands-On Practice

1. **Identify protocols:** Look at your browser's developer tools (Network tab) and identify which layer each visible protocol operates at (HTTP, TCP, IP, TLS).
2. **Calculate throughput:** Download a file and note the download speed. Compare it to your advertised internet bandwidth.
3. **Trace data flow:** Describe what happens when you visit a website - which layers are involved at each step?

Answers

1. Physical → Data Link → Network → Transport → Session → Presentation → Application (or use the mnemonic: Please Do Not Throw Sausage Pizza Away)
2. Network layer (Layer 3) handles routing; Data Link layer (Layer 2) handles MAC addresses
3. Bandwidth is the maximum capacity; throughput is the actual data transferred
4. TCP/IP is the actual internet protocol suite, while OSI is a conceptual teaching model

---

Next Steps

Proceed to Stage 2: Addressing & Identity on Networks to learn how devices are identified on a network.

Stage 2: Addressing & Identity on Networks

Goal: Understand how devices are identified and located on a network.

IPv4 Addressing

IPv4 (Internet Protocol version 4) is the most common addressing scheme. Each device gets a unique 32-bit address, written as four decimal numbers (0-255) separated by dots.

Format

`xxx.xxx.xxx.xxx`

Example: `192.168.1.1`

IPv4 Address Classes

Class	Range	Default Subnet Mask	Use
A	1.0.0.0 - 126.255.255.255	255.0.0.0	Large networks
B	128.0.0.0 - 191.255.255.255	255.255.0.0	Medium networks
C	192.0.0.0 - 223.255.255.255	255.255.255.0	Small networks
D	224.0.0.0 - 239.255.255.255	N/A	Multicast
E	240.0.0.0 - 255.255.255.255	N/A	Reserved

Private vs Public IPv4 Addresses

Private IPs - Not routed on the internet, used internally:

- `10.0.0.0 - 10.255.255.255` (Class A)
- `172.16.0.0 - 172.31.255.255` (Class B)
- `192.168.0.0 - 192.168.255.255` (Class C)

Public IPs - Routed on the internet, assigned by ISP

Special IP Addresses

Address	Purpose
`0.0.0.0`	"This network" or default route
`127.0.0.1`	Localhost (loopback)
`255.255.255.255`	Broadcast address

IPv6 Basics

IPv6 (Internet Protocol version 6) was created because IPv4 ran out of available addresses. IPv6 uses 128-bit addresses.

Format

`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`

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

IPv6 Advantages

- **Vast address space:** 340 undecillion addresses
- **Simplified header:** More efficient routing
- **Built-in security:** IPsec support
- **No NAT needed:** Every device can have a unique global IP

IPv6 Address Types

Type	Description
Global Unicast	Publicly routable (like public IPv4)
Unique Local	Private (like private IPv4)

Type	Description
Link-Local	Auto-assigned, only works on local network
Multicast	Group communication (replaces broadcast)
Loopback	`::1` (like 127.0.0.1)

IPv4 vs IPv6 Comparison

Aspect	IPv4	IPv6
Address length	32 bits	128 bits
Address format	Dotted decimal	Hex groups
Max addresses	~4.3 billion	~340 undecillion
NAT	Often needed	Not needed
Security	Optional	Built-in

Subnetting Fundamentals

Subnetting splits a large network into smaller subnetworks (subnets) for better organization, performance, and security.

Why Subnet?

1. **Performance:** Reduces broadcast domain size
2. **Security:** Isolates sensitive network segments
3. **Organization:** Groups devices by department/location
4. **Address efficiency:** Allocates addresses precisely

Subnet Mask

A subnet mask determines which part of an IP address is the network portion vs. host portion.

CIDR	Subnet Mask	Hosts
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14

CIDR	Subnet Mask	Hosts
/30	255.255.255.252	2

Common Subnets

- **/24** (256 addresses) = typical home network
- **/16** (65,536 addresses) = Class B network
- **/8** (16.7 million addresses) = Class A network

Subnet Example

Network: `192.168.1.0/24`

- Network address: `192.168.1.0`
- Usable hosts: `192.168.1.1` - `192.168.1.254`
- Broadcast address: `192.168.1.255`

DHCP (Dynamic Host Configuration Protocol)

DHCP automatically assigns IP addresses and network settings to devices, so they can join a network without manual configuration.

How DHCP Works (DORA Process)

1. **Discover** - Client broadcasts “Is there a DHCP server?”
2. **Offer** - DHCP server responds with available IP
3. **Request** - Client requests to use the offered IP
4. **Acknowledge** - Server confirms and provides lease

DHCP Lease

- IP addresses are “leased” for a period (typically 24 hours)
- Lease renewal happens automatically
- When lease expires, IP returns to the pool

What DHCP Assigns

- IP address
- Subnet mask

- Default gateway
- DNS server addresses
- Other optional settings

Benefits of DHCP

- **Automatic:** No manual IP configuration needed
- **Centralized:** Manage addresses from one server
- **Efficient:** Reuses addresses, prevents conflicts
- **Scalable:** Easy to add new devices

Key Takeaways

1. **IPv4** uses 32-bit addresses (e.g., 192.168.1.1)
2. **Private IPs** are for internal networks; **public IPs** are internet-routable
3. **IPv6** provides a virtually unlimited address space
4. **Subnetting** divides networks for performance and security
5. **DHCP** automates IP assignment using the DORA process

Exercises

Review Questions

1. What is the difference between a public and private IP address?
2. How many hosts can a /24 network have? How about a /16?
3. Explain the DORA process in DHCP.
4. Why was IPv6 created?

Hands-On Practice

1. **Check your IP:** Run `ipconfig` (Windows) or `ip addr show` (Linux/Mac) and identify your IP address, subnet mask, and gateway.
2. **Identify IP class:** Determine the class of these IPs: 10.0.1.5, 172.16.0.1, 192.168.1.1, 8.8.8.8
3. **Calculate subnets:** How many usable hosts in a /26 network?
4. **Check DHCP:** Release and renew your IP with `ipconfig /release` and `ipconfig /renew`

Answers

1. Public IPs are routable on the internet; private IPs are used internally and NAT is needed to communicate externally
2. /24 has 254 hosts; /16 has 65,534 hosts
3. DORA: Discover (client broadcasts), Offer (server offers IP), Request (client requests), Acknowledge (server confirms)
4. IPv6 was created because IPv4 ran out of available addresses

---

Next Steps

Proceed to Stage 3: Name Resolution & Access to learn how domain names connect to IP addresses.

Stage 3: Name Resolution & Access

Goal: Understand how humans and devices connect to services.

DNS (Domain Name System)

DNS is like the phonebook of the internet. It translates human-friendly domain names (like google.com) into IP addresses that computers use.

How DNS Works

When you type “example.com” in your browser:

1. **Browser check:** Checks cache for IP
2. **Operating system:** Queries local DNS resolver
3. **Recursive resolver:** Asks root DNS server
4. **Root server:** Points to .com TLD server
5. **TLD server:** Points to authoritative server
6. **Authoritative server:** Returns the IP address

DNS Record Types

Record	Purpose	Example
A	Maps domain to IPv4	example.com → 93.184.216.34
AAAA	Maps domain to IPv6	example.com → 2606:2800:220:1
CNAME	Alias to another domain	blog.example.com → example.com
MX	Mail server	example.com → mail.example.com
TXT	Text information	SPF, DKIM records
NS	Name server	example.com → ns1.example.com

DNS Hierarchy

```
Root (.)
  → TLD (.com, .org, .net)
    → Authoritative (example.com)
      → Records (A, MX, CNAME, etc.)
```

Why DNS Matters

- **User-friendly:** People remember names, not numbers
- **Flexibility:** Change server IPs without changing domain
- **Load balancing:** Distribute traffic across servers
- **Email delivery:** MX records route emails

Common Ports and Protocols

Ports are numbered endpoints that identify specific services on a device. Protocols define how data is transmitted.

Well-Known Ports (0-1023)

Port	Protocol	Service	Use
20	TCP	FTP Data	File transfer (data)
21	TCP	FTP Control	File transfer (commands)
22	TCP	SSH	Secure remote access
23	TCP	Telnet	Unsecure remote access

Port	Protocol	Service	Use
25	TCP	SMTP	Email sending
53	UDP/TCP	DNS	Name resolution
80	TCP	HTTP	Web browsing (unencrypted)
110	TCP	POP3	Email retrieval
143	TCP	IMAP	Email retrieval (advanced)
443	TCP	HTTPS	Secure web browsing
3306	TCP	MySQL	Database
3389	TCP	RDP	Remote desktop
5432	TCP	PostgreSQL	Database

Protocol Categories

Web Protocols: - **HTTP:** Unencrypted web traffic - **HTTPS:** Encrypted web traffic (TLS/SSL)

File Transfer: - **FTP:** File transfer (unencrypted) - **SFTP:** Secure file transfer (SSH-based) - **SCP:** Secure copy

Email: - **SMTP:** Send email between servers - **POP3:** Download email to local client - **IMAP:** Sync email across devices

Remote Access: - **SSH:** Secure command-line access - **Telnet:** Legacy remote access (unsecure) - **RDP:** Windows remote desktop

---

Client-Server Communication Model

Most network communication follows the client-server model, where one device (client) requests services from another (server).

How It Works

1. **Client initiates:** Client opens a connection to server
2. **Server listens:** Server waits for requests on a specific port
3. **Request:** Client sends a request (e.g., “give me this webpage”)
4. **Processing:** Server processes the request
5. **Response:** Server sends back the requested data
6. **Connection closes:** Communication ends

Client Examples

- Web browser (Chrome, Firefox)
- Email client (Outlook, Thunderbird)
- FTP client (FileZilla)
- Database client

Server Examples

- Web server (Apache, Nginx)
- Database server (MySQL, PostgreSQL)
- File server
- Email server

Connection Process (TCP)

1. **SYN:** Client sends synchronization request
2. **SYN-ACK:** Server acknowledges and synchronizes
3. **ACK:** Client acknowledges
4. **Data transfer:** Communication begins
5. **FIN:** Connection closes

HTTP Request Methods

Method	Purpose
GET	Retrieve data
POST	Send data to create
PUT	Update/replace data
DELETE	Remove data
PATCH	Partial update

HTTP Response Codes

Code	Meaning
200	Success
301	Moved permanently
400	Bad request
401	Unauthorized
403	Forbidden

Code	Meaning
404	Not found
500	Server error

Key Takeaways

1. **DNS** translates domain names to IP addresses
2. **Ports** identify specific services on a device (0-65535)
3. **Well-known ports** (0-1023) are reserved for common services
4. **HTTP** is unencrypted; **HTTPS** is encrypted with TLS
5. **Client-server model** is the foundation of most network services
6. **HTTP methods** (GET, POST, PUT, DELETE) define actions

Exercises

Review Questions

1. What does DNS do? Describe the lookup process.
2. What is the difference between TCP and UDP?
3. List three well-known ports and their services.
4. What happens during a TCP 3-way handshake?

Hands-On Practice

1. **DNS lookup:** Use `nslookup example.com` to find the IP address. Try different domain types (.org, .net).
2. **Port scanning (your own):** Use `netstat -an` to see open ports on your machine.
3. **HTTP request:** Use `curl -v https://example.com` and examine the headers.
4. **Check protocols:** Visit a website and identify which port the browser connects to.

Answers

1. DNS translates domain names to IP addresses through a hierarchical lookup process (recursive resolver → root → TLD → authoritative)

2. TCP is connection-oriented and reliable; UDP is connectionless and faster but unreliable
3. 80 (HTTP), 443 (HTTPS), 22 (SSH), 21 (FTP), 25 (SMTP)
4. SYN → SYN-ACK → ACK (three-way handshake establishes connection)

Next Steps

Proceed to Stage 4: Network Devices & Traffic Flow to learn how data moves between networks.

Stage 4: Network Devices & Traffic Flow

Goal: Understand hardware devices and how traffic is directed between networks.

Switches vs Routers

Both are essential networking devices, but they operate at different layers and serve different purposes.

Network Switch (Layer 2)

A **switch** connects devices within the same network (LAN). It uses MAC addresses to forward data to the correct device.

Key characteristics: - Operates at Data Link Layer (Layer 2) - Connects computers, printers, servers in a building - Creates a local network (LAN) - Uses MAC addresses, not IP addresses - Learns which MAC addresses are on each port - Reduces collisions and improves performance - “Intelligent” switching (remembers device locations)

Network Router (Layer 3)

A **router** connects different networks together. It uses IP addresses to determine the best path for data.

Key characteristics: - Operates at Network Layer (Layer 3) - Connects LAN to WAN (internet) - Routes traffic between networks - Uses IP addresses for decision-making - Makes forwarding decisions based on routing tables - Gateway to the internet - Often includes DHCP, NAT, firewall features

Switch vs Router Comparison

Feature	Switch	Router
Layer	2 (Data Link)	3 (Network)
Address used	MAC address	IP address
Purpose	Connect devices in LAN	Connect different networks
Broadcast handling	Forwards broadcasts	Blocks broadcasts
Speed	Very fast (wire-speed)	Slower (more processing)
Typical use	Building internal network	Network-to-network connection

Real-World Example

```
[Computer 1]----[Switch]----[Router]----[Internet]
      |                    |
[Computer 2]----+           |
                          |
[Computer 3]----[Switch]--+
```

- **Switch** connects computers 1, 2, 3 together (LAN)
- **Router** connects this LAN to the internet (WAN)

LAN vs WAN

LAN (Local Area Network)

A network confined to a small geographic area, like a home, office, or building.

Characteristics: - High speed (100 Mbps - 10 Gbps) - Limited distance (up to a few hundred meters) - Owned/controlled by organization - Low latency - Shared infrastructure (switches, access points)

Examples: - Home Wi-Fi network - Office Ethernet network - School campus network

WAN (Wide Area Network)

A network that spans large geographic areas, connecting multiple LANs.

Characteristics: - Lower speed (varies widely) - Large geographic coverage - Often provided by telecom companies - Higher latency - Uses routers and leased lines

Examples: - Internet connection - Corporate network connecting offices across cities - MPLS networks

Comparing LAN and WAN

Aspect	LAN	WAN
Geographic scope	Small (building/home)	Large (cities/countries)
Speed	Fast (Gbps)	Variable (Kbps - Gbps)
Ownership	User organization	Service provider
Latency	Low	Higher
Cost	Lower	Higher

Routing Basics

Routing is the process of determining the best path for data to travel from source to destination across multiple networks.

How Routing Works

1. **Source sends data** to its default gateway (router)
2. **Router examines** the destination IP address
3. **Router consults** its routing table
4. **Router determines** best next hop
5. **Router forwards** data to next router

6. **Process repeats** until destination reached

Routing Table

A routing table contains rules that tell the router where to send traffic.

Example routing table:

Destination	Gateway	Interface	Metric
192.168.1.0/24	0.0.0.0	eth0	0
0.0.0.0/0	203.0.113.1	eth1	100
10.0.0.0/8	192.168.1.1	eth0	10

- **0.0.0.0/0** = default route (catch-all)
- **Gateway** = next router to send to
- **Metric** = cost (lower is better)

Types of Routing

Static Routing: - Manual route configuration - Predictable, low overhead - Used for simple networks

Dynamic Routing: - Routes learned automatically via protocols - Adapts to network changes - Used in larger networks

Common Routing Protocols

Protocol	Type	Best For
OSPF	Interior	Large enterprise
RIP	Interior	Small networks
EIGRP	Interior	Cisco networks
BGP	Exterior	Internet backbone

Key Routing Concepts

- **Hop:** One router crossing
- **Next hop:** Next router on the path
- **Default gateway:** Router for unknown destinations
- **Metric:** Cost measure for route preference
- **Longest prefix match:** Most specific route wins

NAT (Network Address Translation)

NAT allows multiple devices to share a single public IP address. It's essential because IPv4 addresses are limited.

Why NAT?

- **IPv4 shortage:** Only ~4 billion addresses needed
- **Security:** Hides internal IP addresses
- **Simplicity:** One public IP for entire network

How NAT Works

When a device on your network accesses the internet:

1. Device has private IP (e.g., 192.168.1.100)
2. Router replaces private IP with public IP
3. Router tracks the connection in NAT table
4. Response comes back to public IP
5. Router looks up the original private IP
6. Router forwards response to correct device

NAT Table Example

Private IP	Port	Public IP	Port
192.168.1.100	5000	203.0.113.50	5000
192.168.1.101	5001	203.0.113.50	5001
192.168.1.102	5002	203.0.113.50	5002

Types of NAT

Static NAT: - One-to-one mapping - Fixed public IP for each device - Used for servers that need consistent access

Dynamic NAT: - Pool of public IPs assigned as needed - Temporary assignments - Common for regular internet access

PAT (Port Address Translation): - Many-to-one mapping - Uses different ports to distinguish connections - Most common type (home routers use this)

NAT Benefits and Limitations

Benefits: - Conserves public IP addresses - Adds basic security (hides internal IPs) - Simple to implement

Limitations: - Some protocols don't work well - End-to-end connectivity issues - Adds latency - Complicates server hosting

---

Key Takeaways

1. **Switches** connect devices within a LAN (Layer 2)
2. **Routers** connect different networks together (Layer 3)
3. **LAN** = local network (home/office); **WAN** = wide network (internet)
4. **Routing** determines the best path for data across networks
5. **NAT** allows multiple devices to share one public IP address
6. Home networks use **switches** (often built into router) and **NAT**

Exercises

Review Questions

1. What is the difference between a switch and a router?
2. Explain the difference between LAN and WAN.
3. What are the three types of NAT?
4. What is the purpose of a default gateway?

Hands-On Practice

1. **Map your network:** Identify your gateway, your device's IP, and trace the path to a public IP using `traceroute`.
2. **Draw your network:** Create a simple diagram showing how your devices connect to the internet.
3. **Check NAT:** Look at your router's NAT table (if accessible) or check how many devices share your public IP.
4. **Identify hops:** Run `traceroute google.com` and count how many routers your data passes through.

Answers

1. Switch connects devices within a LAN (Layer 2); router connects different networks (Layer 3)
2. LAN is local (home/office); WAN is wide (cities, internet)
3. Static NAT (one-to-one), Dynamic NAT (pool), PAT (many-to-one using ports)
4. Default gateway is the router that connects your local network to external networks

---

Next Steps

Proceed to Stage 5: Security Fundamentals to learn how networks are protected.

Stage 5: Security Fundamentals

Goal: Understand basic protections in networking.

Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules.

How Firewalls Work

1. **Inspect:** Analyze each packet of data
2. **Compare:** Match against security rules
3. **Decide:** Allow or block the traffic
4. **Log:** Record the decision for monitoring

Types of Firewalls

Network Firewall: - Hardware device or software at network perimeter - Protects entire network - Example: Cisco ASA, pfSense

Host Firewall: - Software on individual computers - Controls traffic to/from that device - Example: Windows Firewall, iptables

Cloud Firewall: - Managed service protecting cloud infrastructure - Example: AWS Security Groups, Cloudflare

Firewall Rules

Rules determine what traffic is allowed. Common criteria:

- **Source IP:** Where traffic comes from
- **Destination IP:** Where traffic goes
- **Port:** Which service/port
- **Protocol:** TCP, UDP, ICMP
- **Direction:** Inbound or outbound

Example rules:

Action	Source	Destination	Port	Protocol
Allow	Any	192.168.1.10	443	TCP
Allow	10.0.0.0/8	Any	80	TCP
Block	Any	Any	Any	Any

Stateful vs Stateless

Stateless Firewall: - Examines each packet individually - Doesn't track connection state - Faster but less secure

Stateful Firewall (most common): - Tracks active connections - Understands packet context - More secure, slightly slower

Common Firewall Technologies

Technology	Description
iptables	Linux firewall (legacy)
nftables	Modern Linux firewall
UFW	Uncomplicated Firewall (Ubuntu)
Windows Firewall	Built-in Windows defender
pf	BSD/macOS firewall

Network Security Concepts

Trusted vs Untrusted Networks

Trusted Network: - Internal network you control - Known devices and users - Higher privileges and access

Untrusted Network: - External networks (internet) - Unknown devices and users - Limited access, strict controls

Best Practice: Never trust external traffic implicitly

Defense in Depth

Multiple layers of security, so if one fails, others still protect.

Layers: 1. Physical security (locked rooms) 2. Network perimeter (firewall) 3. Network segmentation (VLANs) 4. Endpoint protection (antivirus) 5. Application security (validation) 6. Data encryption

Zero Trust Model

“Never trust, always verify.” Assume threats exist both inside and outside the network.

Principles: - Verify identity explicitly - Use least-privilege access - Assume breach mentality - Continuously validate

Segmentation

Dividing network into separate segments to limitattack spread.

Methods: - VLANs (Virtual LANs) - Subnets - Firewalls between segments - Access control lists (ACLs)

Common Network Threats

Spoofing

Pretending to be a trusted device by falsifying identity.

Types: - **IP spoofing:** Fake source IP address - **MAC spoofing:** Fake network adapter address - **ARP spoofing:** Fake ARP replies

Defense: - ARP inspection - IP validation - Encryption

Sniffing

Intercepting network traffic to capture data.

Types: - **Passive sniffing:** Listening to traffic (hub-based) - **Active sniffing:** Manipulating traffic (switch-based)

Defense: - Switches (not hubs) - Encryption (HTTPS, SSH, VPN) - Port security

Man-in-the-Middle (MITM)

Attacker secretly intercepts communication between two parties.

Examples: - Wi-Fi eavesdropping - SSL stripping - Session hijacking

Defense: - HTTPS always - Certificate validation - VPN for sensitive traffic

Denial of Service (DoS/DDoS)

Overwhelming a system with traffic to make it unavailable.

Types: - **DoS:** Attack from single source - **DDoS:** Attack from multiple sources

Defense: - Firewalls - Rate limiting - CDN protection - IDS/IPS

Unauthorized Access

Gaining access to systems without permission.

Methods: - Weak passwords - Exploiting vulnerabilities - Social engineering

Defense: - Strong authentication - Patch management - Access controls - User training

Malware

Malicious software designed to damage or gain unauthorized access.

Types: - Virus - Worm - Trojan horse - Ransomware - Spyware

Defense: - Antivirus software - Regular updates - User awareness

---

Security Best Practices

For Networks

1. Use strong firewall rules (deny by default)
2. Keep firmware/software updated
3. Use VLANs to segment networks
4. Monitor network traffic
5. Use VPN for remote access
6. Implement intrusion detection

For Devices

1. Change default passwords
2. Disable unnecessary services
3. Enable logging
4. Use encryption (WPA3 for Wi-Fi)
5. Disable remote management when not needed

For Users

1. Use strong, unique passwords
2. Don’t click suspicious links
3. Verify SSL certificates
4. Report security incidents
5. Lock computers when away

Key Takeaways

1. **Firewalls** filter traffic based on rules (allow/deny)
2. **Stateful firewalls** track connections for better security
3. **Defense in depth** uses multiple security layers

4. **Zero trust** assumes no implicit trust
5. **Spoofing** falsifies identity; **sniffing** intercepts traffic
6. **DDoS** overwhelms systems with traffic
7. Best security combines **technology**, **processes**, and **people**

Exercises

Review Questions

1. What is the difference between a stateful and stateless firewall?
2. Explain “defense in depth” and give an example.
3. What is the difference between a DoS and DDoS attack?
4. How does HTTPS protect against sniffing?

Hands-On Practice

1. **Check your firewall:** On Windows, open Windows Security → Firewall. On Mac, check System Preferences → Security & Privacy.
2. **Verify HTTPS:** Visit a website and click the lock icon to see the certificate details.
3. **Check router security:** Log into your home router and review firewall settings, Wi-Fi password, and remote management status.
4. **Password audit:** Check if your Wi-Fi uses WPA2/WPA3 (not WEP).

Answers

1. Stateful firewalls track active connections; stateless examine each packet individually
2. Defense in depth uses multiple layers (firewall, antivirus, encryption, user training); example: network firewall + host firewall + encryption
3. DoS is from one source; DDoS is from multiple sources (botnet)
4. HTTPS encrypts data in transit, preventing sniffing of the content

---

Next Steps

Proceed to Stage 6: Troubleshooting Skills to learn how to diagnose and fix network issues.

Stage 6: Troubleshooting Skills

Goal: Diagnose and fix simple network issues.

---

ping

Tests connectivity between your device and another device on the network or internet.

Basic Usage

```
# Ping a hostname or IP address
ping google.com
ping 192.168.1.1

# Windows: stop with Ctrl+C
# Linux/Mac: ping runs continuously, stop with Ctrl+C
```

Understanding the Output

```
PING google.com (142.250.185.206): 56 data bytes
64 bytes from 142.250.185.206: icmp_seq=0 ttl=115 time=14.382 ms
64 bytes from 142.250.185.206: icmp_seq=1 ttl=115 time=13.891 ms
64 bytes from 142.250.185.206: icmp_seq=2 ttl=115 time=14.012 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max = 13.891/14.095/14.382 ms
```

Key information: - `ttl` (Time To Live): How many hops remaining - `time`: Round-trip latency in milliseconds - `packet loss`: Percentage of failed pings

Common ping Options

Option	Linux/Mac	Windows	Description
Count	`-c 4`	`-n 4`	Number of pings
Interval	`-i 2`	N/A	Seconds between pings
Size	`-s 100`	`-l 100`	Packet size

Troubleshooting with ping

1. **Ping localhost:** `ping 127.0.0.1` — verifies TCP/IP stack
2. **Ping local IP:** `ping 192.168.1.100` — verifies network card
3. **Ping gateway:** `ping 192.168.1.1` — verifies local network
4. **Ping remote:** `ping google.com` — verifies internet connectivity

What ping tells you

- **Success:** Network path is working
- **Request timed out:** Network path blocked or slow
- **Destination unreachable:** Routing issue
- **Unknown host:** DNS resolution failed

---

traceroute / tracert

Shows the path (hops) that packets take to reach a destination. Helps identify where delays or failures occur.

Usage

```
# Linux/Mac
traceroute google.com
tracert google.com

# Windows
tracert google.com
```

Understanding the Output

```
traceroute to google.com (142.250.185.206), 30 hops max, 60 byte
packets
 1  192.168.1.1 (192.168.1.1)  1.234 ms  1.189 ms  1.123 ms
 2  10.0.0.1 (10.0.0.1)        5.432 ms  5.389 ms  5.401 ms
 3  72.14.215.85 (72.14.215.85)  12.345 ms  12.234 ms  12.567 ms
 4  142.250.185.206 (142.250.185.206)  14.123 ms  14.089 ms
14.045 ms
```

Each line = one hop (router)

What to look for: - High latency at specific hop → problem router - `* * *` → hop not responding (blocked or down) - Many hops → long path

Common Options

Option	Linux/Mac	Windows	Description
Max hops	`-m 15`	`-h 15`	Maximum hops
Wait time	`-w 2`	`-w 2000`	Timeout in seconds

When to use traceroute

- Slow connection → find slow hop
- Connection timeout → find failing router
- Learning path → understand routing

---

ipconfig / ifconfig

Displays network configuration information for your device.

Usage

```
# Windows
ipconfig
ipconfig /all

# Linux/Mac
ifconfig
ip addr show
```

Understanding ipconfig Output (Windows)

```
Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Key Information

Field	Description
IPv4 Address	Your device's IP on the network
Subnet Mask	Determines network size
Default Gateway	Your router's IP
DNS Server	Server that resolves domain names
MAC Address	Physical network adapter address

Useful Commands

```
# Windows - Release and renew DHCP lease
ipconfig /release
ipconfig /renew

# Windows - Clear DNS cache
ipconfig /flushdns

# Linux/Mac - Show specific interface
ip addr show eth0
ip addr show en0

# Linux/Mac - Bring interface up/down
sudo ifconfig eth0 down
sudo ifconfig eth0 up
```

---

nslookup

Queries DNS to find IP addresses and other DNS records.

Basic Usage

```
# Look up IP address for domain
nslookup google.com

# Look up specific record type
nslookup -type=MX google.com
nslookup -type=TXT google.com
```

Understanding the Output

```
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.185.206
```

Key information: - **Server:** DNS server used (usually your router) - **Address:** Resolved IP address

Common Options

Option	Description
`-type=MX`	Query mail servers
`-type=TXT`	Query TXT records
`-type=NS`	Query name servers
`-type=AAAA`	Query IPv6 addresses

Troubleshooting DNS

1. **nslookup fails:** DNS server not responding
2. **Wrong IP:** DNS cache issue or poisoning
3. **No response:** Network connectivity problem
4. **Different results:** Multiple DNS records

---

netstat

Displays network connections, routing tables, and interface statistics.

Usage

```
# Show all connections
netstat -a

# Show active connections
netstat -an
```

```
# Show routing table
netstat -r
```

Useful Options

Option	Description
`-a`	Show all connections
`-n`	Show addresses numerically
`-p`	Show process using connection
`-r`	Show routing table

---

curl / telnet

curl

Tests HTTP/HTTPS connections and displays response details.

```
# Basic GET request
curl -v https://example.com

# Show headers only
curl -I https://example.com
```

telnet

Tests if a specific port is open and reachable.

```
# Test HTTP port 80
telnet example.com 80

# Test SSH port 22
telnet example.com 22
```

Note: telnet may need to be installed separately on some systems.

Quick Troubleshooting Workflow

Step 1: Check Local Configuration

```
# Windows
ipconfig /all

# Linux/Mac
ip addr show
```

Verify: IP address, subnet mask, gateway, DNS

Step 2: Test Local Connectivity

```
# Ping localhost
ping 127.0.0.1

# Ping your IP
ping 192.168.1.100

# Ping gateway
ping 192.168.1.1
```

Step 3: Test Remote Connectivity

```
# Ping known good destination
ping 8.8.8.8
ping google.com
```

Step 4: Trace the Path

```
# See where packets go
traceroute google.com   # Linux/Mac
tracert google.com      # Windows
```

Step 5: Check DNS

```
# Test DNS resolution
nslookup google.com
```

Common Issues and Solutions

Problem	Likely Cause	Fix
No internet, but local works	DNS issue	Flush DNS, check gateway
Can’t reach specific site	Firewall or site issue	Try another site, check firewall
Slow connection	Congestion or ISP issue	Run traceroute, test speed
Can’t connect to local device	IP/subnet mismatch	Check IP config
Intermittent connectivity	Hardware or interference	Check cables, restart devices

---

Key Takeaways

1. **ping** tests basic connectivity and latency
2. **traceroute** shows the path and identifies slow hops
3. **ipconfig/ifconfig** shows your network configuration
4. **nslookup** tests DNS resolution
5. **netstat** shows active connections and ports
6. Follow the workflow: local → gateway → remote → DNS
7. Most issues are: cable, IP config, DNS, or firewall

Exercises

Review Questions

1. What is the correct troubleshooting order (local → remote)?
2. What does each command do: ping, traceroute, nslookup, netstat?
3. What does it mean if ping works but DNS doesn’t?

4. How do you release and renew your DHCP IP address?

Hands-On Practice

1. **Full diagnosis:** Run through the troubleshooting workflow on your own network.
2. **Test connectivity:** Ping various addresses (localhost, gateway, 8.8.8.8, google.com) and explain the results.
3. **Trace your path:** Run `traceroute` to a website and identify each hop.
4. **Check DNS:** Use `nslookup` to resolve different domains. Use different DNS servers (e.g., `nslookup google.com 8.8.8.8`).
5. **View connections:** Run `netstat -an` and identify what connections are active on your machine.

Answers

1. Local config → local connectivity → gateway → remote → DNS
2. ping: tests connectivity; traceroute: shows path; nslookup: DNS queries; netstat: shows connections
3. Network works but DNS is broken - check DNS settings, flush cache
4. Windows: `ipconfig /release` then `ipconfig /renew`; Linux: `sudo dhclient -r` then `sudo dhclient`

Congratulations!

You've completed all 6 stages of the Networking Learning Roadmap:

1. **Core Concepts** — OSI/TCP-IP models, terminology
2. **Addressing & Identity** — IPv4, IPv6, subnetting, DHCP
3. **Name Resolution & Access** — DNS, ports, protocols
4. **Network Devices & Traffic Flow** — Switches, routers, NAT
5. **Security Fundamentals** — Firewalls, threats, best practices
6. **Troubleshooting Skills** — Diagnostic tools and workflow

You now have the foundational knowledge to understand, configure, and troubleshoot networks at a working level.

Appendix A: Dictionary of Terms

A quick reference for key networking terms used throughout this roadmap.

A

ACK (Acknowledgment) — A signal sent to confirm receipt of data in TCP communication.

ACL (Access Control List) — A list of rules that define what traffic is allowed or denied.

ARP (Address Resolution Protocol) — A protocol that maps IP addresses to MAC addresses on a local network.

Application Layer — Layer 7 of the OSI model; provides network services to end-user applications.

B

Bandwidth — The maximum data transfer capacity of a network connection, measured in bits per second (bps).

BGP (Border Gateway Protocol) — The routing protocol used between autonomous systems on the internet.

Broadcast — A communication method where data is sent to all devices on a network.

C

CIDR (Classless Inter-Domain Routing) — A method of IP addressing that allocates IP addresses based on network prefixes (e.g., /24, /16).

Client — A device or application that requests services from a server.

Collision Domain — A network segment where data collisions can occur if two devices transmit simultaneously.

D

Data Link Layer — Layer 2 of the OSI model; handles physical addressing (MAC) and frame transmission.

DHCP (Dynamic Host Configuration Protocol) — A protocol that automatically assigns IP addresses and network settings to devices.

DNS (Domain Name System) — A system that translates domain names into IP addresses.

DORA — The DHCP process: Discover, Offer, Request, Acknowledge.

E

Ethernet — A standard technology for connecting devices in a wired local area network (LAN).

F

Firewall — A network security device that monitors and filters incoming and outgoing traffic based on security rules.

FTP (File Transfer Protocol) — A protocol used for transferring files between a client and server.

G

Gateway — A device (usually a router) that connects one network to another, serving as an entry/exit point.

H

HTTP (Hypertext Transfer Protocol) — The protocol used for transferring web pages and data on the internet.

HTTPS (HTTP Secure) — Encrypted version of HTTP for secure web communication.

I

ICMP (Internet Control Message Protocol) — A protocol used for error reporting and diagnostics (used by ping).

IDS (Intrusion Detection System) — A system that monitors network traffic for suspicious activity.

IP (Internet Protocol) — The protocol that defines how data is addressed and routed across networks.

IP Address — A unique numerical identifier assigned to each device on a network.

IPv4 — IP version 4; uses 32-bit addresses (e.g., 192.168.1.1).

IPv6 — IP version 6; uses 128-bit addresses for virtually unlimited addressing.

IPS (Intrusion Prevention System) — An IDS that actively blocks detected threats.

L

LAN (Local Area Network) — A network confined to a small geographic area like a home, office, or building.

Latency — The time delay in data transmission, measured in milliseconds (ms).

Link-Local Address — An IPv6 address automatically assigned to a device for local network communication only.

M

MAC Address (Media Access Control Address) — A unique hardware identifier assigned to network adapters.

MITM (Man-in-the-Middle) Attack — An attack where an attacker secretly intercepts communication between two parties.

MPLS (Multi-Protocol Label Switching) — A routing technique used by ISPs for faster data forwarding.

N

NAT (Network Address Translation) — A technique that allows multiple devices to share a single public IP address.

Network Layer — Layer 3 of the OSI model; handles logical addressing and routing.

O

OSI Model (Open Systems Interconnection) — A conceptual 7-layer framework for understanding network communication.

OSPF (Open Shortest Path First) — A dynamic routing protocol used in interior networks.

P

Packet — The basic unit of data transmitted over a network, containing header, payload, and trailer information.

PAT (Port Address Translation) — A type of NAT that maps multiple private IPs to a single public IP using ports.

Ping — A diagnostic tool that tests connectivity between devices using ICMP.

Port — A numbered endpoint that identifies a specific service or application on a device.

Private IP Address — An IP address used within a private network, not routable on the internet.

Protocol — A set of rules that govern how data is transmitted over a network.

Public IP Address — An IP address that is routable on the internet, assigned by an ISP.

Q

QoS (Quality of Service) — A technique that prioritizes certain types of network traffic.

R

RIP (Routing Information Protocol) — A simple dynamic routing protocol for small networks.

Router — A device that connects different networks and directs traffic between them.

Routing Table — A table stored in a router that determines the best path for forwarding data.

S

Server — A computer or application that provides services to clients.

SMTP (Simple Mail Transfer Protocol) — The protocol used for sending emails between servers.

SSH (Secure Shell) — A protocol for secure remote access to computers.

Stateful Firewall — A firewall that tracks active connections and makes decisions based on connection state.

Stateless Firewall — A firewall that evaluates each packet individually without tracking connections.

Subnet — A smaller network created by dividing a larger network.

Subnet Mask — A number that defines which portion of an IP address is the network vs. host portion.

Switch — A device that connects devices within a single network (LAN) using MAC addresses.

T

TCP (Transmission Control Protocol) — A connection-oriented protocol that ensures reliable, ordered data delivery.

Throughput — The actual amount of data successfully transferred over a network.

TLD (Top-Level Domain) — The highest level in the DNS hierarchy (e.g., .com, .org, .net).

Traceroute — A diagnostic tool that shows the path (hops) data takes to reach a destination.

Transport Layer — Layer 4 of the OSI model; handles end-to-end communication and data flow control.

U

UDP (User Datagram Protocol) — A connectionless protocol that sends data without guaranteeing delivery.

V

VLAN (Virtual Local Area Network) — A logical network that segments devices regardless of physical location.

VPN (Virtual Private Network) — A secure, encrypted connection over a public network.

W

WAN (Wide Area Network) — A network spanning large geographic areas, connecting multiple LANs.

WPA (Wi-Fi Protected Access) — A security protocol for wireless networks.

Quick Reference Tables

OSI Model Layers

#	Layer	Mnemonic
7	Application	Away
6	Presentation	Pizza
5	Session	Sausage
4	Transport	Throw
3	Network	Not
2	Data Link	Do
1	Physical	Please

Common Ports

Port	Service
20	FTP Data
21	FTP Control
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS
3306	MySQL

Port	Service
3389	RDP
5432	PostgreSQL
8080	HTTP Proxy

DNS Record Types

Record	Purpose
A	IPv4 address
AAAA	IPv6 address
CNAME	Alias
MX	Mail server
NS	Name server
TXT	Text record
PTR	Reverse DNS

Routing Protocols

Protocol	Type	Use
RIP	Interior	Small networks
OSPF	Interior	Large enterprise
EIGRP	Interior	Cisco networks
BGP	Exterior	Internet backbone

Subnet Quick Reference

CIDR	Hosts	Subnet Mask
/24	254	255.255.255.0
/25	126	255.255.255.128
/26	62	255.255.255.192
/27	30	255.255.255.224
/28	14	255.255.255.240
/30	2	255.255.255.252

Return to Table of Contents

Quick Reference Card

OSI 7 Layers

Please **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

#	Layer	What it does	Examples
7	Application	User interface	HTTP, DNS
6	Presentation	Data format	SSL, JPEG
5	Session	Connection	NetBIOS
4	Transport	Reliable delivery	TCP, UDP
3	Network	Routing	IP, ICMP
2	Data Link	Frames	Ethernet
1	Physical	Bits	Cables

Common Ports

Port	Service	Port	Service
20	FTP Data	110	POP3
21	FTP Control	143	IMAP
22	SSH	443	HTTPS
25	SMTP	3306	MySQL
53	DNS	3389	RDP
80	HTTP	8080	Proxy

IP Addressing

Private IP Ranges

- 10.0.0.0/8 (10.x.x.x)
- 172.16.0.0/12 (172.16.x.x - 172.31.x.x)
- 192.168.0.0/16 (192.168.x.x)

Subnet Quick Reference

CIDR	Usable Hosts	Mask
/24	254	255.255.255.0
/25	126	255.255.255.128
/26	62	255.255.255.192
/27	30	255.255.255.224
/28	14	255.255.255.240
/30	2	255.255.255.252

Troubleshooting Commands

Windows

```
ipconfig /all           # Show config
ipconfig /release       # Release DHCP
ipconfig /renew         # Renew DHCP
ipconfig /flushdns      # Clear DNS cache
ping <host>             # Test connectivity
tracert <host>          # Trace route
nslookup <domain>       # DNS lookup
netstat -an             # Show connections
```

Linux/Mac

```
ip addr show            # Show config
ifconfig                # Show config (legacy)
ping <host>             # Test connectivity
traceroute <host>       # Trace route (Linux)
tracert <host>          # Trace route (Mac)
nslookup <domain>       # DNS lookup
dig <domain>            # DNS lookup (detailed)
netstat -an             # Show connections
```

Troubleshooting Workflow

```
1. Check local config       → ipconfig / ip addr
2. Test localhost           → ping 127.0.0.1
```

```
3. Test gateway              → ping <gateway IP>
4. Test remote               → ping 8.8.8.8
5. Trace path                → traceroute
6. Check DNS                 → nslookup
```

DNS Record Types

Record	Purpose
A	IPv4 address
AAAA	IPv6 address
CNAME	Alias
MX	Mail server
NS	Name server
TXT	Text (SPF, etc.)

HTTP Status Codes

Code	Meaning	Code	Meaning
200	OK	400	Bad Request
301	Moved	401	Unauthorized
304	Not Modified	403	Forbidden
404	Not Found	500	Server Error
502	Bad Gateway	503	Unavailable

Security Terms

Term	Definition
Firewall	Filters traffic by rules
NAT	Shares one IP with many devices
VPN	Secure encrypted tunnel
VLAN	Logical network segment
DoS	Denial of Service attack
DDoS	Distributed DoS attack

Term	Definition
MITM	Man-in-the-Middle attack

Print this page and keep it handy!