Networking Fundamentals

Understanding How Networks Work

1-Day Training Course

Course Overview

Learn basic networking knowledge and skills essential for systems administrators and developers.

What You'll Learn

- OSI and TCP/IP reference models
- Common protocols and ports
- IP addressing and subnetting
- CIDR notation
- NAT, DHCP, and routing
- DNS fundamentals

> **Course Philosophy:** 70% hands-on labs, 30% instructor-led discussion

Agenda

MORNING

- OSI Reference Model
- TCP/IP Model
- Protocols and Ports
- Network Tools Overview

AFTERNOON

- IP Addressing Fundamentals
- Subnetting and CIDR
- NAT and Routing
- DHCP and DNS

Module 1

The OSI Model

Why Reference Models?

Reference models provide a common framework for understanding how network communication works.

Benefits

- **Standardization:** Common language for vendors and engineers
- **Modularity:** Changes to one layer don't affect others
- **Troubleshooting:** Isolate problems to specific layers
- **Interoperability:** Different vendors' equipment can work together

OSI Model - 7 Layers

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Mnemonic:

"**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing"

Or bottom-up:

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

Upper Layers (7-5)

7. APPLICATION

- User interface
- HTTP, FTP, SMTP
- DNS, SSH

6. PRESENTATION

- Data formatting
- Encryption/Decryption
- Compression

5. SESSION

- Session management
- Authentication
- Connection recovery

Key Insight: These layers deal with application data and are often combined in practice (TCP/IP model)

Lower Layers (4-1)

Layer	Function	PDU	Examples
4. Transport	End-to-end delivery	Segment	TCP, UDP
3. Network	Logical addressing, routing	Packet	IP, ICMP
2. Data Link	Physical addressing, framing	Frame	Ethernet, Wi-Fi
1. Physical	Bit transmission	Bits	Cables, signals

> **PDU:** Protocol Data Unit - the name for data at each layer

Data Encapsulation

As data travels down the stack, each layer adds its own header (and sometimes trailer).

Data

TCP Header | Data

IP Header | TCP Header | Data

Frame Header | IP Header | TCP Header | Data | Frame Trailer

> **De-encapsulation:** The reverse happens at the receiving end - headers are stripped as data moves up

Module 2

TCP/IP Model

TCP/IP vs OSI Model

OSI (7 LAYERS)

Application

Presentation

Session

Transport

Network

Data Link

Physical

TCP/IP (4 LAYERS)

Application

Transport

Internet

Link (Network Access)

> **Reality:** TCP/IP is what the Internet actually uses. OSI is primarily a teaching/reference model.

TCP/IP Layer Details

Layer	OSI Equivalent	Key Protocols
Application	Layers 5-7	HTTP, HTTPS, FTP, SSH, DNS, SMTP
Transport	Layer 4	TCP, UDP
Internet	Layer 3	IP, ICMP, ARP
Link	Layers 1-2	Ethernet, Wi-Fi, PPP

TCP vs UDP

TCP (TRANSMISSION CONTROL PROTOCOL)

- Connection-oriented
- Reliable delivery
- Ordered packets
- Error checking & retransmission
- Flow control

Use: Web, email, file transfer

UDP (USER DATAGRAM PROTOCOL)

- Connectionless
- Best-effort delivery
- No ordering guarantee
- No retransmission
- Lower overhead

Use: Streaming, gaming, DNS

TCP Three-Way Handshake

TCP establishes connections using a three-step process:

Client Server

1. SYN →

← 2. SYN-ACK

3. ACK →

> **Result:** Both sides agree on initial sequence numbers and connection parameters

Module 3

Protocols and Ports

Understanding Ports

Ports allow multiple services to run on a single IP address.

Port Ranges

Range	Name	Description
0-1023	Well-Known	Reserved for system services (requires root)
1024-49151	Registered	Assigned by IANA for specific services
49152-65535	Dynamic/Ephemeral	Used by client applications

Common Ports to Know

Port	Protocol	Service
20-21	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
67-68	UDP	DHCP

Port	Protocol	Service
80	TCP	HTTP
110	TCP	POP3
143	TCP	IMAP
443	TCP	HTTPS
3306	TCP	MySQL
5432	TCP	PostgreSQL

Lab: OSI Model and Protocols

Exercise Objectives

- Explore network interfaces and configuration
- Use common networking commands
- Analyze network traffic at different layers
- Identify protocols and ports in use

Tools You'll Use

- `ip`, `ss`, `netstat`
- `tcpdump`, `ping`, `traceroute`

Module 4

IP Addressing

IPv4 Address Structure

IPv4 addresses are 32-bit numbers, typically written in dotted-decimal notation.

```
192.168.1.100
```

BINARY REPRESENTATION

Each octet is 8 bits (0-255)

```
11000000.10101000.00000001.01100100
```

TOTAL ADDRESSES

2^32 = ~4.3 billion addresses

Not enough for today's devices!

IPv4 Address Classes

Class	First Octet	Default Mask	Use
A	1-126	255.0.0.0 (/8)	Large networks
B	128-191	255.255.0.0 (/16)	Medium networks
C	192-223	255.255.255.0 (/24)	Small networks
D	224-239	N/A	Multicast
E	240-255	N/A	Experimental

> **Note:** Classful addressing is largely historical. Modern networks use CIDR.

Private IP Address Ranges

Reserved for internal networks, not routable on the Internet.

Class	Range	CIDR	Addresses
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8	16.7 million
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12	1 million
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16	65,536

> **Common:** Home routers typically use 192.168.0.0/24 or 192.168.1.0/24

CIDR Notation

CIDR (Classless Inter-Domain Routing) replaced classful addressing.

```
192.168.1.0/24 ← /24 means 24 bits for network, 8 bits for hosts
```

CIDR	Subnet Mask	Hosts	Use
/24	255.255.255.0	254	Small office
/16	255.255.0.0	65,534	Large campus
/30	255.255.255.252	2	Point-to-point
/32	255.255.255.255	1	Single host

Subnetting Basics

Subnetting divides a network into smaller networks for better organization and security.

WHY SUBNET?

- Reduce broadcast domains
- Improve security (segment traffic)
- Efficient IP allocation
- Easier management

EXAMPLE

Split 192.168.1.0/24 into 4 subnets:

- 192.168.1.0/26 (0-63)
- 192.168.1.64/26 (64-127)
- 192.168.1.128/26 (128-191)
- 192.168.1.192/26 (192-255)

IPv6 Overview

IPv6 uses 128-bit addresses, providing virtually unlimited addresses.

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

Key Differences from IPv4

- **Address space:** 2^128 addresses (340 undecillion)
- **No NAT needed:** Every device can have a public address
- **No broadcast:** Uses multicast instead
- **Auto-configuration:** SLAAC (Stateless Address Autoconfiguration)

> **Shorthand:** `::` represents consecutive zeros: `2001:db8::1`

Lab: IP Addressing and Subnets

Exercise Objectives

- View and configure IP addresses
- Calculate subnet ranges
- Understand CIDR notation
- Explore IPv6 addresses

Tools You'll Use

- `ip addr`, `ip route`
- `ipcalc` for subnet calculations

Module 5

NAT, Routing, and DHCP

Network Address Translation (NAT)

NAT translates private IP addresses to public IP addresses, allowing multiple devices to share one public IP.

WITHOUT NAT

Every device needs a public IP

IPv4 exhaustion!

WITH NAT

Many private IPs → One public IP

Conserves addresses

NAT Types

- **SNAT:** Source NAT - changes source address (outbound)
- **DNAT:** Destination NAT - changes destination address (inbound/port forwarding)
- **PAT/NAPT:** Port Address Translation - multiple internal IPs share one external IP using different ports

IP Routing Basics

Routing determines how packets travel from source to destination across networks.

Key Concepts

- **Routing Table:** Maps destination networks to next-hop addresses
- **Default Gateway:** Where to send packets for unknown destinations
- **Hop:** Each router the packet passes through
- **TTL:** Time-to-live prevents infinite loops

```
# View routing table
ip route show
default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0 proto kernel scope link
```

Dynamic Host Configuration Protocol

DHCP automatically assigns IP addresses and network configuration to devices.

DHCP Process (DORA)

1. DISCOVER
Client broadcasts

2. OFFER
Server responds

3. REQUEST
Client accepts

4. ACKNOWLEDGE
Server confirms

DHCP Provides

- IP address and subnet mask
- Default gateway
- DNS server addresses
- Lease time

Module 6

Domain Name System (DNS)

What is DNS?

DNS translates human-readable domain names to IP addresses.

```
www.example.com → 93.184.216.34
```

Why DNS?

- Humans remember names better than numbers
- IP addresses can change without affecting users
- Enables load balancing (multiple IPs per name)
- Distributed, hierarchical system for scalability

DNS Hierarchy

Root DNS Servers (.)

TLD Servers (.com, .org, .net)

Authoritative Servers (example.com)

Local DNS Resolver (Your ISP/Company)

> **Resolution:** Queries flow down from root to find the authoritative server for a domain

Common DNS Record Types

Type	Purpose	Example
A	Maps name to IPv4	example.com → 93.184.216.34
AAAA	Maps name to IPv6	example.com → 2606:2800:220:1:...
CNAME	Alias to another name	www → example.com
MX	Mail server	mail.example.com (priority 10)
NS	Name server	ns1.example.com
TXT	Text records	SPF, DKIM verification

DNS Lookup Tools

```
# Simple lookup
host example.com

# Detailed query
dig example.com

# Query specific record type
dig example.com MX

# Query specific DNS server
dig @8.8.8.8 example.com

# Reverse lookup (IP to name)
dig -x 93.184.216.34
```

Lab: NAT, Routing, and DNS

Exercise Objectives

- Examine routing tables and gateways
- Trace packet paths across networks
- Query DNS records
- Understand DNS resolution process

Tools You'll Use

- `ip route`, `traceroute`
- `dig`, `host`, `nslookup`

Course Summary

> ### MODELS
> - OSI 7-layer model
> - TCP/IP 4-layer model
> - Encapsulation
>
> ### ADDRESSING
> - IPv4 and IPv6
> - CIDR notation
> - Subnetting
>
> ### SERVICES
> - NAT and routing
> - DHCP
> - DNS

Key Takeaways

- Reference models help troubleshoot by isolating problems to layers

- TCP provides reliability; UDP provides speed
- Private IP addresses + NAT enable Internet scalability
- DNS is the "phone book" of the Internet

Questions?

Networking Fundamentals

Speaker notes