

School Network Design

Cisco Packet Tracer · Network Configuration · Logan Pride

Cisco Packet Tracer	Networking	Subnetting	DHCP	ACL	SSH	Logan Pride
---------------------	------------	------------	------	-----	-----	-------------

PROJECT OVERVIEW

Overview

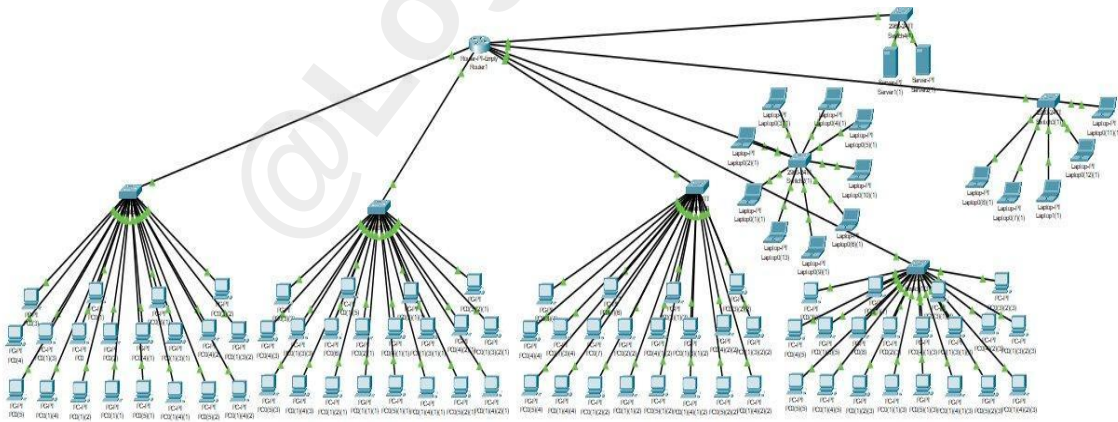
A two-phase school network design and expansion project built entirely in Cisco Packet Tracer. Starting from a blank 10.0.0.0/24 address space, I designed, subnetted, configured, and secured a full school network serving 4 classrooms (80 PCs), an admin office (10 laptops), a staff room (5 laptops), and a server room. I then expanded it with Wi-Fi access points, dedicated servers, guest network isolation, SSH remote management, and enhanced ACL-based security.

Every subnet calculation, DHCP pool, ACL rule, and router configuration was designed and implemented by hand using Cisco IOS commands.

NETWORK DIAGRAM

Topology

Full network topology built in Cisco Packet Tracer — showing the central router, 4 classroom switches, admin/staff/server subnets, and expanded Wi-Fi and server infrastructure:



Cisco Packet Tracer topology — full school network with subnets, switches, servers, and Wi-Fi APs

PHASE 1 — BASE NETWORK

Subnetting Design

Starting with 10.0.0.0/24 (256 total IPs), I calculated and allocated subnets sized to each room's device count, minimizing wasted addresses:

Room	Subnet	Mask	Usable IPs	Router IP
Classroom 1-4 (each)	10.0.0.x/27	255.255.255.224	30 usable	10.0.0.1 / .33 / .65 / .97
Admin Office	10.0.0.128/28	255.255.255.240	14 usable	10.0.0.129
Staff Room	10.0.0.144/29	255.255.255.248	6 usable	10.0.0.145
Server Room	10.0.0.152/29	255.255.255.248	6 usable	10.0.0.153

DHCP Configuration

DHCP pools were configured on the router for all four classroom subnets, with excluded addresses reserving the router interface IPs:

```
ip dhcp excluded-address 10.0.0.1
ip dhcp pool Classroom1
 network 10.0.0.0 255.255.255.224
 default-router 10.0.0.1
 dns-server 8.8.8.8
! (Repeated for Classroom2-4 on .32, .64, .96 subnets)
```

Static IPs were assigned manually to admin laptops (10.0.0.130–.139), staff laptops (10.0.0.146–.151), and both servers within their respective subnets.

Access Control Lists (ACL 100)

ACL 100 blocks all classroom traffic from reaching the admin office subnet, applied inbound on each classroom router interface:

```
access-list 100 deny ip 10.0.0.0 0.0.0.31 10.0.0.128 0.0.0.15
access-list 100 deny ip 10.0.0.32 0.0.0.31 10.0.0.128 0.0.0.15
access-list 100 deny ip 10.0.0.64 0.0.0.31 10.0.0.128 0.0.0.15
access-list 100 deny ip 10.0.0.96 0.0.0.31 10.0.0.128 0.0.0.15
access-list 100 permit ip any any
interface GigabitEthernet0/1
 ip access-group 100 in
```

Connectivity tests confirmed ACL 100 worked — classroom PCs successfully pinged each other but were blocked from the admin subnet.

PHASE 2 — NETWORK EXPANSION

Wi-Fi & Guest Network

- Deployed two home wireless routers as access points: **School_WiFi** (staff/students) and **Guest_WiFi** (visitors), both secured with WPA2 encryption.
- Guest network isolated on its own subnet with DHCP range restricted to guest IPs only, preventing access to internal school resources.
- QoS data cap of 2GB/day applied to guest devices.

Server Infrastructure

Three dedicated servers added to the network, each with role-specific ACL rules:

- **Email Server:** static IP, ACL 110 restricts access to school network IPs only (10.0.0.0/24); external traffic denied.
- **File Server:** ACL 120 blocks all classroom subnets; only admin (10.0.0.128/28) and staff (10.0.0.144/29) can access.
- **Print Server:** ACL 130 mirrors file server access rules — admin and staff only, classrooms blocked.

```
! File Server ACL (example)
access-list 120 deny ip 10.0.0.0 0.0.0.31 host 10.0.0.20
access-list 120 deny ip 10.0.0.32 0.0.0.31 host 10.0.0.20
access-list 120 permit ip 10.0.0.128 0.0.0.15 host 10.0.0.20
access-list 120 permit ip 10.0.0.144 0.0.0.7 host 10.0.0.20
access-list 120 permit ip any any
```

Enhanced Security

- **ACL 150:** blocks ICMP (ping) from all classroom subnets to the server room, preventing classroom devices from probing servers.
- **ACL 160:** guest network isolation: all guest IPs blocked from reaching any internal subnet (classrooms, admin, staff, servers).
- **SSH** configured on router and switches for encrypted remote management access.

TECHNICAL HIGHLIGHTS

Technical Highlights

Tool	Cisco Packet Tracer
Address Space	10.0.0.0/24 — 256 total IPs, fully subnetted
Subnets	/27 (classrooms) · /28 (admin) · /29 (staff, servers)
DHCP	4 pools for classrooms; static IPs for admin, staff, servers
ACLs	ACL 100, 110, 120, 130, 150, 160 — role-based access control
Wi-Fi	WPA2-secured School_WiFi + Guest_WiFi with subnet isolation
Servers	Email, File, and Print servers with per-role ACL restrictions
SSH	Remote management configured on router and switches
Devices	80 classroom PCs + 10 admin + 5 staff + 2 servers + APs

TAKEAWAYS

What I Learned

- Subnetting from scratch; calculating /27, /28, and /29 subnets from a /24 space to minimize wasted IPs while meeting each room's device count.
- How DHCP works at the IOS configuration level: building pools, excluding router IPs, and understanding why static IPs matter for servers and admin devices.

- ACL design thinking, writing deny/permit rules in the correct order, applying them to the right interface direction, and testing to verify they block what they should.
- Network security layering: combining ACLs, WPA2 Wi-Fi encryption, guest network isolation, and SSH management creates a defense-in-depth approach even in a small school network.
- Troubleshooting in Packet Tracer, using ping and traceroute to diagnose routing failures, and resetting configurations to test from a clean state.
- The value of documentation, writing out subnet calculations and ACL logic before touching the router saved significant time during configuration.

Full Packet Tracer file available upon request — loganpride525@email.com

@Logan Pride