BELL RINGER

From yesterday.

Take 60 seconds. Answer in your notebook or in the LMS quiz.

Q1. What is the difference between a hub and a switch?

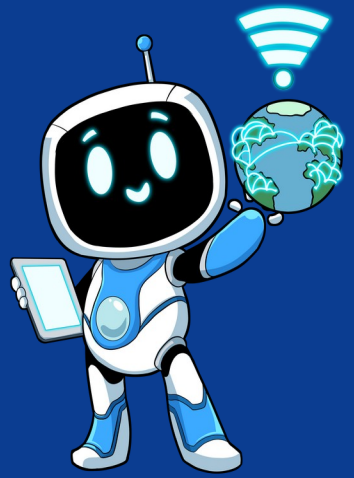
Q2. Name one device that uses MAC addresses to forward traffic.

Q3. True or false: a router operates at the same OSI layer as a switch.

A+ CORE 1 · DOMAIN 2: NETWORKING

LESSON 2.3

Ports & Protocols



TCP vs UDP, the well-known ports every tech needs cold, and how to use them to troubleshoot real tickets.

50-minute class · V15 objectives 2.1 + 2.4

Revy's Tech Journey

Today's path.

Five stops in 50 minutes. We're going to make ports feel obvious.

1	2	3	4	5
Bell ringer	**The big picture**	**TCP vs UDP**	**Well-known ports**	**Real tickets**
Yesterday in 60 sec	What ports actually are	Reliable vs fast	The list you memorize	Troubleshoot like a pro

0:00 - 0:05 · 0:05 - 0:15 · 0:15 - 0:25 · 0:25 - 0:40 · 0:40 - 0:50

WHY THIS MATTERS

Ports show up in every help desk ticket you'll triage on day one.

T1

Help desk tier 1

Half of "my internet's broken" tickets are really a blocked port. Knowing which service uses what port lets you triage in seconds.

NA

Network admin

Every firewall rule, ACL, and VPN tunnel is built on port numbers. You will write these from memory in five years.

CA

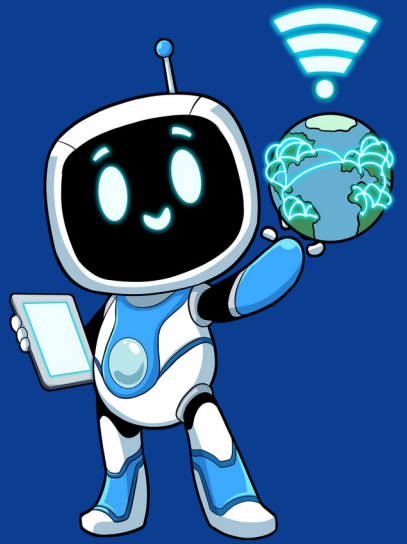
Cyber analyst

Threat hunting starts at "why is something talking on port 4444?" If you don't know the well-known ports cold, you can't spot the weird ones.

Section 1

The big picture.

What is a port? Why do we have 65,536 of them?



Think of an IP address as a building.

IP

The building

IP address

One address points to one server, one PC, one phone. Like a street address points to one building.

:443

The doors

Port number

A port number tells the building which door to send the visitor to. Each door connects to one service running inside.

The takeaway

An IP + port = a complete address. IP gets you to the device. Port gets you to the service.

Every building has 65,536 doors.

Port numbers run from 0 to 65,535. They split into three pools by job.

0 to 1023

Well-known

Reserved for standard services (HTTP, HTTPS, SSH, DNS). These are the ports you memorize for the A+.

1024 to 49151

Registered

Vendor-assigned (Stripe, Steam, custom apps). You meet these case-by-case.

49152 to 65535

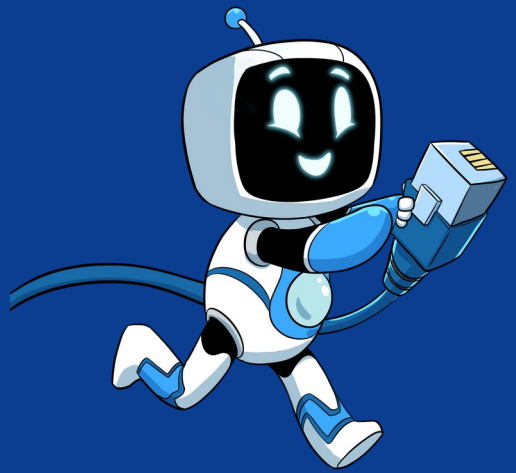
Dynamic / Ephemeral

Your OS picks one of these every time YOU make an outbound connection. Comes back, returns to pool.

Section 2

TCP vs UDP.

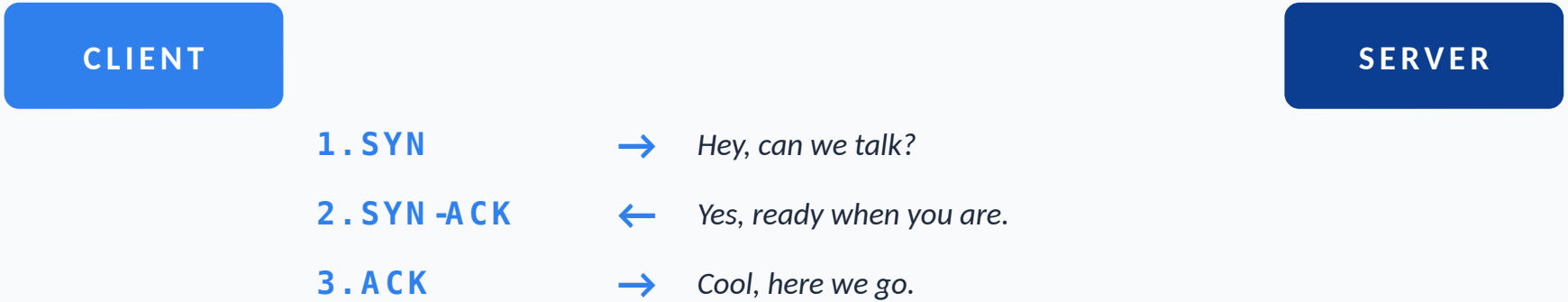
Reliable vs fast. Pick the right protocol for the job.



PROTOCOL 1

TCP. The careful conversation.

Transmission Control Protocol. Connection-oriented. Every packet acknowledged.



Used by:
Web (HTTP/HTTPS), email (SMTP/IMAP/POP3), file transfer (FTP/SFTP/SMB), remote desktop (RDP), secure login (SSH).

PROTOCOL 2

UDP. The yell into the void.

User Datagram Protocol. Connectionless. No handshake, no acknowledgment, no resend.

Faster. Less overhead. If a packet drops, it's gone.

Sometimes that is the right trade. Voice calls, video streams, DNS lookups, game data. Losing one packet matters less than getting the rest fast.

Used by:
DNS (53), DHCP (67/68), VoIP (voice calls), video streaming, online gaming.

So which one when?

Property	TCP	UDP
Connection model	Connection-oriented	Connectionless
Handshake	3-way (SYN, SYN-ACK, ACK)	None
Reliability	Guaranteed delivery + order	Best effort
Speed / overhead	Slower, more overhead	Faster, less overhead
Good for	**Web, email, file transfer, SSH**	**DNS, DHCP, VoIP, gaming, streaming**

Section 3

Well-known ports.

The list you memorize. Going to be on every exam you ever take.

Memorize these by Friday.

Tested on every A+ Core 1 attempt. Email ports + sharing detailed on slide 17.

Port	Protocol	Service	What it does
20 /21	TCP	FTP	File transfer (data / control)
22	TCP	SSH / SFTP	Secure shell, encrypted remote login + file transfer
23	TCP	Telnet	Unencrypted remote login. Do NOT use in production.
25	TCP	SMTP	Send email (server to server)
53	UDP/TCP	DNS	Resolve names to IPs. Mostly UDP, TCP for big responses.
67 /68	UDP	DHCP	Auto-assigns IP addresses (67 server, 68 client)
80	TCP	HTTP	Plaintext web traffic
443	TCP	HTTPS	Encrypted web (default since ~2018)
445	TCP	SMB	Windows file/printer sharing
3389	TCP	RDP	Remote Desktop to Windows

PORTS 80 + 443

The web's plumbing.

80

HTTP

Plaintext

Anyone on the wire can read what you're sending. Largely deprecated for anything sensitive. Still shows up on internal networks and legacy systems.

Avoid for any login or PII

443

HTTPS

Encrypted (TLS)

HTTP wrapped in TLS (Transport Layer Security, the modern encryption layer). Server proves its identity with a certificate, then everything is encrypted end-to-end.

Use this. Always.

PORTS 53 + 67/68

Foundation services. Almost always UDP.

53

DNS

You type: www.example.com

→ Your PC asks: "What's the IP?"

→ DNS server: "192.0.2.42"

→ Your PC connects to that IP

Port 53. UDP for normal lookups, TCP if response is too big.

67/68

DHCP

You plug in / connect WiFi

→ Your PC: "Anyone got an IP for me?" (port 68)

→ DHCP server: "Take 192.168.1.50" (port 67)

→ Your PC: "Thanks, I'll take it."

Port 67 server, 68 client. UDP. The reason your phone gets internet at every coffee shop.

ADMIN TOOLS

How techs reach machines that aren't in front of them.

22

SSH

Secure terminal access to Linux + macOS + network gear. Encrypted from the start. Standard for Linux server work.

3389

RDP

Remote Desktop to Windows. Full graphical session. Standard for Windows server + helpdesk work.

21

FTP

Legacy file transfer. Unencrypted. SFTP (over port 22) or FTPS (over 990) replaced it almost everywhere.

EMAIL + SHARING

Email + file sharing.

Email

25 SMTP
Send mail (server to server)

110 POP3
Download mail (older, single-device)

143 IMAP
Sync mail across devices (modern default)

587 SMTP Sub.
Send mail (client to server, authenticated)

993 IMAPS
IMAP over TLS

995 POP3S
POP3 over TLS

File + printer sharing

445 SMB
Windows file + printer sharing

139 NetBIOS
Older Windows file sharing

548 AFP
Apple File Protocol

631 IPP
Internet Printing Protocol

3306 MySQL
MySQL database (registered, but worth knowing)

1433 SQL Server
Microsoft SQL Server (registered)

COMMON MISTAKES

Where students lose points.

✗ DNS = TCP

✓ DNS = mostly UDP

DNS uses UDP/53 for normal lookups. TCP only for big zone transfers.

✗ Port 80 + 443 are different protocols

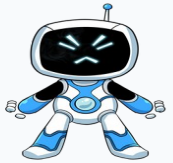
✓ Same protocol (HTTP), different encryption

443 is HTTP wrapped in TLS. Same web traffic underneath.

✗ Telnet is fine for internal devices

✓ Telnet is never fine

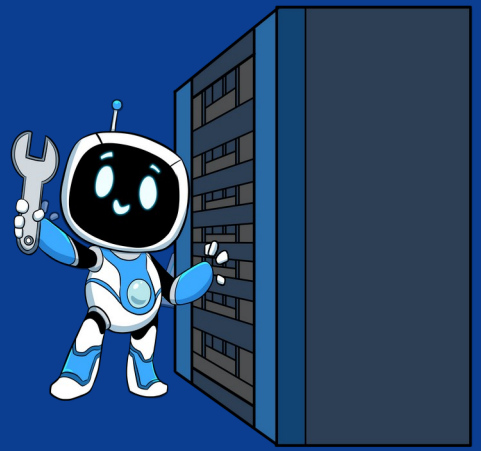
Plaintext credentials. Use SSH even on internal networks. Exam answer + real life.



Section 4

Real tickets.

Using ports to troubleshoot what's actually broken.



SCENARIO 1

"My internet's broken."

User can't reach amazon.com. Use what you know about ports to triage.

Step 1. **Can they reach 8.8.8.8 by IP?**	YES → DNS issue (port 53)	NO → Network issue (try ping gateway)
Step 2. **If reachable by IP, can they ping by name?**	YES → DNS works. Check browser, certs, or port 443.	NO → DNS broken. Check resolver, /etc/hosts, or DHCP.
Step 3. **Is port 443 blocked?**	YES → Firewall or proxy issue. Check corporate filter.	NO → Try port 80 (HTTP). If that works, TLS cert issue.

SCENARIO 2

"My email won't send."

They can RECEIVE email fine. SEND fails. Port-based diagnosis.

✓ RECEIVING works

That means inbound traffic on 143 (IMAP) or 993 (IMAPS) is fine. DNS resolves the mail server. Auth works. The user is connected.

So skip those checks. They're proven.

✗ SENDING fails

Sending uses different ports. Check, in order:

- Port 587 (SMTP submission, authenticated)
- Port 465 (SMTPS)
- Port 25 (server-to-server, often blocked on home ISPs)

The pattern

Ask which direction is failing. Then think in PORTS, not services. "Email" isn't one port; it's six.

TOOLS

Commands that show what's listening.

$ netstat -an

Windows / older Linux

List every open connection and listening port on this machine. Old school but every tech knows it.

$ ss -tuln

Modern Linux

Newer, faster replacement for netstat. TCP + UDP, listening, numeric.

$ nslookup

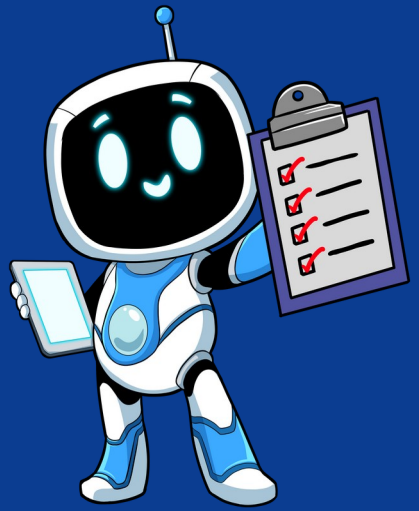
Cross-platform

Manually query DNS. Confirms if port 53 / DNS resolution is working.

Section 5

Lock it in.

Five takeaways. One exit ticket. See you tomorrow.



SUMMARY

Today's five things.

1. An IP gets you to the device. A port gets you to the right service on it.
2. TCP is reliable (3-way handshake). UDP is fast (no handshake). Pick by job.
3. HTTP=80, HTTPS=443, SSH=22, RDP=3389, DNS=53 (UDP), DHCP=67/68 (UDP), SMB=445.
4. Email isn't one port. SMTP=25, SMTP submission=587, IMAP=143, POP3=110.
5. Troubleshoot by asking: which direction is failing? Which port handles it?

EXIT TICKET

Before you go.

Answer three. Drop in the LMS or hand in on paper. Tomorrow we'll review.

1. **Name one well-known port and the service it runs.**

(any from today's list)

2. **What's the main difference between TCP and UDP?**

(handshake vs no handshake, reliable vs fast)

3. **What did you find tricky today? Write one sentence.**

(tomorrow's warm-up uses this)

TOMORROW

Lesson 2.4

Wireless standards. 802.11ax vs 802.11ac. Why your WiFi is slow.