16 NETWORK ENGINEERING PROJECTS

The 6 from the video plus 10 more, every one built with free tools. Each project gives you:

- The lab layout with every address
- Step-by-step build with the exact commands
- How to check it works, and what you should see
- What to do when it breaks
- An interview question you can now answer
- A line for your resume

START HERE

Make a free NetAcad account and download Cisco Packet Tracer. That one tool covers projects 1, 2, 5, 7, 8, 9 and 12.

`netacad.com`

THE 16 PROJECTS

Pick one, build it, post it

Tap a project to jump to it. Every link in this guide is tappable.

#	Project	Time	Level	Main tool
01	Multi-Site Office Network	2 to 3 hours	Beginner	Packet Tracer
02	Break-and-Fix Troubleshooting Lab	2 hours	Beginner	Packet Tracer
03	Segmented Home Lab + Own DNS	3 to 4 hours	Intermediate	VirtualBox
04	Decode a Real Capture	1 to 2 hours	Beginner	Wireshark
05	Follow a Packet End to End	1.5 hours	Beginner	Packet Tracer
06	Config Backup Bot	3 hours	Intermediate	Modeling Labs Free
07	Redundant Gateway with HSRP	1 hour	Intermediate	Packet Tracer
08	ACL Security Policy	1.5 hours	Intermediate	Packet Tracer
09	Edge Router: DHCP + NAT	1.5 hours	Intermediate	Packet Tracer
10	Site-to-Site IPsec VPN	2 hours	Advanced	Modeling Labs Free
11	Network Monitoring Dashboard	2 hours	Intermediate	LibreNMS
12	IPv6 Dual-Stack Upgrade	1.5 hours	Intermediate	Packet Tracer
13	IP Address Plan with VLSM	1 hour	Beginner	A spreadsheet
14	BGP Between Three "ISPs"	2 hours	Advanced	Modeling Labs Free
15	Network Documentation Pack	2 hours	Beginner	draw.io
16	Ansible Config Push	2 to 3 hours	Advanced	Ansible

Projects 1 to 6 are the ones from the video. 7 to 16 are the next level.

HOW TO SHOW IT ON YOUR RESUME

One GitHub repo per project, with this layout. Recruiters and interviewers open the README first.

```
project-01-multi-site-office/
  README.md        what you built, why, the diagram
  diagram.png      from project 15
  configs/         every device config
  screenshots/     the "check it works" results
  LESSONS.md       what broke and how you fixed it
```

Then put the resume line from the end of each project on your resume and LinkedIn, with the repo link.

PROJECT 01 / ROUTING & SWITCHING / FROM THE VIDEO

Multi-Site Office Network

You can build a small company network from scratch: VLANs, inter-VLAN routing and a routing protocol between two sites.

TIME 2 to 3 hours	**LEVEL** Beginner

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

LAB LAYOUT

Device	Interface	Address
R1 (Site A)	G0/0.10 Staff	`10.1.10.1 /24`
R1	G0/0.20 Guest	`10.1.20.1 /24`
R1	G0/1 to R2	`10.0.12.1 /30`
R2 (Site B)	G0/0.10 Staff	`10.2.10.1 /24`
R2	G0/0.20 Guest	`10.2.20.1 /24`
R2	G0/1 to R1	`10.0.12.2 /30`
PCs	Staff on Fa0/1-2, Guest on Fa0/3-4	`.11, .12 in each VLAN`

BUILD IT

01 Place the devices and cable them.

Per site: one 2911 router, one 2960 switch, 4 PCs. PCs to Fa0/1 to Fa0/4, switch G0/1 to router G0/0, R1 G0/1 to R2 G0/1.

02 Create the VLANs and put ports in them.

On each switch:

```
vlan 10
 name Staff
vlan 20
 name Guest
interface range fa0/1-2
 switchport mode access
 switchport access vlan 10
interface range fa0/3-4
 switchport mode access
 switchport access vlan 20
```

03 Trunk the uplink to the router.

The trunk carries both VLANs to the router on one cable.

```
interface g0/1
 switchport mode trunk
```

04 Route between VLANs with router-on-a-stick.

On R1 (use 10.2.x on R2):

```
interface g0/0
 no shutdown
interface g0/0.10
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
interface g0/0.20
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
```

05 Address the link between the sites.

R1 shown; R2 uses 10.0.12.2.

```
interface g0/1
 ip address 10.0.12.1 255.255.255.252
 no shutdown
```

06 Join the sites with OSPF area 0.

Same two lines on both routers. Every 10.x interface joins OSPF.

```
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

07 Give the PCs addresses.

PC > Desktop > IP Configuration. Static for now (project 9 adds DHCP). Example: 10.1.10.11, mask 255.255.255.0, gateway 10.1.10.1.

08 Save your work.

On every device, so a reload does not wipe it.

```
copy running-config startup-config
```

CHECK IT WORKS

Run or check	You should see
`show vlan brief`	Fa0/1-2 under VLAN 10, Fa0/3-4 under VLAN 20
`show interfaces trunk`	G0/1 listed as trunking
`show ip ospf neighbor`	the other router in state FULL
`show ip route`	lines starting with O for the other site's subnets
`ping 10.2.10.11 (from a Site A Staff PC)`	replies

IF IT BREAKS

Problem	Fix
PC cannot ping its own gateway	Check the PC port is in the right VLAN, the uplink is a trunk, and the router's physical G0/0 is not shut down.

Problem	Fix
No OSPF neighbor	Both ends of the link must be in 10.0.12.0/30 and both routers need the network line.
Local works, other site does not	Check the PC's default gateway, then show ip route on both routers.

GO FURTHER

Swap router-on-a-stick for a layer 3 switch (3560) with SVIs: interface vlan 10, ip routing.

INTERVIEW QUESTION YOU CAN NOW ANSWER

How does a PC in VLAN 10 talk to a PC in VLAN 20?

Through a router or layer 3 switch. VLANs are separate broadcast domains, so traffic between them has to be routed: here by subinterfaces on one trunk link.

RESUME LINE

Designed a two-site network in Cisco Packet Tracer with VLAN segmentation, router-on-a-stick inter-VLAN routing and OSPF, and verified end-to-end reachability.

PROJECT 02 / NETWORK TROUBLESHOOTING / FROM THE VIDEO

Break-and-Fix Troubleshooting Lab

You can find and fix a broken network the way a help desk or NOC engineer does, and write it up as a ticket.

TIME 2 hours	**LEVEL** Beginner

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

BUILD IT

01 **Save a working copy of project 1.**

File > Save As "project2-broken.pkt". Keep the original so you can compare.

02 **Break 5 things.**

Better: ask a friend to do it so you do not know where the faults are. Or write them down and come back tomorrow.

03 **Work bottom-up, one layer at a time.**

From the PC: can it reach its gateway? Then the far router? Then the far PC? tracert shows the last hop that answered.

```
ipconfig
ping 10.1.10.1
ping 10.0.12.2
tracert 10.2.10.11
```

04 **Confirm with show commands on the device you suspect.**

```
show ip interface brief
show vlan brief
show interfaces trunk
show ip route
show ip ospf neighbor
```

05 **Change one thing, then test again.**

Fixing two things at once means you never learn which one was the fault.

06 **Write a ticket for each fault.**

Symptom, what you checked, the cause, the fix, and the test that proved it was fixed.

THE 5 FAULTS TO INJECT

Fault	Symptom	Found with	Fix
Wrong VLAN on a port	PC cannot ping its gateway	show vlan brief	switchport access vlan 10
Port shut down	Red link light	show ip int brief: administratively down	no shutdown
Wrong mask on a PC	Some hosts reachable, not others	ipconfig on the PC	Correct the mask
OSPF network line removed	Other site unreachable	show ip route: no O routes	Re-add the network line
Wrong default gateway	Local pings work, remote fail	ipconfig on the PC	Correct the gateway

EXAMPLE TICKET

```
TICKET 001
Symptom:  PC-A3 cannot reach anything
Checked:  ipconfig ok, ping gateway fails
Cause:    Fa0/3 in VLAN 1, should be VLAN 20
Fix:      switchport access vlan 20
Verified: ping 10.1.20.1 and 10.2.20.11 ok
```

CHECK IT WORKS

Run or check	You should see
All 5 PCs ping across both sites	every fault fixed
5 tickets written	one per fault, in your own words

IF IT BREAKS

Problem	Fix
You fixed it but do not know why	Undo your change, confirm the fault comes back, then redo it. That is your proof.
Stuck on one fault	Compare that device's running-config with the same device in your saved working copy.

GO FURTHER

Bonus fault: switchport trunk allowed vlan 10 on the trunk. Guest dies, Staff works. Find it with show interfaces trunk.

INTERVIEW QUESTION YOU CAN NOW ANSWER

A user says "the internet is down". Walk me through it.

Start at the user: link and IP address, ping the gateway, ping an outside IP, then test DNS by name. Each step tells you which layer the fault is in.

RESUME LINE

Built a fault-injection lab in Packet Tracer and diagnosed 5 layer 1 to 3 faults (VLAN, port, mask, routing, gateway) with ping, traceroute and IOS show commands; documented each as a ticket.

Segmented Home Lab + Own DNS

You can separate networks with a real firewall and run your own DNS, the way a small office does.

TIME 3 to 4 hours	**LEVEL** Intermediate

TOOLS

VirtualBox (free)
pfSense CE (free; the download goes through Netgate's $0 installer checkout)
Pi-hole (free)

A computer with 8 GB of RAM. pfSense VM 1 GB, Pi-hole VM 1 GB, plus one small test VM.

LAB LAYOUT

Network	pfSense interface	Subnet
WAN	Adapter 1, NAT	from VirtualBox
LAN	Adapter 2, Internal "LAN"	192.168.10.1 /24
IOT	Adapter 3, Internal "IOT"	192.168.20.1 /24
GUEST	Adapter 4, Internal "GUEST"	192.168.30.1 /24
Pi-hole	VM on LAN	192.168.10.5 (static)

BUILD IT

01 **Create the pfSense VM with 4 adapters.**
Adapter 1 NAT (internet). Adapters 2 to 4 set to Internal Network named LAN, IOT and GUEST. Install pfSense CE.

02 **Assign interfaces at the console.**
Option 1: first adapter WAN, second LAN, third and fourth as OPT1 and OPT2. Option 2: LAN to 192.168.10.1/24 with DHCP on.

03 **Open the web interface from a VM on LAN.**
Browse to https://192.168.10.1, sign in with the default admin / pfsense and change that password straight away.

04 **Turn OPT1 and OPT2 into IOT and GUEST.**
Interfaces > OPT1: enable, rename IOT, static 192.168.20.1/24. Same for OPT2 as GUEST with 192.168.30.1/24. Services > DHCP Server: enable on each.

05 **Build the Pi-hole.**

Debian VM on LAN, static 192.168.10.5. Then:

```
curl -sSL https://install.pi-hole.net | bash
```

06 **Let Pi-hole answer the other networks.**

Pi-hole only answers its own subnet by default. Settings > DNS: choose "Permit all origins". Safe here, because the firewall decides who can reach it.

07 **Point every network at Pi-hole.**

Services > DHCP Server, on LAN, IOT and GUEST: DNS server 192.168.10.5.

08 **Write the GUEST firewall rules, top to bottom.**

Firewall > Aliases: make PRIVATE = 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Then on GUEST:

```
1  Pass   TCP/UDP  GUEST net -> 192.168.10.5 port 53
2  Block  any      GUEST net -> PRIVATE
3  Pass   any      GUEST net -> any
```

09 **Do the same for IOT.**

Same three rules on the IOT tab. LAN keeps its default allow rule.

10 **Add local DNS records.**

Pi-hole > Local DNS > DNS Records: nas.lab -> 192.168.10.20.

CHECK IT WORKS

Run or check	You should see
From a GUEST VM: ping 192.168.10.5	fails (only DNS is allowed through)
From a GUEST VM: nslookup nas.lab	answers 192.168.10.20
From a GUEST VM: open any website	loads
Pi-hole Query Log	queries arriving from 192.168.30.x

IF IT BREAKS

Problem	Fix
Guest has no internet	Rule order. pfSense reads top to bottom and stops at the first match.
DNS times out from IOT or GUEST	Pi-hole is still on local-only. Set "Permit all origins".
A VM gets no address	The Internal Network name on the VM must match the pfSense adapter exactly, and DHCP must be on.

GO FURTHER

Use real 802.1Q VLANs on one adapter (Interfaces > Assignments > VLANs). Use .home.arpa instead of .lab: it is the name reserved for home networks.

INTERVIEW QUESTION YOU CAN NOW ANSWER

Why put IoT devices on their own network?

Cheap devices get few security updates. If one is compromised, segmentation stops it reaching laptops and file servers.

RESUME LINE

Built a segmented virtual lab with pfSense (3 networks, firewall policy isolating guest and IoT traffic) and Pi-hole as internal DNS with local records.

PROJECT 04 / WIRESHARK / FROM THE VIDEO

Decode a Real Capture

You can read real traffic and explain what happens when someone opens a website.

TIME 1 to 2 hours	LEVEL Beginner

TOOLS

Wireshark (free)

Only capture on your own network and your own devices.

BUILD IT

01 Install Wireshark.

Windows: accept the Npcap install. macOS: install ChmodBPF when asked. Linux: add yourself to the wireshark group.

02 Clear your DNS cache so a fresh lookup happens.

```
Windows:  ipconfig /flushdns
macOS:    sudo dscacheutil -flushcache
          sudo killall -HUP mDNSResponder
```

03 Start a capture on the busy interface.

Pick the one with the moving line. Open one website you have not visited today. Stop after about 2 minutes.

04 Find the DNS lookup.

Read the name asked for, the record type (A or AAAA), the answer IP and the TTL.

```
dns.qry.name contains "example"
```

05 Follow the TCP handshake.

SYN, then SYN-ACK, then ACK. The time between SYN and SYN-ACK is your round-trip time to that server.

```
ip.addr == <answer IP> && tcp.flags.syn == 1
```

06 Read the server name in TLS.

Open the Client Hello: Transport Layer Security > Handshake > Extension: server_name.

```
tls.handshake.type == 1
```

07 **No TCP at all? Look for QUIC.**

Many sites use HTTP/3, which runs over UDP 443.

```
quic
```

08 **See the big picture.**

Statistics > Conversations > IPv4, sort by Bytes. Then Statistics > Protocol Hierarchy.

09 **Write a one-page report.**

DNS server and answer, handshake RTT, server name, top 3 conversations. Add screenshots.

CHECK IT WORKS

Run or check	You should see
Your report names	DNS server IP, answer IP, RTT in ms, server name, top talker

IF IT BREAKS

Problem	Fix
No interfaces listed	Npcap (Windows) or capture permissions (macOS, Linux) are missing. Reinstall or re-run as admin once.
No DNS packets	Your browser may use encrypted DNS (Secure DNS). Turn it off for the test, or run nslookup in a terminal.
No server name	The site uses Encrypted Client Hello. Pick another site.

GO FURTHER

Capture a file download and use Statistics > I/O Graphs to watch the throughput ramp up.

INTERVIEW QUESTION YOU CAN NOW ANSWER

What happens when you type a website into a browser?

DNS turns the name into an IP, TCP opens a connection with a three-way handshake (or QUIC over UDP), TLS sets up encryption, then HTTP requests the page.

RESUME LINE

Captured and analysed live traffic in Wireshark (DNS resolution, TCP three-way handshake, TLS server name, top conversations) and wrote a one-page findings report.

PROJECT 05 / PACKET TRACING / FROM THE VIDEO

Follow a Packet End to End

You understand what happens at each OSI layer, hop by hop. Interviewers ask this constantly.

TIME 1.5 hours	**LEVEL** Beginner

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

LAB LAYOUT

Device	Interface	Address
PC0	Fa0	DHCP from R1
R1	G0/0 PC side	10.10.1.1 /24
R1	G0/1 server side	10.10.2.1 /24
Server0	Fa0	10.10.2.10 /24, gateway 10.10.2.1

BUILD IT

01 **Build it: PC0, a switch, R1, Server0.**

Address R1 and the server as in the table, no shutdown on both router ports.

02 **Hand out addresses from R1.**

```
ip dhcp pool LAN
 network 10.10.1.0 255.255.255.0
 default-router 10.10.1.1
 dns-server 10.10.2.10
```

03 **Set up the server.**

Services > DNS: on, add an A record www.lab.local -> 10.10.2.10. Services > HTTP: on.

04 **Set PC0 to DHCP.**

Desktop > IP Configuration > DHCP. It should get 10.10.1.x.

05 **Switch to Simulation mode.**

Bottom right. Edit Filters: tick only ARP, DNS, TCP and HTTP.

06 **Open the page from PC0.**

Desktop > Web Browser > http://www.lab.local

07 **Step through every hop.**

Press Capture/Forward. Click each envelope and read the OSI Model tab, inbound and outbound.

08 **Fill in the hop table.**

One row per hop: source MAC, destination MAC, source IP, destination IP, TTL.

CHECK IT WORKS

Run or check	You should see
First packet	ARP for the gateway 10.10.1.1
Before any HTTP	a DNS query and answer, then the TCP handshake
At R1	source and destination MAC change, IPs stay the same, TTL drops by 1

IF IT BREAKS

Problem	Fix
Page does not load	Check the DNS service is on and the A record name matches exactly.
PC0 shows 169.254.x.x	It got no DHCP answer. Check the pool network and that R1 G0/0 is up.

GO FURTHER

Add a second router between them and watch the MAC change again at every hop.

INTERVIEW QUESTION YOU CAN NOW ANSWER

As a packet crosses routers, what changes: the MAC or the IP?

The MAC addresses are rewritten at every hop. The source and destination IPs stay the same end to end, unless NAT is in the path.

RESUME LINE

Traced DHCP, ARP, DNS and HTTP hop by hop in Packet Tracer simulation mode and documented how layer 2 and layer 3 headers change at each device.

PROJECT 06 / NETWORK AUTOMATION / FROM THE VIDEO

Config Backup Bot

You can automate a real network task with Python, the skill that sets junior candidates apart.

TIME 3 hours	**LEVEL** Intermediate

TOOLS

Cisco Modeling Labs Free (free, up to 5 nodes at once)
Cisco DevNet Sandbox (free, reserve with a Cisco.com account)
Netmiko (free Python library)
Git (free)

Routers you can SSH into. Packet Tracer devices cannot be reached from Python. GNS3 also works, but needs a router image you are licensed to use.

BUILD IT

01 Get lab routers.

CML Free: two IOL routers plus an External Connector so your computer can reach them. Or reserve a DevNet Sandbox and use the details it gives you.

02 Turn on SSH on each router.

Use your own password.

```
hostname R1
ip domain-name lab.local
crypto key generate rsa modulus 2048
username admin privilege 15 secret <your-password>
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
```

03 Set up the project folder.

```
mkdir netbackup && cd netbackup
python -m venv venv
source venv/bin/activate   (Windows: venv\Scripts\activate)
pip install netmiko pyyaml
git init
```

04 List your devices in devices.yaml.

No password in the file.

```
- host: 192.168.1.11
  device_type: cisco_ios
  username: admin
- host: 192.168.1.12
  device_type: cisco_ios
  username: admin
```

05 Write backup.py.

One file per device. Git keeps the history, so git diff shows exactly what changed.

```
import os, yaml, subprocess, datetime
from netmiko import ConnectHandler

devices = yaml.safe_load(open("devices.yaml"))
os.makedirs("configs", exist_ok=True)
for d in devices:
    d["password"] = os.environ["NET_PASS"]
    with ConnectHandler(**d) as conn:
        cfg = conn.send_command("show running-config")
    with open(f"configs/{d['host']}.txt", "w") as f:
        f.write(cfg)

subprocess.run(["git", "add", "configs"])
subprocess.run(["git", "commit", "-m",
                f"backup {datetime.date.today()}"])
```

06 Run it.

Set the password in the terminal session only.

```
export NET_PASS='<your-password>'   (Windows: set NET_PASS=...)
python backup.py
```

07 Schedule it nightly.

macOS or Linux, crontab -e. On Windows use Task Scheduler.

```
0 2 * * * cd ~/netbackup && NET_PASS=... ./venv/bin/python backup.py
```

CHECK IT WORKS

Run or check	You should see
ls configs	one .txt per router
Change an interface description, run again, then: git diff HEAD~1	exactly that line shows as changed

IF IT BREAKS

Problem	Fix
Authentication failed	NET_PASS is not set in this terminal, or the username differs from the router.
Timed out	Your computer cannot reach the router. ping it first; check the CML External Connector.
Pattern not detected	Wrong device_type for that box (cisco_ios for IOS and IOL).

GO FURTHER

Push the repo to GitHub with a README and a screenshot of a diff. Add a Slack or email alert when a diff appears.

INTERVIEW QUESTION YOU CAN NOW ANSWER

Why back up configs into Git instead of a folder?

Git keeps every version with a date, shows the exact lines that changed and who changed them, and lets you roll back.

RESUME LINE

Wrote a Python/Netmiko tool that backs up router configurations into Git on a schedule and flags configuration drift with diffs.

PROJECT 07 / REDUNDANCY

Redundant Gateway with HSRP

You can keep a network running when a router dies.

TIME 1 hour	**LEVEL** Intermediate

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

LAB LAYOUT

Device	Interface	Address
R1	G0/0	10.1.10.2 /24, priority 110
R2	G0/0	10.1.10.3 /24, priority 100
Virtual gateway	shared	10.1.10.1
PCs	gateway	10.1.10.1

BUILD IT

01 Put R1 and R2 on the same switch as the PCs.

02 Configure R1 as the preferred gateway.

```
interface g0/0
 ip address 10.1.10.2 255.255.255.0
 standby 1 ip 10.1.10.1
 standby 1 priority 110
 standby 1 preempt
 no shutdown
```

03 Configure R2 as the standby.

```
interface g0/0
 ip address 10.1.10.3 255.255.255.0
 standby 1 ip 10.1.10.1
 no shutdown
```

04 Test the failover.

On a PC run ping -t 10.1.10.1. Shut R1 G0/0. Watch R2 take over after a few lost pings (the default hold time is 10 seconds). Bring R1 back: preempt makes it active again.

CHECK IT WORKS

Run or check	You should see
show standby brief	R1 Active, R2 Standby, virtual IP 10.1.10.1

IF IT BREAKS

Problem	Fix
Both routers say Active	They cannot hear each other. Check they are in the same VLAN and the group number matches.

INTERVIEW QUESTION YOU CAN NOW ANSWER

What problem does HSRP solve?

A PC can only have one default gateway. HSRP lets two routers share one virtual gateway IP, so one can fail without users noticing.

RESUME LINE

Configured HSRP gateway redundancy and tested failover with a continuous ping.

PROJECT 08 / SECURITY

ACL Security Policy

You can enforce who can talk to what, the core of network security work.

TIME 1.5 hours	LEVEL Intermediate

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

BUILD IT

01 Start from project 1.

Add a "public" web server at 203.0.113.10 (a range reserved for examples) behind R2, and add it to OSPF on R2.

02 Write the Guest policy on R1.

Order matters: the first matching line wins, and anything not permitted is denied at the end.

```
ip access-list extended GUEST-IN
 permit udp any any eq bootps
 permit udp 10.1.20.0 0.0.0.255 any eq 53
 deny   ip  10.1.20.0 0.0.0.255 10.0.0.0 0.255.255.255
 permit tcp 10.1.20.0 0.0.0.255 any eq 80
 permit tcp 10.1.20.0 0.0.0.255 any eq 443
```

03 Apply it where Guest traffic enters the router.

```
interface g0/0.20
 ip access-group GUEST-IN in
```

04 Test from a Guest PC.

Browser to 203.0.113.10: works. Ping 203.0.113.10: fails (ICMP not permitted). Ping a Staff PC: fails.

CHECK IT WORKS

Run or check	You should see
`show access-lists`	hit counters climbing on the lines you tested

IF IT BREAKS

Problem	Fix
Everything is blocked	The ACL is applied out instead of in, or on the wrong subinterface.

INTERVIEW QUESTION YOU CAN NOW ANSWER

Where do you put an extended ACL, and why?

Close to the source, so unwanted traffic is dropped before it crosses the network.

RESUME LINE

Wrote and applied extended ACLs enforcing a guest-access policy, verified with hit counters.

PROJECT 09 / SERVICES

Edge Router: DHCP + NAT

You can build the edge of an office network: automatic addressing and shared internet access.

TIME 1.5 hours	**LEVEL** Intermediate

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

LAB LAYOUT

Device	Interface	Address
R1	G0/2 to ISP	`198.51.100.2 /30`
ISP router	to R1	`198.51.100.1 /30`
ISP router	to server	`203.0.113.1 /24`
Internet server	Fa0	`203.0.113.10`

BUILD IT

01 Hand out addresses for each VLAN.

Start from a copy of project 1. On R1:

```
ip dhcp excluded-address 10.1.10.1 10.1.10.10
ip dhcp pool STAFF
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 dns-server 203.0.113.10
```

02 Repeat for Guest.

Pool GUEST, network 10.1.20.0, gateway 10.1.20.1. Set the PCs to DHCP.

03 Translate inside addresses to the one public address.

```
access-list 1 permit 10.1.0.0 0.0.255.255
interface g0/0.10
 ip nat inside
interface g0/0.20
 ip nat inside
interface g0/2
 ip address 198.51.100.2 255.255.255.252
 ip nat outside
 no shutdown
ip nat inside source list 1 interface g0/2 overload
ip route 0.0.0.0 0.0.0.0 198.51.100.1
```

04 Browse to 203.0.113.10 from a PC.

CHECK IT WORKS

Run or check	You should see
`show ip dhcp binding`	each PC with a leased address
`show ip nat translations`	10.1.10.x mapped to 198.51.100.2 with different ports

IF IT BREAKS

Problem	Fix
PCs get 169.254.x.x	The pool network does not match the subinterface, or the gateway address is inside the pool (exclude it).

INTERVIEW QUESTION YOU CAN NOW ANSWER

What is PAT?

Port Address Translation: many private addresses share one public IP, told apart by port numbers. It is what "overload" turns on.

RESUME LINE

Configured router-based DHCP and PAT for a multi-VLAN office edge.

PROJECT 10 / VPN

Site-to-Site IPsec VPN

You can connect two offices securely over the internet.

TIME 2 hours	**LEVEL** Advanced

TOOLS

Cisco Modeling Labs Free (free, up to 5 nodes at once)

LAB LAYOUT

Device	Interface	Address
Branch A	E0/0 to ISP	198.51.100.2 /30
Branch A	Loopback0 LAN	10.1.1.1 /24
ISP	E0/0 / E0/1	198.51.100.1 /30, 203.0.113.1 /30
Branch B	E0/0 to ISP	203.0.113.2 /30
Branch B	Loopback0 LAN	10.2.2.1 /24

BUILD IT

01 Build 3 IOL routers and address them.

Give each branch a default route to the ISP. The ISP needs no routes to the 10.x networks: that is the point.

02 Configure Branch A.

Use your own pre-shared key. Branch B is the mirror image (peer 198.51.100.2, ACL reversed).

```
crypto isakmp policy 10
 encryption aes 256
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key <your-key> address 203.0.113.2
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel
access-list 110 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
crypto map VPN 10 ipsec-isakmp
 set peer 203.0.113.2
 set transform-set TS
 match address 110
interface e0/0
 crypto map VPN
```

03 Send traffic through the tunnel.

```
ping 10.2.2.1 source loopback0
```

CHECK IT WORKS

Run or check	You should see
`show crypto isakmp sa`	state QM_IDLE
`show crypto ipsec sa`	#pkts encaps and decaps climbing

IF IT BREAKS

Problem	Fix
No SA comes up	The keys, the policy settings or the mirrored ACLs do not match on both sides.

INTERVIEW QUESTION YOU CAN NOW ANSWER

What is the difference between IKE phase 1 and phase 2?

Phase 1 builds a secure channel between the two routers. Phase 2 uses it to agree the IPsec tunnel that carries the actual traffic.

RESUME LINE

Built and verified a site-to-site IPsec VPN between two branch routers.

PROJECT 11 / MONITORING

Network Monitoring Dashboard

You can watch a network and get told when something breaks, the daily job of a NOC.

TIME 2 hours	**LEVEL** Intermediate

TOOLS

LibreNMS (free, open source)

BUILD IT

01 Install LibreNMS on a small Linux VM.

The official Docker setup is the quickest route. Zabbix (also free) works the same way.

02 Turn on SNMP on your lab routers.

Version 2c is fine in a lab. Use SNMPv3 anywhere real.

```
snmp-server community labRO RO
```

03 Add the devices.

Devices > Add Device: the router IP, version v2c, community labRO. Add your home router too if it supports SNMP.

04 Turn on alerting.

Enable the built-in device-down alert rule and set up an email transport.

05 Break something.

Shut down a router interface or power off a lab router, and wait for the alert.

CHECK IT WORKS

Run or check	You should see
Device page	CPU, memory and traffic graphs filling in
Inbox	a down alert, then a recovery alert

IF IT BREAKS

Problem	Fix
Device will not add	Check the community string and that UDP 161 from the VM reaches the router.

INTERVIEW QUESTION YOU CAN NOW ANSWER

What is SNMP for?

Polling devices for health and traffic data (and receiving traps), so a monitoring system can graph it and alert on problems.

RESUME LINE

Deployed open-source network monitoring with SNMP polling and down alerts.

PROJECT 12 / IPV6

IPv6 Dual-Stack Upgrade

You can run IPv6 next to IPv4, which every modern network does.

TIME 1.5 hours	**LEVEL** Intermediate

TOOLS

Cisco Packet Tracer (free with a NetAcad account)

LAB LAYOUT

Network	IPv6 prefix	
Site A Staff	2001:db8:1:10::/64	gateway ::1
Site B Staff	2001:db8:2:10::/64	gateway ::1
R1 to R2 link	2001:db8:0:12::/64	

BUILD IT

01 Turn on IPv6 routing and address R1.

2001:db8::/32 is the range reserved for documentation, ideal for labs.

```
ipv6 unicast-routing
interface g0/0.10
 ipv6 address 2001:db8:1:10::1/64
 ipv6 ospf 1 area 0
interface g0/1
 ipv6 address 2001:db8:0:12::1/64
 ipv6 ospf 1 area 0
ipv6 router ospf 1
 router-id 1.1.1.1
```

02 Do the same on R2.

Use 2001:db8:2:10::1, 2001:db8:0:12::2 and router-id 2.2.2.2.

03 Set the PCs to automatic IPv6.

Desktop > IP Configuration > IPv6: Automatic (SLAAC).

CHECK IT WORKS

Run or check	You should see
`show ipv6 ospf neighbor`	the other router, FULL
`show ipv6 route`	O routes for the other site
`ping 2001:db8:2:10::<host>` from a Site A PC	replies

IF IT BREAKS

Problem	Fix
PCs get no IPv6 address	ipv6 unicast-routing is missing, so the router is not sending router advertisements.

INTERVIEW QUESTION YOU CAN NOW ANSWER

How does SLAAC work?

The router advertises the /64 prefix and the host builds its own address from it, with no DHCP server needed.

RESUME LINE

Migrated a two-site lab to dual-stack IPv4/IPv6 with SLAAC and OSPFv3.

PROJECT 13 / SUBNETTING

IP Address Plan with VLSM

You can plan addressing for a whole company without wasting space. Every network job tests this.

TIME 1 hour	LEVEL Beginner

TOOLS

A spreadsheet (any)

BUILD IT

01 **The brief.**

HQ has 200 users, Branch 1 has 60, Branch 2 has 25, plus 3 router-to-router links. You have 10.20.0.0/23.

02 **Size each subnet, biggest first.**

Usable hosts = 2^(host bits) - 2. 200 needs /24 (254), 60 needs /26 (62), 25 needs /27 (30), a link needs /30 (2).

03 **Allocate in order and fill the table.**

Columns: subnet, mask, gateway, first host, last host, broadcast. Try it before you check the answer below.

04 **Then a curveball.**

A Branch 3 with 50 users opens. Where does it go without renumbering anything?

CHECK YOUR ANSWER

Site	Subnet	Hosts	Broadcast
HQ	10.20.0.0 /24	.1 to .254	10.20.0.255
Branch 1	10.20.1.0 /26	.1 to .62	10.20.1.63
Branch 2	10.20.1.64 /27	.65 to .94	10.20.1.95
Link 1	10.20.1.96 /30	.97 to .98	10.20.1.99
Link 2	10.20.1.100 /30	.101 to .102	10.20.1.103
Link 3	10.20.1.104 /30	.105 to .106	10.20.1.107
Branch 3	10.20.1.128 /26	.129 to .190	10.20.1.191

CHECK IT WORKS

Run or check	You should see
No two subnets overlap	and every site fits its user count

IF IT BREAKS

Problem	Fix
Overlaps	You allocated a small subnet before a big one. Always go biggest first.

INTERVIEW QUESTION YOU CAN NOW ANSWER

How many usable hosts in a /27?

30. 32 addresses minus the network and broadcast addresses.

RESUME LINE

Designed a VLSM addressing plan for a three-site company with room to grow.

PROJECT 14 / BGP

BGP Between Three "ISPs"

You understand how the internet routes between companies, the step up from OSPF.

TIME 2 hours	**LEVEL** Advanced

TOOLS

Cisco Modeling Labs Free (free, up to 5 nodes at once)

LAB LAYOUT

Router	AS	Loopback0 / links
R1	65001	172.16.1.1/24, 10.0.12.1/30
R2	65002	172.16.2.1/24, 10.0.12.2, 10.0.23.2
R3	65003	172.16.3.1/24, 10.0.23.3/30

BUILD IT

01 **Build 3 IOL routers in a line and address them.**

65001 to 65003 are private AS numbers, safe for labs.

02 **Peer R1 with R2 and advertise R1's loopback.**

R2 peers with both neighbours, R3 with R2, each advertising its own loopback.

```
router bgp 65001
 neighbor 10.0.12.2 remote-as 65002
 network 172.16.1.0 mask 255.255.255.0
```

03 **Filter one route on R2.**

Stop R1 learning R3's network.

```
ip prefix-list NO-R3 deny 172.16.3.0/24
ip prefix-list NO-R3 permit 0.0.0.0/0 le 32
router bgp 65002
 neighbor 10.0.12.1 prefix-list NO-R3 out
end
clear ip bgp 10.0.12.1 soft out
```

CHECK IT WORKS

Run or check	You should see
show ip bgp summary	a prefix count (not Idle or Active) for each neighbour
show ip bgp on R1	172.16.3.0 with path 65002 65003 before the filter, gone after

IF IT BREAKS

Problem	Fix
Neighbour stuck in Active	The neighbor IP or remote-as is wrong, or the link itself is down.
Route not advertised	The network line must match a route already in the routing table exactly, mask included.

INTERVIEW QUESTION YOU CAN NOW ANSWER

Why does the internet use BGP and not OSPF?

BGP is built for routing between organisations: it scales to the whole internet and lets each AS choose paths by policy, not just by shortest path.

RESUME LINE

Configured eBGP peering between three autonomous systems with prefix-list filtering.

PROJECT 15 / DOCUMENTATION

Network Documentation Pack

You can document a network so someone else can run it, a skill every hiring manager wants.

TIME	LEVEL
2 hours	Beginner

TOOLS

draw.io (free, runs in the browser)

BUILD IT

01 **Draw project 1.**
Use the network shapes in draw.io. Every device named, every link labelled with interfaces, every subnet and VLAN shown.

02 **Make the IP table.**
Device, interface, IP, mask, VLAN, description.

03 **Make the VLAN table.**
VLAN ID, name, subnet, gateway, which ports.

04 **Write a runbook: "a user cannot reach the internet".**
Numbered steps someone new could follow, with the exact commands and what a good result looks like.

05 **Put it all in one PDF or a GitHub README.**
This becomes the front page of your portfolio.

CHECK IT WORKS

Run or check	You should see
Hand it to a friend	they can find any device's IP in under 10 seconds

IF IT BREAKS

Problem	Fix
Diagram is a mess	Draw layer 3 (routers and subnets) and layer 2 (switches and VLANs) as two separate diagrams.

INTERVIEW QUESTION YOU CAN NOW ANSWER

How do you document a network?

A current diagram, IP and VLAN tables, and runbooks for common problems, kept in one place and updated with every change.

RESUME LINE

Produced topology diagrams, addressing tables and a troubleshooting runbook for a multi-site network.

PROJECT 16 / AUTOMATION

Ansible Config Push

You can configure many devices the same way at once, the next step after project 6.

TIME 2 to 3 hours	**LEVEL** Advanced

TOOLS

Ansible (free; needs Linux, macOS or WSL)

The routers from project 6 (CML Free or a DevNet Sandbox) with SSH on.

BUILD IT

01 Install Ansible and the Cisco modules.

```
pip install ansible ansible-pylibssh
ansible-galaxy collection install cisco.ios
```

02 Write inventory.ini.

```
[routers]
r1 ansible_host=192.168.1.11 lo_ip=10.100.100.1
r2 ansible_host=192.168.1.12 lo_ip=10.100.100.2

[routers:vars]
ansible_connection=ansible.netcommon.network_cli
ansible_network_os=cisco.ios.ios
ansible_user=admin
ansible_password="{{ lookup('env', 'NET_PASS') }}"
```

03 Write site.yml.

```
- hosts: routers
  gather_facts: false
  tasks:
    - name: NTP server
      cisco.ios.ios_config:
        lines:
          - ntp server 192.168.1.1
    - name: Loopback for management
      cisco.ios.ios_config:
        parents: interface Loopback100
        lines:
          - description managed by ansible
          - ip address {{ lo_ip }} 255.255.255.255
```

04 Run it twice.

The first run reports changed. The second should report changed=0: that is idempotence.

```
ansible-playbook -i inventory.ini site.yml
```

05 Keep it in Git.

Same repo as project 6, so your backups show every change Ansible made.

CHECK IT WORKS

Run or check	You should see
`Second run`	ok=2 changed=0 on every router
`show run interface Loopback100`	the description and the right IP on each router

IF IT BREAKS

Problem	Fix
Connection fails	Check NET_PASS is set and you can SSH to the router by hand first.

INTERVIEW QUESTION YOU CAN NOW ANSWER

What does idempotent mean in automation?

Running the same job again changes nothing if the device is already right. You can run it any time, safely.

RESUME LINE

Automated consistent router configuration across devices with idempotent Ansible playbooks.

WHAT TO DO NEXT

A 4-week plan

Week	Build	Why
1	Projects 1 and 2	Build a network, then break and fix it
2	Projects 4, 5 and 13	See real traffic and master subnetting
3	Projects 3 and 15	Your own firewall and DNS, then document it
4	Project 6	Your first automation, on GitHub
After	Pick from 7 to 16	Match the job posts you are applying to

PAIR THE PROJECTS WITH THE CERT

Network+ then CCNA

Projects prove you can do the work. The cert gets your resume past the filter. VLANs, routing, DNS, subnetting and troubleshooting are on both exams, so practise the questions while you build.

Try 15 free Network+ questions. No sign-up needed.

getuprep.com/paths/networking

Built one? Post it on LinkedIn and GitHub with the resume line, and tag @getuacademy.

If this helped, please consider following @getuacademy.