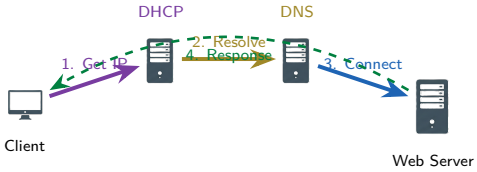
Module 6.0: Implementing Network Services

Intro to Networks

Brendan Shea, PhD

Introduction to Networking

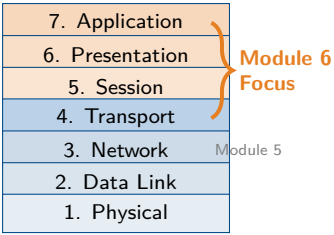


Outline I

Review: Building on Module 5

What We Learned (Module 5)

- **Routing**: How packets find their way
- **NAT/PAT**: Address translation
- **VLANs**: Network segmentation
- **Firewalls**: Traffic filtering



The Missing Piece

We can route packets, but how do devices **get their addresses**? How do they **find services** by name?

Module 6 Focus

Services that make networks usable: TCP/UDP, DHCP, DNS

Module 6 Overview

Topics Covered

1. **Transport Protocols**
   TCP, UDP, ports, connections
2. **DHCP**
   Automatic IP configuration
3. **APIPA & SLAAC**
   Fallback and IPv6 auto-config
4. **DHCP Troubleshooting**
   Relay agents, common issues
5. **DNS Fundamentals**
   Name resolution, records
6. **DNS Troubleshooting**
   nslookup, dig, common problems

Learning Outcomes

By the end of this module, you will be able to:

- Explain TCP vs UDP and when to use each
- Describe the DHCP DORA process
- Configure DHCP scopes and options
- Explain DNS hierarchy and record types
- Use nslookup and dig for troubleshooting
- Identify common service misconfigurations

Batman Universe

Case studies featuring Batman, Oracle, Batgirl, Alfred, Catwoman, and The Riddler!

Learning Outcomes I

After completing this module, you will be able to:

- Explain the differences between **TCP** (reliable, connection-oriented) and **UDP** (fast, connectionless) and identify appropriate use cases for each protocol.
- Describe how **ports** (0–65535) identify services and how **sockets** (IP address + port) establish connections between applications.
- Configure and manage **DHCP** servers, including defining **scopes**, creating **reservations**, and setting **DHCP options** (gateway, DNS, lease time).
- Explain the **DORA** process (Discover, Offer, Request, Acknowledge) used by DHCP clients to obtain IP addresses.
- Configure **DHCP relay agents** to forward DHCP messages across subnets and troubleshoot common DHCP issues.

Learning Outcomes II

- Describe **APIPA** (169.254.x.x/16) as a fallback mechanism when DHCP is unavailable and explain its limitations (link-local only).
- Explain IPv6 **SLAAC** (Stateless Address Autoconfiguration) using Router Advertisements and **DHCPv6** (stateful and stateless modes).
- Describe the **DNS** hierarchy (Root, TLD, Domain, Host) and explain how DNS resolves domain names to IP addresses.
- Identify common DNS record types: **A** (IPv4), **AAAA** (IPv6), **CNAME** (alias), **MX** (mail server), **PTR** (reverse lookup).
- Use DNS troubleshooting tools like **nslookup** and **dig** to query DNS records, diagnose resolution issues, and verify zone transfers.

Transport Layer and Ports

- **Layer 4** provides host-to-host communication.
- **Ports** identify specific services/applications.
- Port range: **0–65535**
- A **socket** = IP address + port number

Example

Web server: `10.0.0.5:443`

TCP: Reliable Delivery

- **Transmission Control Protocol**
- **Connection-oriented**: Establishes session first
- **Reliable**: Guarantees delivery
- **Ordered**: Packets arrive in sequence
- **Error-checked**: Detects corruption
- **Flow control**: Prevents overwhelming receiver

TCP Header (20+ bytes)

Source Port	**Dest Port**
Sequence Number	
Acknowledgment Number	
Offset | **Flags**	Window Size
Checksum	Urgent Pointer
Options (variable)	

Flags : SYN, ACK, FIN, RST, PSH, URG

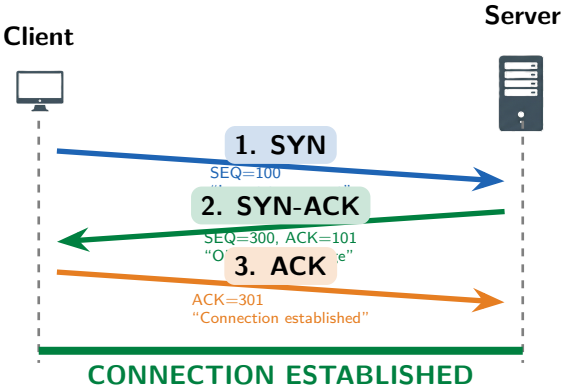
Trade-off

Reliability costs **speed** and **overhead**. TCP headers are 20+ bytes.

Common TCP Applications

HTTP/S, FTP, SSH, SMTP, Telnet

TCP Three-Way Handshake



Purpose

Synchronize sequence numbers and confirm both sides are ready to communicate.

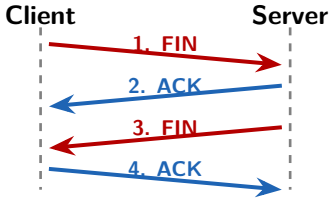
Memory Tip

Think: "**S**end → **S**end back with **A**ck → **A**cknowledge"

TCP Connection Teardown

Graceful Close (4-way)

1. **FIN**: "I'm done sending"
2. **ACK**: "Got it"
3. **FIN**: "I'm done too"
4. **ACK**: "Goodbye"



Abrupt Close (RST)

RST flag immediately terminates. Used when something goes wrong.

Key Point

Either side can initiate close. Process is bidirectional.

TIME_WAIT

Socket waits 2 min before reuse to avoid confusion with late packets.

UDP: Fast and Simple

- **User Datagram Protocol**
- **Connectionless**: No handshake
- **Unreliable**: No delivery guarantee
- **Unordered**: May arrive out of order
- **No flow control**: Send as fast as possible
- "Fire and forget"

UDP Header (8 bytes only!)

Source Port 16 bits	**Dest Port** 16 bits
Length 16 bits	**Checksum** 16 bits
Data (Payload)	

Only 8 bytes vs TCP's 20+ bytes!

Why Use UDP?

When **speed** matters more than perfection: streaming, gaming, VoIP, DNS queries.

No Handshake Needed

Data sent immediately—no connection setup overhead. Trade-off: no delivery guarantee.

Common UDP Applications

DNS, DHCP, TFTP, SNMP, VoIP, Streaming

TCP vs UDP Comparison

Feature	TCP	UDP
Connection	Connection-oriented	Connectionless
Reliability	Guaranteed	Best effort
Ordering	In-order delivery	No ordering
Speed	Slower	Faster
Header Size	20+ bytes	8 bytes

Use TCP When...

- Data must arrive complete (files, email)
- Order matters (web pages)
- Errors are unacceptable (banking)

Use UDP When...

- Speed is critical (gaming, video)
- Small queries (DNS lookups)
- Loss is tolerable (streaming)

Case Study: Batman & Oracle

▶ Case Study: The Mission Communications Problem

Batman is pursuing criminals through Gotham while coordinating with Oracle at the Clocktower. He needs to accomplish two things simultaneously:

1. Transfer surveillance footage from the Batmobile cameras to Oracle's servers (large video files, **must not lose any frames**).
2. Maintain **real-time voice communication** with Oracle during the high-speed chase (some audio glitches are acceptable).

The Batcomputer must choose the right transport protocol for each task.

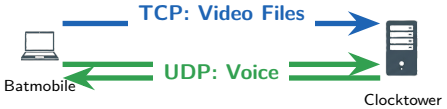
Review Questions

1. Which protocol should be used for the video file transfer? Why?
2. Which protocol should be used for the voice communication? Why?
3. What would happen if the protocols were swapped?

Case Study Solution: Batman & Oracle

✓ Solution: The Mission Communications Problem

1. **Video files** → **TCP**: Missing frames corrupt evidence. TCP guarantees delivery.
2. **Voice comms** → **UDP**: Real-time essential. Brief glitches beat lag. UDP wins.
3. If swapped: Corrupted files (UDP) or unacceptable voice delay (TCP).



Key Lesson

"The mission requires choosing the right tool." Match protocol to need: reliability vs speed.

Common TCP and UDP Ports

Port	Protocol	Service	Description
20-21	TCP	FTP	File Transfer Protocol
22	TCP	SSH	Secure Shell
23	TCP	Telnet	Remote terminal (insecure)
25	TCP	SMTP	Email sending
53	TCP/UDP	DNS	Domain Name System
67-68	UDP	DHCP	Dynamic Host Config
80	TCP	HTTP	Web (unencrypted)
110	TCP	POP3	Email retrieval
143	TCP	IMAP	Email retrieval
443	TCP	HTTPS	Web (encrypted)
3389	TCP	RDP	Remote Desktop

Color Key

TCP UDP Both

Exam Tip

Memorize these ports! They appear frequently on the Network+ exam.

The netstat Command

What is netstat?

netstat displays active connections, listening ports, and network statistics.

Common Options

`-a`	Show all connections
`-n`	Numeric (no DNS)
`-t/-u`	TCP/UDP only
`-l`	Listening ports only
`-p`	Show process ID

Security Use

Identify suspicious connections or unexpected services.

Sample Output

Proto	Local	Foreign	State
tcp	0.0.0.0:22	*:*	LISTEN
tcp	0.0.0.0:80	*:*	LISTEN
tcp	10.0.0.5:443	52.1.2.3:54321	ESTAB
udp	0.0.0.0:53	*:*	

Reading Output

- **LISTEN**: Waiting for connections
- **ESTABLISHED**: Active session
- **0.0.0.0**: All interfaces

DHCP Overview

The Problem

Manually configuring IP addresses on every device doesn't scale. Imagine a network with 500 devices!

The Solution: DHCP

Dynamic Host Configuration Protocol automatically assigns:

- IP address
- Subnet mask
- Default gateway
- DNS server addresses

Key Details

Uses **UDP ports 67** (server) and **68** (client). Client-server model with lease-based addressing.

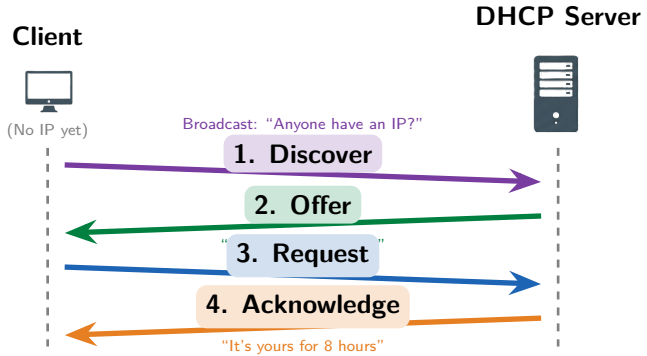
Without DHCP

Configure each manually?

With DHCP

Automatic!

DHCP DORA Process



Memory Trick

DORA the Explorer finds IP addresses!

Lease Time

IP is "rented" for a set period. Client must renew before expiration.

DHCP Server Configuration

Scope (Address Pool)

A **scope** defines the range of IP addresses the DHCP server can assign.

Start IP	192.168.1.100
End IP	192.168.1.200
Subnet	255.255.255.0
Available	101 addresses

Required Settings

- **IP range**: Start and end addresses
- **Subnet mask**: Network size
- **Default gateway**: Router IP
- **DNS servers**: Name resolution
- **Lease time**: How long to keep IP

Lease Duration

- Typical: 8 hours to 8 days
- Short leases: Mobile environments
- Long leases: Stable networks
- Client renews at 50% of lease time

Best Practice

Leave some addresses outside the scope for static assignments (servers, printers, routers).

DHCP Options

Common DHCP Options

Option	Name	Purpose
1	Subnet Mask	Network size
3	Default Gateway	Router address
6	DNS Servers	Name resolution
15	Domain Name	DNS suffix
51	Lease Time	Duration in seconds
66	TFTP Server	Boot server
150	VoIP Server	Phone config

Vendor Options

Options 43 and 60 allow vendor-specific settings for specialized devices.

How Options Work

DHCP options are sent with the Offer and Acknowledge messages.

Client receives:

- IP: 192.168.1.100
- Mask: 255.255.255.0
- Gateway: 192.168.1.1
- DNS: 8.8.8.8

NTP Option

Option 42 provides time servers—critical for authentication!

DHCP Reservations and Exclusions

Reservations

A **reservation** binds a specific IP to a MAC address. The device always gets the same IP.

Use for:

- Servers
- Network printers
- Security cameras
- VoIP phones

Reservation Example

MAC: `AA:BB:CC:11:22:33`
Reserved IP: `192.168.1.50`

Exclusions

An **exclusion** removes addresses from the DHCP pool. These IPs will never be assigned.

Use for:

- Statically configured devices
- Router interfaces
- Addresses already in use

Key Difference

Reservation: DHCP assigns specific IP to specific MAC.
Exclusion: DHCP never touches these IPs.

DHCP Relay and IP Helper

The Problem

DHCP Discover is a **broadcast**. Broadcasts don't cross routers! How do remote subnets get DHCP?

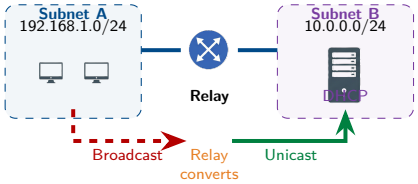
The Solution

DHCP Relay (IP Helper) forwards DHCP broadcasts to a remote server as unicast.

```
ip helper-address 10.0.0.5
```

Configure On

The router interface facing the clients (not the server).



Result

One DHCP server can serve multiple subnets through relay agents.

Case Study: Batgirl & Alfred

▶ Case Study: The Wayne Manor Network Problem

Batgirl installed new training equipment in the Wayne Manor gym (**VLAN 30**). All devices are getting `169.254.x.x` addresses! The DHCP server is on **VLAN 10** and works fine there.

VLAN	Subnet	Purpose
VLAN 10	192.168.10.0/24	Main house (DHCP here)
VLAN 30	192.168.30.0/24	Gym (problem devices)

Review Questions

1. What does the 169.254.x.x address indicate?
2. Why can't devices on VLAN 30 reach the DHCP server?
3. What solution would fix this problem?

Case Study Solution: Batgirl & Alfred

✓ Solution: The Wayne Manor Network Problem

1. **169.254.x.x** = APIPA address. DHCP failed, device assigned link-local IP.
2. **DHCP broadcasts don't cross VLANs/subnets**. The router blocks them.
3. Configure **DHCP Relay** on VLAN 30's router interface:
   `ip helper-address 192.168.10.5`

Key Lesson

"Even the Bat-family needs proper network configuration, Miss Barbara." — Alfred.
DHCP relay enables centralized DHCP across multiple subnets.

APIPA: Automatic Private IP Addressing

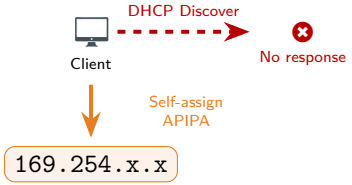
What is APIPA?

When DHCP fails, devices assign themselves an IP from the **169.254.0.0/16** range.

- Automatic fallback mechanism
- Link-local addresses only
- No gateway, no DNS
- Can only talk to local subnet

Symptom Alert

If you see `169.254.x.x`, DHCP is broken! Check server, network path, or relay.



Limited Connectivity

APIPA devices can communicate with each other but cannot reach the internet or other subnets.

DHCP Troubleshooting

Common DHCP Issues

- **Server down**: Service stopped
- **Scope exhausted**: No IPs left
- **Wrong VLAN**: Client isolated
- **Firewall blocking**: Ports 67/68
- **Rogue DHCP**: Unauthorized server
- **Relay missing**: Cross-subnet issue

Troubleshooting Commands

Windows:

- `ipconfig /release`
- `ipconfig /renew`
- `ipconfig /all`

Linux:

- `dhclient -r` (release)
- `dhclient` (renew)
- `ip addr show`

Rogue DHCP

Unauthorized DHCP servers can give wrong IPs, gateways, or DNS—security risk!

Quick Check

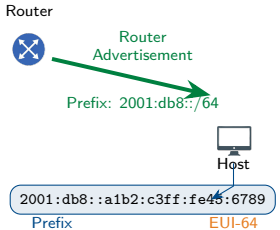
Got 169.254.x.x? $\rightarrow$ DHCP failed
Got 0.0.0.0? $\rightarrow$ No address assigned

IPv6 SLAAC: Stateless Address Autoconfiguration

What is SLAAC?

SLAAC lets IPv6 hosts configure themselves **without a DHCP server**.

1. Router sends **prefix** (RA)
2. Host generates **interface ID**
3. Combines: prefix + interface ID
4. Result: Full IPv6 address



EUI-64

Interface ID created from MAC address:

- Insert `FF:FE` in middle
- Flip 7th bit

No Server Needed

SLAAC is truly stateless—router just advertises prefix, host does the rest!

DHCPv6: IPv6 Address Assignment

DHCPv6 Modes

Stateful DHCPv6:

- Server assigns full address
- Tracks leases like DHCPv4
- Full control over addressing

Stateless DHCPv6:

- SLAAC provides address
- DHCPv6 provides options only
- DNS, NTP, domain name

Router Advertisement Flags

M flag Managed (use DHCPv6)
O flag Other (get options)

M	O	Result
0	0	SLAAC only
0	1	SLAAC + DHCPv6 options
1	0	Stateful DHCPv6
1	1	Stateful + options

Key Difference

DHCPv4 uses broadcast; DHCPv6 uses multicast (ff02::1:2).

DNS: The Internet's Phone Book

The Problem

Humans remember **names**, computers use **numbers**.

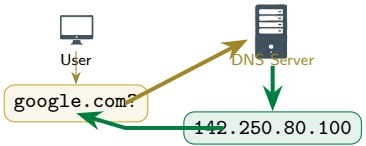
Which is easier to remember?

- `www.google.com`
- `142.250.80.100`

The Solution: DNS

Domain Name System translates names to IP addresses (and vice versa).

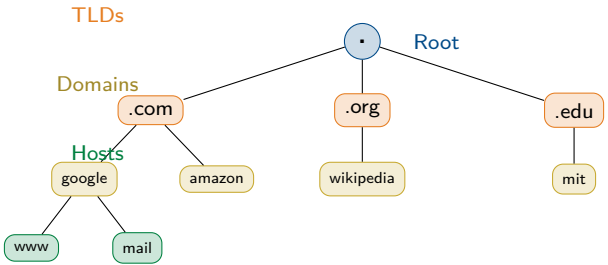
- Uses **UDP port 53** (queries)
- Uses **TCP port 53** (zone transfers)
- Hierarchical, distributed database



Critical Service

Without DNS, you'd need to memorize IP addresses for every website!

DNS Hierarchy



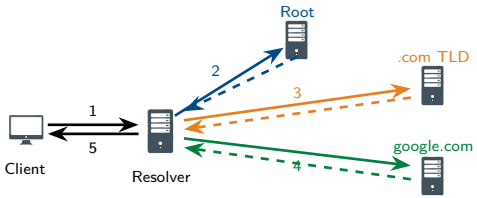
FQDN Example

`www.google.com.`
Host.Domain.TLD.Root

13 Root Servers

Named A through M, distributed globally with anycast.

DNS Name Resolution Process



Resolution Steps

1. Client asks resolver
2. Resolver asks root → "Try .com"
3. Resolver asks .com → "Try google.com NS"
4. Resolver asks google.com → IP!
5. Resolver returns IP to client

Caching

Results cached based on **TTL** (Time To Live).
Reduces repeated lookups!

DNS Records: A, AAAA, CNAME

A Record (Address)

Maps hostname to **IPv4** address.

```
www.example.com.  IN A 93.184.216.34
```

AAAA Record (Quad-A)

Maps hostname to **IPv6** address.

```
www.example.com.  IN AAAA
2606:2800:220:1::248
```

Memory Tip

AAAA = 4 A's = IPv**4** $\times$ **4** = IPv6 (4$\times$ longer)

CNAME Record (Alias)

Creates an **alias** pointing to another name (not an IP).

```
mail.example.com.  IN CNAME
  mailserver.example.com.
```

Use cases:

- Multiple names $\rightarrow$ same server
- CDN redirects
- Service migrations

CNAME Rule

CNAME cannot coexist with other records for the same name.

DNS Records: MX, SRV, TXT, PTR

Record Types

Type	Purpose	Example
MX	Mail server routing	`example.com. MX 10 mail.example.com.`
SRV	Service location	`_sip._tcp.example.com. SRV 10 5 5060 sip.example.com`
TXT	Text data (SPF, DKIM)	`example.com. TXT "v=spf1 include:_spf.google.com"`
PTR	Reverse lookup (IP→name)	`34.216.184.93.in-addr.arpa. PTR www.example.com.`

MX Priority

Lower number = higher priority.
MX 10 tried before MX 20.

PTR for Email

Many mail servers require valid PTR records to accept email (anti-spam).

DNS Server Configuration

Zone Types

- **Primary**: Read-write, authoritative
- **Secondary**: Read-only copy
- **Forward**: Passes queries elsewhere
- **Reverse**: IP-to-name lookups

Zone Transfers

- **AXFR**: Full transfer
- **IXFR**: Incremental
- Uses TCP port 53

Internal vs External DNS

Internal: Resolves private hostnames, not internet-accessible.

External: Public records (www, mail) hosted by registrar.

Split DNS

Different answers for internal vs external queries—security best practice.

Restrict Transfers

Only allow zone transfers to authorized secondary servers!

Case Study: Catwoman & The Riddler

▶ Case Study: The Suspicious Bank Website

Catwoman is accessing `gotham-bank.com` but the site looks off and asks for extra info. She runs `nslookup`:

```
Name:     gotham-bank.com
Address:  10.66.6.66
```

The real bank IP should be `203.0.113.50`. She suspects The Riddler.

Review Questions

1. What type of attack is this?
2. How could Riddler have accomplished this?
3. How can Catwoman fix and prevent this?

Case Study Solution: Catwoman & The Riddler

✓ Solution: The Suspicious Bank Website

1. **DNS Cache Poisoning** (or DNS Spoofing)—fake DNS records redirect to malicious site.
2. Riddler could have: poisoned her local DNS cache, compromised the router's DNS, or set up a rogue DNS server.
3. **Fix**: Flush DNS cache, verify DNS server settings, use secure DNS (DoH/DoT), check with external DNS (8.8.8.8).

Flush DNS Cache

```
Windows:  ipconfig /flushdns
Linux:  systemd-resolve -flush-caches
Mac:  sudo dscacheutil -flushcache
```

Verify with External DNS

```
nslookup gotham-bank.com 8.8.8.8
```

Key Lesson

"Curiosity and caution, darling." Always verify suspicious websites. DNS attacks can redirect you to convincing fakes!

DNS Troubleshooting Tools

nslookup

Basic DNS query tool (Windows/Linux/Mac).

```
nslookup google.com
nslookup -type=MX google.com
nslookup google.com 8.8.8.8
```

- Simple, quick lookups
- Specify record type
- Query specific server

dig (Domain Information Groper)

Advanced DNS tool (Linux/Mac).

```
dig google.com
dig google.com MX
dig +trace google.com
```

- Detailed output
- `+trace`: Show full resolution path
- `+short`: Minimal output

Troubleshooting Steps

1. Check local DNS settings (`ipconfig /all`) → 2. Query local resolver → 3. Query external DNS (8.8.8.8) → 4. Compare results

Module 6.0 Summary I

Key Concepts:

- **TCP** (Transmission Control Protocol): Reliable, connection-oriented, with error checking and retransmission. Use for data integrity.
- **UDP** (User Datagram Protocol): Fast, connectionless, no delivery guarantees. Use for real-time applications (VoIP, streaming).
- **Ports** identify services (0–65535): Well-known (0–1023), Registered (1024–49151), Dynamic (49152–65535).
- **Socket** = IP address + port number. Use **netstat** to view active connections.
- **DHCP** automates IP configuration via **DORA**: Discover, Offer, Request, Acknowledge.
- **DHCP scope**: Range of assignable IPs. **Reservation**: permanent assignment for specific MAC. **Options**: gateway, DNS servers, lease time.
- **DHCP relay agent** forwards DHCP messages across subnets (uses broadcast-to-unicast conversion).

Module 6.0 Summary II

- **APIPA** (169.254.x.x/16): Automatic fallback when DHCP unavailable (link-local only, no routing).
- IPv6 **SLAAC** (Stateless): Auto-config using Router Advertisement (RA) + **EUI-64** (MAC-derived host portion).
- **DHCPv6**: Stateful (assigns addresses) or stateless (provides options only).
- **DNS** resolves names to IPs. Hierarchy: Root, TLD (Top-Level Domain), Domain, Host.
- DNS records: **A** (IPv4), **AAAA** (IPv6), **CNAME** (alias), **MX** (mail server), **PTR** (reverse lookup).
- Troubleshooting tools: **nslookup** (basic queries), **dig** (detailed analysis). Check cache poisoning, TTL issues, zone transfers.