NetForge-AI

Networking Course — Syllabus

Updated 2026-10-27 · netforge-ai.com/course/syllabus

A self-paced networking course that takes you from your first network to advanced, hands-on skills, entirely in the browser. 8 modules, 54 chapters and about 38 hours of study, each chapter with a short quiz and many with a hands-on lab, ending in the Final Weighted Exam and a Verified Certificate.

8	54	~38h	33	435
MODULES	CHAPTERS	STUDY TIME	HANDS-ON LABS	PRACTICE QUESTIONS

How each chapter works

- Read — a short, focused chapter with its learning objectives up front. ARIA, the AI tutor, can read it aloud.
- Build — 33 chapters open a hands-on lab in the browser-based simulator, 30 of them as a step-by-step guided build that checks your network as you go.
- Quiz — every chapter ends with a short quiz — four questions, three right passes it (the final mixed practice set has thirty) — and most add optional extra practice: 435 questions across the course, marked as you answer.
- Prove it — finish every chapter, then pass the 60-question Final Weighted Exam to earn the Verified Certificate.

What the course gives you

+ A complete path from beginner to advanced: how networks work, addressing and subnetting, routing, switching and the LAN, network services, security and automation, then a final review.
+ Hands-on practice with no hardware and nothing to install: 33 chapters include a lab in a browser-based simulator with an industry-standard CLI, and 30 open a guided build checked live.
+ 435 practice questions — a short quiz in every chapter plus optional extra practice — marked as you answer, so you know what to review.
+ ARIA, the AI tutor, reads every chapter aloud with the words highlighted as she goes.
+ A 60-question Final Weighted Exam and, when you pass it, a Verified Certificate anyone can check online.
+ About 38 hours of study, at your own pace — most learners spread it over 6–10 weeks.

What it does not give you

- It is not an official vendor or certification-body credential. NetForge-AI is an independent educational platform, not affiliated with, endorsed by or sponsored by any networking vendor or certification body; the Verified Certificate is NetForge-AI's own.
- No physical equipment. The labs run in a simulator; some technologies are taught in the chapters but not simulated in the lab — for example site-to-site VPNs and IPsec, HSRP and GLBP (VRRP is simulated), 802.1X with RADIUS or TACACS+, wireless LAN controllers, QoS policies, MPLS and BGP — and cable-level faults such as signal loss are not modelled.
- It is not instructor-led: there are no live classes or human graders. (Lecturers can teach their own class on

NetForge-AI, with live sessions, assignments and a gradebook.)

- ARIA's answers to your questions inside the chapters come with All-Access Max, or with your own AI provider's API key on any plan; they are not included in the Course & Lab Pass.

Who it's for

- Students starting out — no prior networking experience needed.
- Career changers who want job-ready, hands-on networking skills.
- Lecturers and instructors who want a ready-made course with real labs for their class.
- Anyone preparing for a networking exam who learns best by doing.

Modules and chapters

MODULE 1 — 8 chapters · 4h 30m · 14% of the exam · free with an account

How Networks Work

How packets travel — from cables to the OSI model.

1.1 What is a network? — Beginner · 40 min · guided lab
- Define host, node, link, address, and protocol in plain language.
- Identify the four physical components that make any network possible.
- Trace, at a high level, how a packet moves between two hosts on the same LAN.

1.2 The OSI and TCP/IP models — Beginner · 40 min · guided lab
- List the seven OSI layers in order, top down and bottom up.
- Map each OSI layer to its equivalent TCP/IP layer.
- Place common protocols (HTTP, TCP, IP, Ethernet, Wi-Fi) on the correct layer.

1.3 Cabling, interfaces, and the physical layer — Beginner · 25 min
- Choose the right cable category for a given speed and distance.
- Distinguish single-mode from multi-mode fiber and explain when to use each.
- Identify common interface types: RJ-45, SFP, SFP+, QSFP, console.

1.4 When a link misbehaves — counters, duplex and speed — Intermediate · 40 min · guided lab
- Identify duplex mismatch from interface counters.
- Distinguish collisions, runts, giants, and CRC errors.
- Decide when to set speed/duplex statically vs auto.

1.5 Devices and the shapes networks take — Beginner · 30 min
- Describe the role of each common network device kind.
- Compare the two-tier collapsed-core and three-tier hierarchical designs.
- Explain spine-leaf data center topology and where it fits.

1.6 TCP, UDP, and well-known ports — Beginner · 30 min
- Describe the TCP three-way handshake and connection teardown.
- Explain when an application chooses UDP over TCP.
- Memorize the well-known ports for HTTP, HTTPS, SSH, DNS, DHCP, SMTP, FTP, Telnet, NTP, SNMP.

1.7 The host's own view — checking IP settings on any OS — Beginner · 40 min · guided lab
- Read IPv4/IPv6 address, mask, and gateway on Windows.
- Read the same on macOS and Linux.
- Spot APIPA (169.254.x.x) and what it tells you.

1.8 Networks inside one box — VMs, containers and VRFs — Intermediate · 25 min
- Compare a VM and a container in terms of isolation and overhead.
- Explain what a hypervisor does (Type 1 vs Type 2).
- Describe a VRF and when an enterprise uses one.

MODULE 2 — 6 chapters · 4h 40m · 14% of the exam

Addresses and Subnets

Prefix length, the magic number, VLSM, and IPv6.

2.1 IPv4 address structure

Beginner · 40 min · guided lab

- Convert between dotted decimal and binary for any /8 boundary.
- Explain why classful addressing was replaced by CIDR.
- Describe what the prefix length actually counts.

2.2 Subnet masks and prefix length

Beginner · 50 min · guided lab

- Convert any /n prefix to its dotted-decimal mask without a calculator.
- Compute usable hosts for any prefix in two seconds.
- Recognize /30, /31, and /32 by use case.

2.3 Subnetting in your head — the 5-step method

Beginner · 45 min · guided lab

- Find the network and broadcast for any IP/mask combination.
- Count usable hosts and list the first/last usable IP.
- Apply the method quickly against a practice set.

2.4 VLSM and address planning

Intermediate · 45 min · guided lab

- Design a VLSM plan for an organization with mixed subnet sizes.
- Justify the order in which subnets are allocated.
- Detect overlapping or wasteful allocations in a given plan.

2.5 Private addresses, special blocks, and NAT preview

Beginner · 45 min · guided lab

- Identify the three RFC 1918 private ranges.
- Recognize loopback, link-local, multicast, and TEST-NET addresses.
- Explain at a high level why private addresses require NAT to reach the public Internet.

2.6 IPv6 fundamentals

Intermediate · 55 min · guided lab

- Compress and expand any IPv6 address using the :: shorthand rules.
- Distinguish global unicast, unique local, link-local, multicast, and anycast.
- Describe SLAAC and how a host self-configures an IPv6 address.

MODULE 3 — 5 chapters · 4h 45m · 15% of the exam

Routing Between Networks

Get packets from one network to the next: static routes, OSPF, and a gateway that survives failure.

3.1 How a router forwards a packet

Beginner · 60 min · guided lab

- Describe the per-packet process inside a router.
- Explain longest-prefix match and why it overrides administrative distance.
- Read 'show ip route' output cleanly.

3.2 Routes you write by hand — static, default and backup

Intermediate · 55 min · guided lab

- Configure a next-hop static route and an exit-interface static route.
- Configure a default route and an IPv6 default route.
- Configure a host route (/32 or /128).
- Use a floating static route as a backup to a dynamic protocol.

3.3 OSPF in a single area

Intermediate · 60 min · guided lab

- Configure OSPFv2 in a single area with the network and router-id commands.
- Explain Hello/Dead timers and the conditions for adjacency.
- Identify when DR/BDR is elected and when it is bypassed.

3.4 Administrative distance and metrics

Intermediate · 55 min · guided lab

- Recite the default AD for connected, static, OSPF, EIGRP, RIP, and external BGP.
- Compare metric calculations between OSPF (cost) and RIP (hop count).

3.5 A gateway that survives failure — HSRP, VRRP and GLBP

Intermediate · 55 min · guided lab

- Explain why endpoints need a redundant first hop.
- Compare HSRP, VRRP, and GLBP feature by feature.
- Configure VRRP for a master/backup pair.

MODULE 4 — 9 chapters · 6h 25m · 20% of the exam

Building the LAN

Everything that happens at Layer 2 inside a building — switching, VLANs, spanning tree, and Wi-Fi.

4.1 Ethernet, MAC tables, and switching

Beginner · 45 min · guided lab

- Describe the format of an Ethernet II frame.
- Walk through how a switch learns and populates its MAC address table.
- State the three forwarding outcomes: forward, flood, drop.

4.2 VLANs and access ports

Beginner · 45 min · guided lab

- Create and name VLANs in the VLAN database.
- Assign an access port to a VLAN and verify with show vlan brief.
- Explain the default behaviour of unassigned switch ports.

4.3 802.1Q trunking

Intermediate · 45 min · guided lab

- Describe the 802.1Q tag format and the role of the native VLAN.
- Configure a trunk and restrict its allowed VLAN list.
- Diagnose a native-VLAN mismatch.

4.4 Inter-VLAN routing

Intermediate · 45 min · guided lab

- Configure router-on-a-stick with subinterfaces and 802.1Q encapsulation.
- Configure SVIs on an L3 switch and enable ip routing.
- Choose between router-on-a-stick and L3 switch for a given scale.

4.5 Spanning-Tree Protocol (STP & RSTP)

Intermediate · 55 min · guided lab

- Explain why L2 loops are catastrophic and how STP prevents them.
- Identify the Root Bridge from a set of Bridge IDs.
- Compare STP, PVST+, RPVST+, and MST.
- Use PortFast and BPDU Guard correctly on access ports.

4.6 EtherChannel — link aggregation

Intermediate · 40 min · guided lab

- Describe the benefits of EtherChannel over independent links.
- Configure an LACP EtherChannel between two switches.
- Identify which interface settings must match on both sides.

4.7 Wireless LAN fundamentals

Beginner · 50 min · guided lab

- Distinguish autonomous AP, lightweight AP + WLC, and cloud-managed AP architectures.
- Explain SSID, BSSID, and ESSID.
- Describe non-overlapping 2.4 GHz channels and the role of 5/6 GHz bands.

4.8 Controller-based Wi-Fi — where the tunnel ends

Intermediate · 25 min

- Split 802.11 responsibilities between a controller-based AP and its controller.
- Describe the CAPWAP control and data tunnels and the ports they use.
- Match a requirement to a radio role: serve clients (centrally or locally switched), monitor the air, capture frames, or carry mesh backhaul.
- Decide whether a given AP needs an access port or an 802.1Q trunk, and say why.
- Describe how a controller attaches to the wired network: a management address, client VLANs on a trunked uplink, an optional out-of-band port, and link aggregation.
- Plan 2.4 GHz channels and 5 GHz channel widths for coverage versus capacity.

4.9 CDP and LLDP — Layer 2 discovery

Beginner · 35 min · guided lab

- Enable and disable CDP and LLDP globally and per-interface.
- Read 'show cdp/lldp neighbors' output.
- Decide when to disable discovery for security.

MODULE 5 — 6 chapters · 4h 45m · 14% of the exam

Running the Network

DHCP, NAT, DNS, NTP, SNMP, syslog, SSH, file transfer, and QoS.

5.1 DHCP — server, relay, and client

Intermediate · 55 min · lab

- List the four DHCP messages in order: Discover, Offer, Request, Acknowledge.
- Configure a DHCP pool on a router.
- Explain when ip helper-address is required.

5.2 NAT and PAT

Intermediate · 50 min · lab

- Compare static NAT, dynamic NAT, and PAT.
- Identify the inside/outside interface roles.
- Configure PAT on a router for an entire LAN.

5.3 DNS, NTP, SNMP, and Syslog

Intermediate · 60 min · guided lab

- Configure a router with DNS resolvers and an NTP server.
- Describe SNMPv2c vs SNMPv3 differences.
- Set up syslog to a remote collector.

5.4 SSH and secure management

Beginner · 55 min · guided lab

- Generate an RSA key pair for SSH.
- Configure local username/password and apply to VTY.
- Disable Telnet on VTY lines.

5.5 TFTP and FTP — moving files to and from a router

Beginner · 30 min

- Compare TFTP and FTP on ports, transport, auth, and reliability.
- Back up a running-config to a TFTP server.
- Restore a firmware image from FTP.

5.6 QoS fundamentals

Advanced · 35 min

- Explain why QoS only matters during congestion.
- Identify common DSCP values: EF, AF41, CS6, default.
- Describe the role of marking, queueing, and policing.

MODULE 6 — 6 chapters · 4h 10m · 13% of the exam

Securing the Network

Threats, AAA, awareness and physical control, ACLs, port security, VPNs, wireless.

6.1 Threats, AAA, and 802.1X

Intermediate · 30 min

- Define threat, vulnerability, exploit, and attack vector.
- Explain AAA's three components and the role of RADIUS and TACACS+.
- Describe 802.1X's three roles: supplicant, authenticator, authentication server.

6.2 Security beyond the config — people, locks and passwords

Beginner · 45 min · guided lab

- Explain why users are the dominant attack surface, and describe what a working awareness program contains and measures.
- Justify physical access control as a network security control — starting with why console access defeats every logical control on the device.
- Apply current password-policy guidance: length over composition, blocklist screening, rotation only on evidence of compromise, salted slow-hash storage.
- Distinguish the three authentication factor categories, and place certificate-based authentication and biometrics alongside their failure modes.

6.3 Port security and DHCP snooping

Intermediate · 50 min · guided lab

- Configure port security with sticky MAC learning.
- Enable DHCP snooping and mark trusted ports.
- Explain how DAI builds on the snooping binding table.

6.4 Standard and Extended ACLs

Intermediate · 60 min · lab

- Write a numbered standard ACL and apply it to an interface.
- Write a numbered or named extended ACL with protocol/port matches.
- Explain the implicit deny and the importance of order.

6.5 Private tunnels across public networks — VPNs

Advanced · 25 min

- Compare site-to-site and remote-access VPN use cases.
- List the four IPsec services: confidentiality, integrity, authentication, anti-replay.
- Describe SSL VPN's advantage over IKEv2 for remote users.

6.6 Wireless security — WPA2 vs WPA3

Intermediate · 40 min · guided lab

- Describe the difference between WPA2-Personal and WPA2-Enterprise.
- List the security improvements WPA3 makes over WPA2.
- Recognize when 802.1X is in use.

MODULE 7 — 7 chapters · 3h · 10% of the exam

Automating the Network

APIs and data formats, controllers, configuration as code, AI in operations, change pipelines, and YANG device APIs.

7.1 Why automate networks?

Beginner · 25 min

- Spot the four ways hand-typed changes go wrong at scale — drift, delay, no audit trail, copy-paste mistakes.
- Define configuration management, infrastructure as code, and intent-based networking.
- Recognize the trade-off between flexibility and consistency.

7.2 REST APIs, JSON, and YAML

Intermediate · 35 min

- Read and modify a small JSON document.
- Read a YAML file and understand its mapping/list syntax.
- Identify HTTP verbs and status codes used in REST.

7.3 Controllers, SDN, and intent-based networking

Advanced · 25 min

- Define the control plane and data plane and where SDN moves the control plane.
- Compare northbound and southbound APIs.
- Recognize SDN controllers and software-defined fabrics at a high level.

7.4 Configuration as code — push, pull and plan

Intermediate · 30 min

- Identify each tool's transport model and language.
- Recognize a small Ansible playbook.

7.5 AI on the operations desk — prediction and assistants

Intermediate · 25 min

- Differentiate generative AI from predictive AI/ML.
- Cite at least three netops use cases for each.
- Recognise the operational and security risks of letting an AI touch production.

7.6 Source of truth and change pipelines

Advanced · 20 min

- Explain what a source of truth is, and why it holds the intended state rather than the configuration running on the devices.
- Use the Git vocabulary of a network change: commit, branch, pull request, review, history and revert.
- Put the stages of a change pipeline in order and say what each one catches: peer review, CI checks, an approved deploy, post-change verification and rollback.
- Explain how a template and its variables render device configuration, so that the data is what gets reviewed.
- Detect configuration drift by comparing rendered intended configuration with running configuration, and choose what to do with each difference.

7.7 Data models and device APIs: YANG, NETCONF, RESTCONF and XML

Advanced · 20 min

- Explain why scripts that screen-scrape CLI output break, and what a data model fixes.
- Read a small YANG model: module, container, list, key and leaf, and tell configuration data from state data.
- Describe a NETCONF change: SSH on port 830, get, get-config and edit-config, and the candidate and running datastores with lock and commit.
- Build and read a RESTCONF request: the URL that mirrors the YANG path, the HTTP method, and the JSON or XML media types.

- Compare the CLI, SNMP, NETCONF, RESTCONF and streaming telemetry, and choose one for a given job.

MODULE 8 — 7 chapters · 5h 30m · review module

Final Review

Cheat sheets, drills, an area-by-area review, exhibit practice, and your Final Weighted Exam game plan.

8.1 The 50-command cheat sheet — Intermediate · 35 min
- Recall the most-used CLI commands without prompting.
- Recognize each command's mode and purpose.

8.2 Subnetting drills with worked answers — Intermediate · 50 min · guided lab
- Subnet quickly under time pressure.
- Recognize trick wording around 'usable' vs 'total' addresses.

8.3 Full enterprise lab walkthrough — Advanced · 105 min · guided lab
- Build a multi-site topology end to end without referring to the cheat sheet.
- Verify reachability layer by layer.
- Save and load the topology as a NetForge-AI JSON file.

8.4 Final Weighted Exam strategy — Beginner · 5 min
- Allocate time across question types correctly.
- Decide when to flag and skip a question.
- Read an exhibit before the options, and answer from the evidence rather than from memory.

8.5 Area-by-area review — Advanced · 45 min
- State the key facts of each of the seven topic areas without looking them up.
- Read the decisive output for each area and name the line that answers the question.
- Recognise and correct the most common misconceptions in each area.
- Use the area scores on your results page to decide what to revise next.

8.6 Reading the exhibit — Advanced · 40 min
- Apply a fixed method to an exhibit question: read the question first, find the one line that decides it, and ignore the rest.
- Name the deciding line in each of the common show outputs, and in a protocol ladder.
- Recognise the classic misreading of each output before it costs a mark.

8.7 Mixed practice set — Advanced · 50 min
- Answer 30 mixed questions from all seven topic areas at the exam's pace.
- Read show output, captures and ladders under time pressure.
- Trace every miss back to the chapter that teaches it, and close the gap before the exam.

Final Weighted Exam and certificate

- 60 questions in 105 minutes, drawn from all 7 teaching modules and weighted by each module's share of the course.
- To pass: 70% overall and at least 1 in 3 right in every topic area.
- It unlocks once every chapter is complete. Passing it earns the Verified Certificate, checkable online by its serial number.

Access

- Module 1 is free with an account.
- The full course — every module, the Final Weighted Exam and the Verified Certificate — comes with the Course & Lab Pass or All-Access Max.
- ARIA in every chapter is included with All-Access Max; with your own AI provider's API key it works on any

plan.

NetForge-AI is an independent educational platform and is not affiliated with, endorsed by, or sponsored by any networking vendor or certification body.