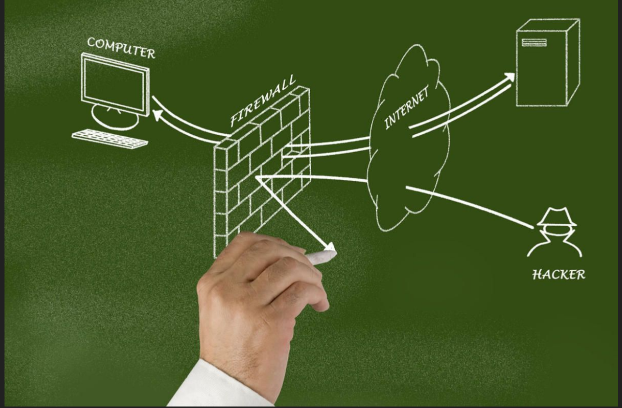
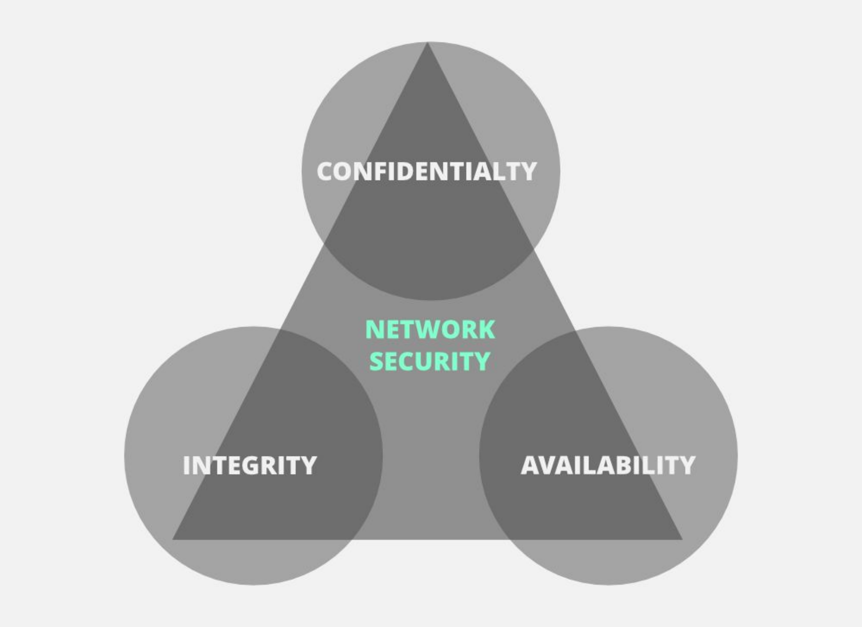


Network Security

What it takes to make a network secure

What is Network Security?

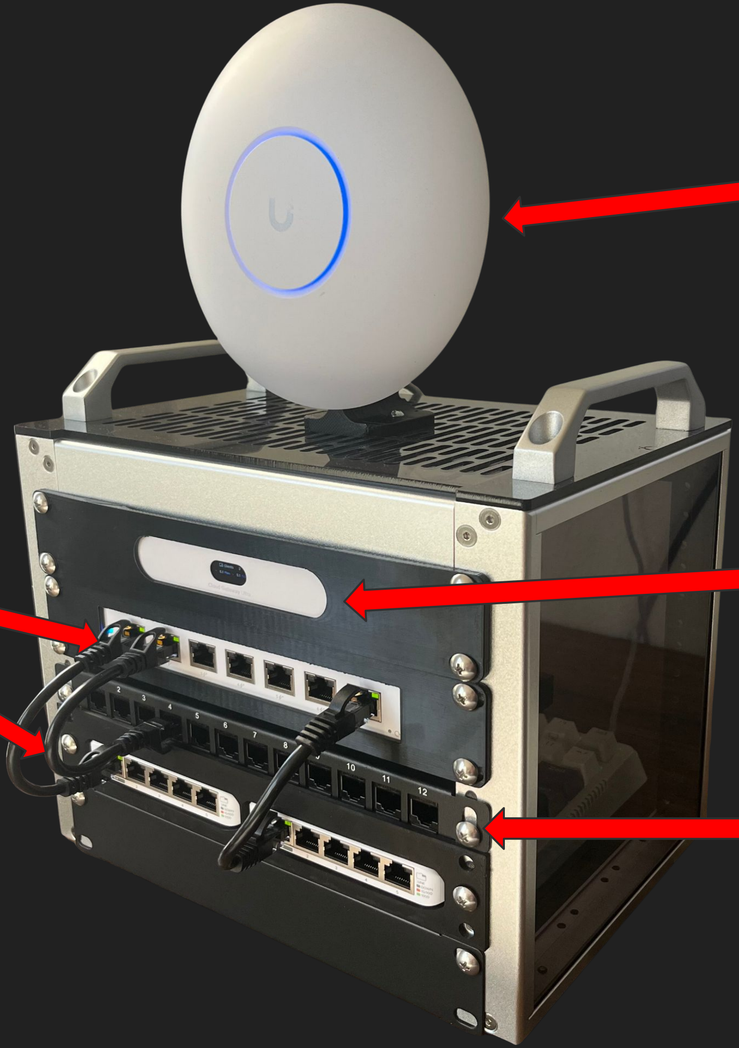
Network security is the practice of protecting computer networks and their data from unauthorized access, misuse, attacks, and damage



What we are going to discuss today (with exercises!)

- Network Segmentation (VLANs)
- Zero Trust Architecture
- DMZs
- Firewalls
- Intrusion Detection/Prevention
- DNS
- DHCP
- Ports

My Rack



Access Point (WiFi)

Switches

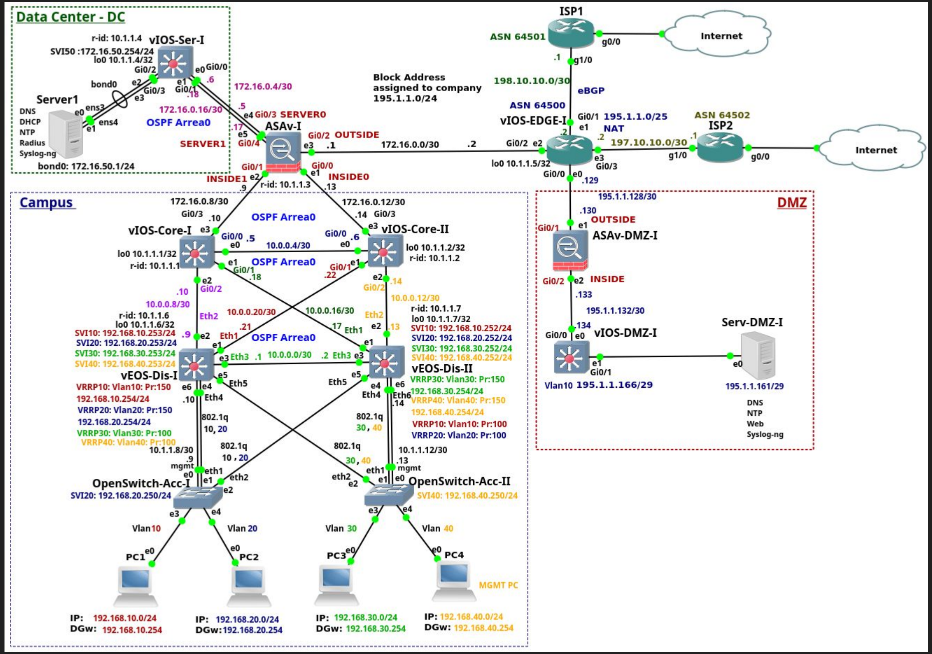
Router

Patch Panel

Why Build the Rack?

The idea here is to develop an enterprise level network in a much smaller form factor and simpler design

For small businesses or homelabs



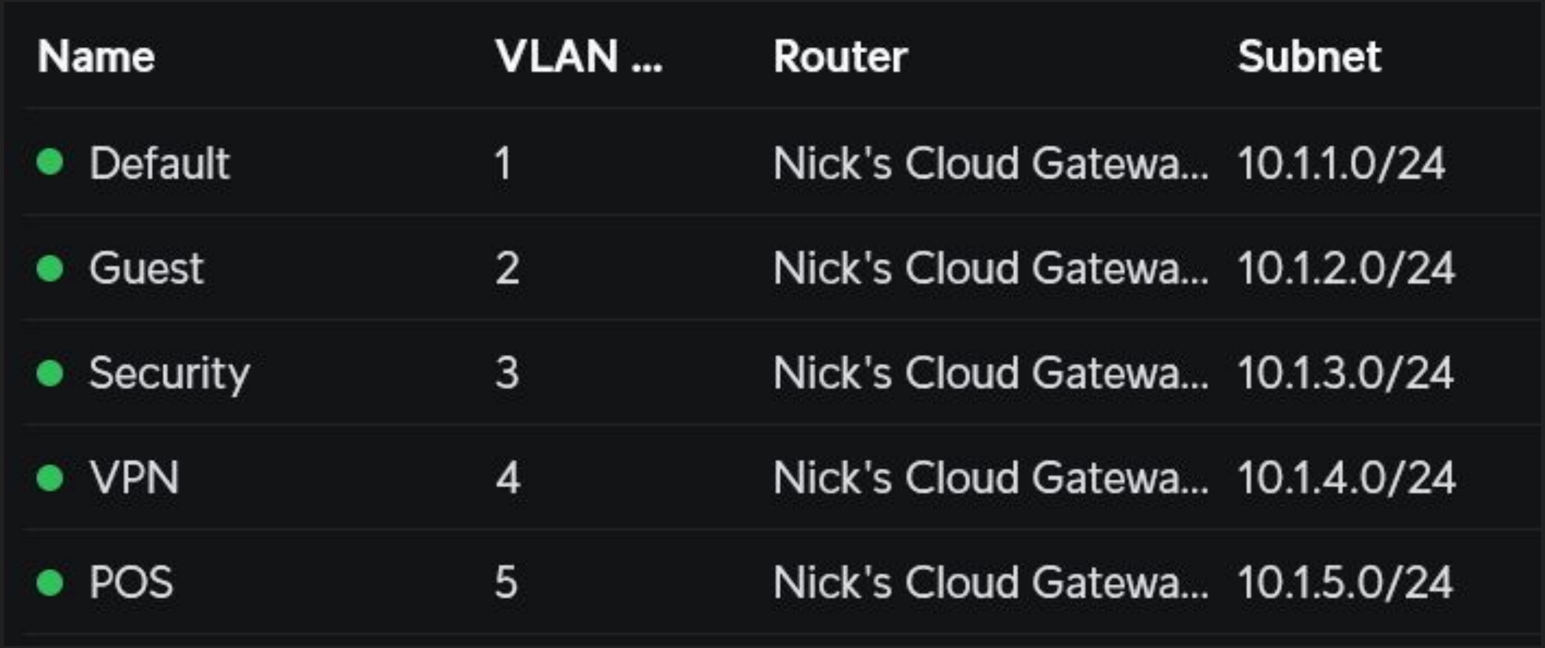
Zero Trust Architecture

“Never Trust, Always Verify”

It assumes that no user, device, or network, whether inside or outside the organization, should be automatically trusted.

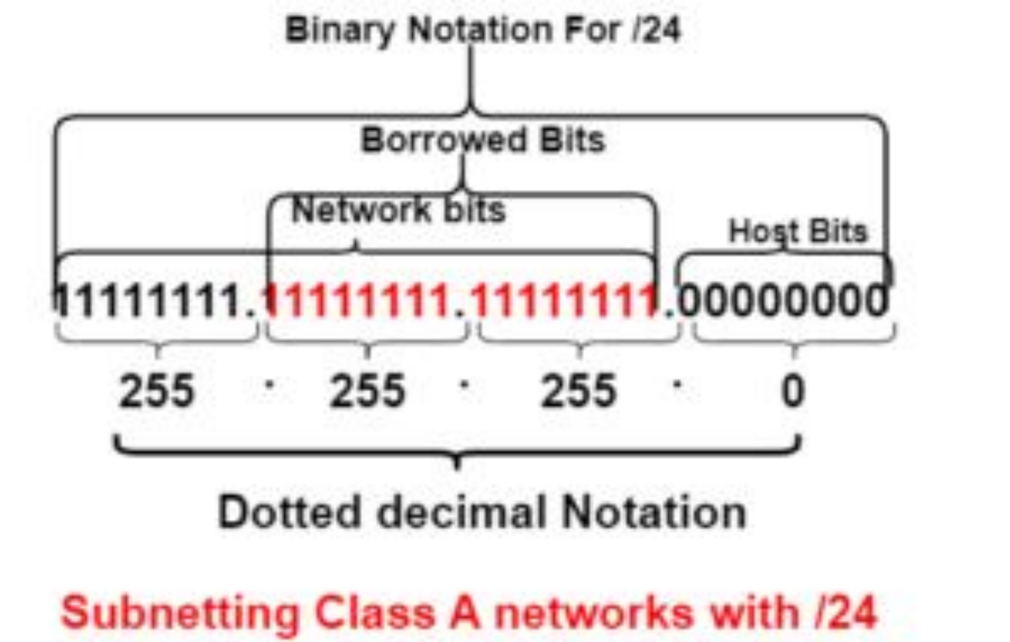
Network Segmentation

Network segmentation is the practice of dividing a computer network into smaller, isolated sections or subnetworks (subnets)



Name	VLAN ...	Router	Subnet
● Default	1	Nick's Cloud Gatewa...	10.1.1.0/24
● Guest	2	Nick's Cloud Gatewa...	10.1.2.0/24
● Security	3	Nick's Cloud Gatewa...	10.1.3.0/24
● VPN	4	Nick's Cloud Gatewa...	10.1.4.0/24
● POS	5	Nick's Cloud Gatewa...	10.1.5.0/24

Subnetting



254 usable IP addresses (256 total, minus network and broadcast addresses)

The network address is the first IP address in a subnet. It identifies the network itself and is used for routing purposes

The broadcast address is the last IP address in a subnet

Small Networks

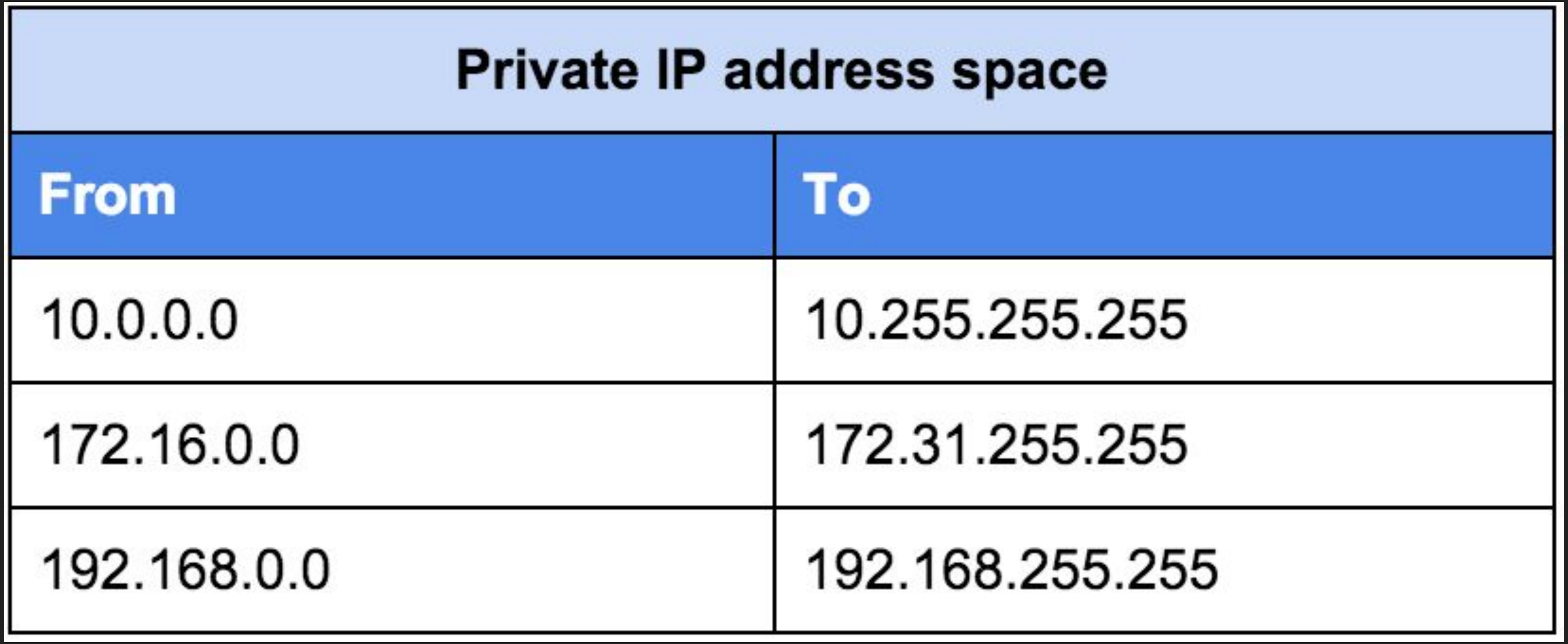
192.168.1.0/28

Subnet mask of 255.255.255.240 or 11111111.11111111.11111111.11110000

2^4 = 16 total addresses

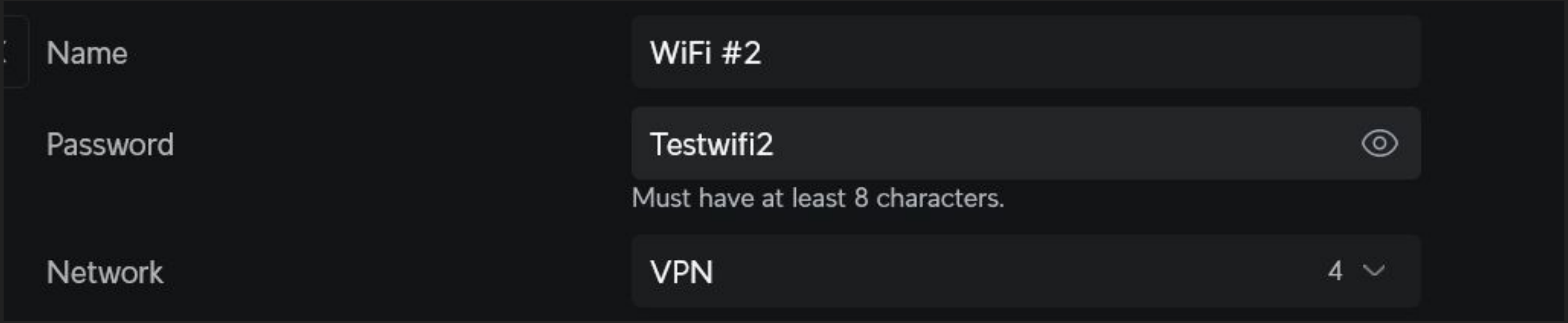
16 - 2 = 14 usable addresses

Internal IP Addresses



Private IP address space	
From	**To**
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

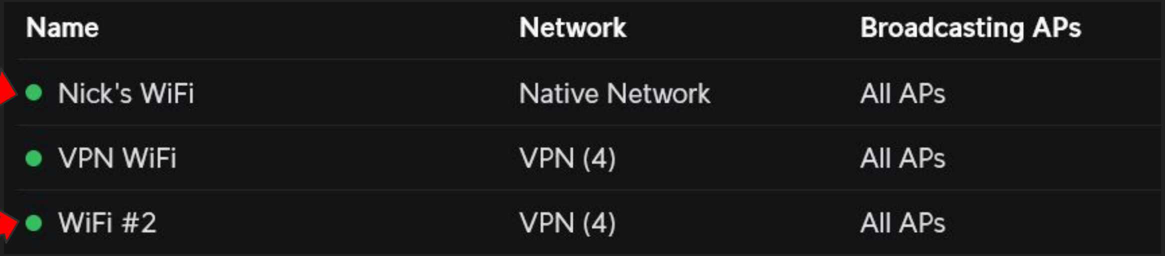
You Try! Join a WiFi and Try to Ping the Other Subnet



Name	WiFi #2
Password	Testwifi2 Must have at least 8 characters.
Network	VPN 4

Command: ping 10.1.1.29

My Computer

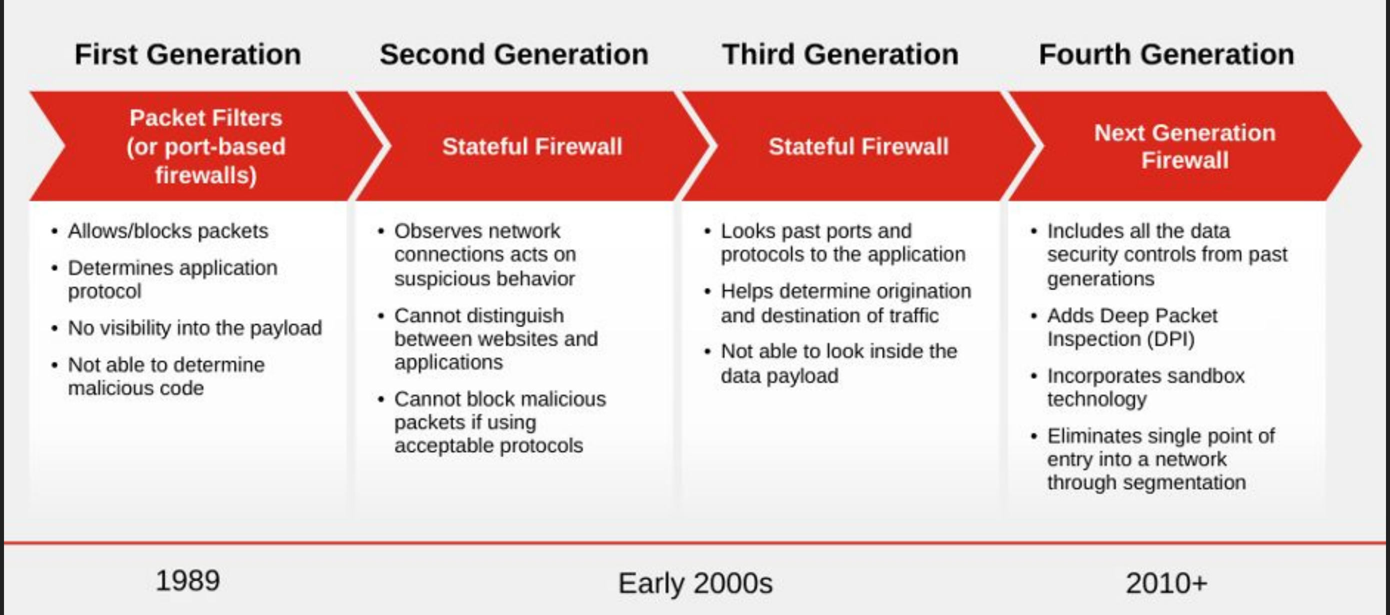


Name	Network	Broadcasting APs
● Nick's WiFi	Native Network	All APs
● VPN WiFi	VPN (4)	All APs
● WiFi #2	VPN (4)	All APs

Your computers

Firewalls

Monitors and controls incoming and outgoing network traffic based on predetermined security rules

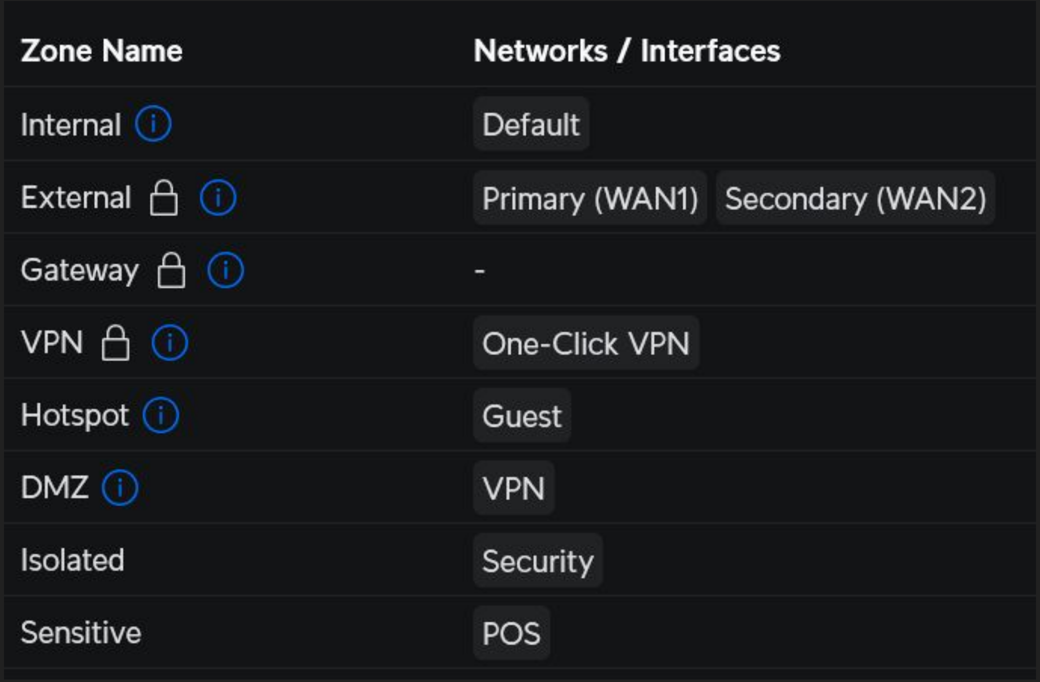


First Generation	Second Generation	Third Generation	Fourth Generation
Packet Filters (or port-based firewalls)	Stateful Firewall	Stateful Firewall	Next Generation Firewall
• Allows/blocks packets • Determines application protocol • No visibility into the payload • Not able to determine malicious code	• Observes network connections acts on suspicious behavior • Cannot distinguish between websites and applications • Cannot block malicious packets if using acceptable protocols	• Looks past ports and protocols to the application • Helps determine origination and destination of traffic • Not able to look inside the data payload	• Includes all the data security controls from past generations • Adds Deep Packet Inspection (DPI) • Incorporates sandbox technology • Eliminates single point of entry into a network through segmentation

1989 | Early 2000s | 2010+

My Firewall

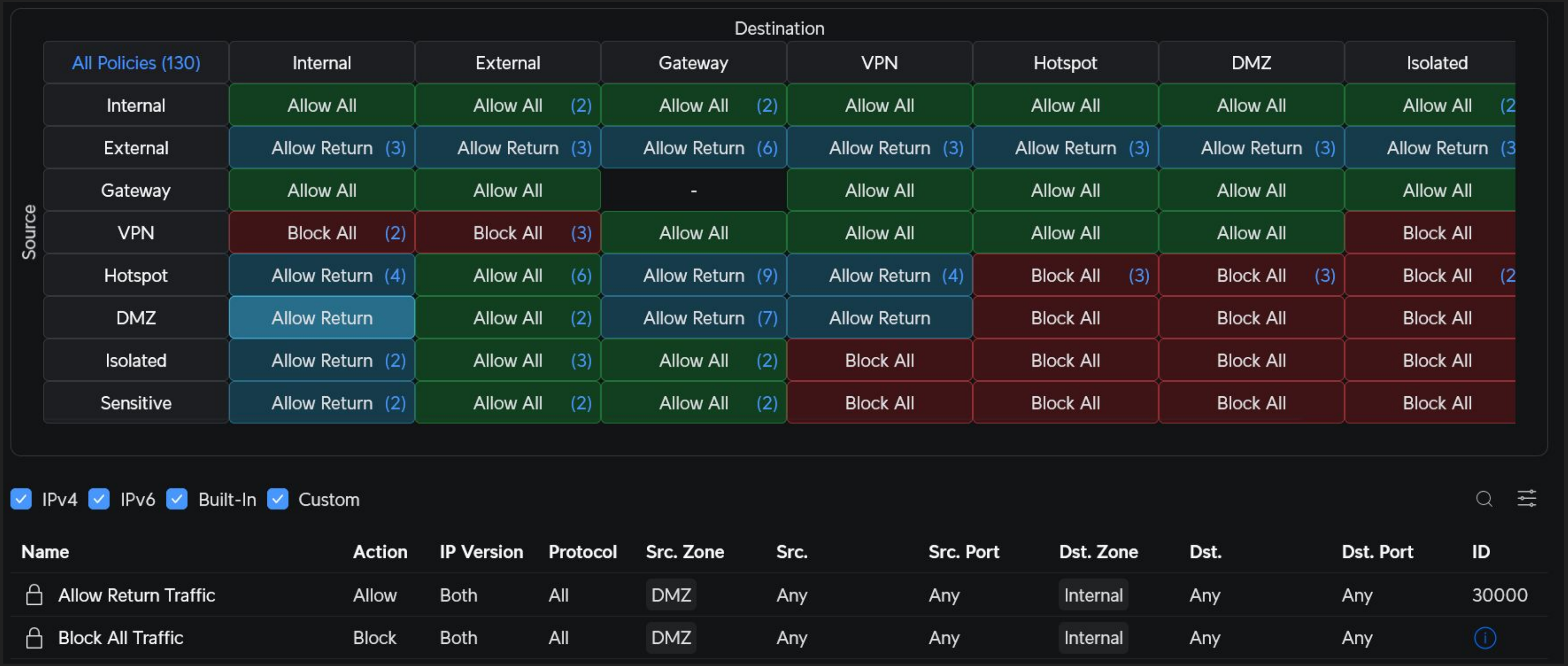
Zone based vs interface (eth0) based



Zone Name	Networks / Interfaces
Internal ⓘ	Default
External 🔒 ⓘ	Primary (WAN1) Secondary (WAN2)
Gateway 🔒 ⓘ	-
VPN 🔒 ⓘ	One-Click VPN
Hotspot ⓘ	Guest
DMZ ⓘ	VPN
Isolated	Security
Sensitive	POS

Why you can’t access my laptop

My laptop is in the internal zone, as before you cannot ping me!



Destination

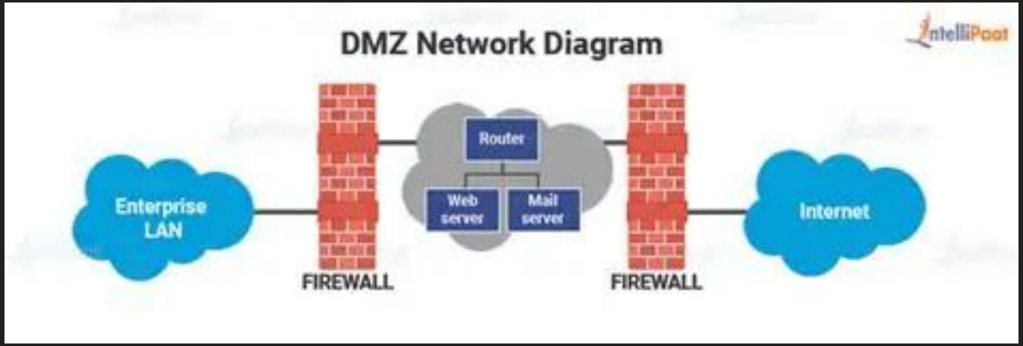
Source

All Policies (130)	Internal	External	Gateway	VPN	Hotspot	DMZ	Isolated
Internal	Allow All	Allow All (2)	Allow All (2)	Allow All	Allow All	Allow All	Allow All (2
External	Allow Return (3)	Allow Return (3)	Allow Return (6)	Allow Return (3)	Allow Return (3)	Allow Return (3)	Allow Return (3
Gateway	Allow All	Allow All	-	Allow All	Allow All	Allow All	Allow All
VPN	Block All (2)	Block All (3)	Allow All	Allow All	Allow All	Allow All	Block All
Hotspot	Allow Return (4)	Allow All (6)	Allow Return (9)	Allow Return (4)	Block All (3)	Block All (3)	Block All (2
DMZ	Allow Return	Allow All (2)	Allow Return (7)	Allow Return	Block All	Block All	Block All
Isolated	Allow Return (2)	Allow All (3)	Allow All (2)	Block All	Block All	Block All	Block All
Sensitive	Allow Return (2)	Allow All (2)	Allow All (2)	Block All	Block All	Block All	Block All

☑ IPv4 ☑ IPv6 ☑ Built-In ☑ Custom

Name	Action	IP Version	Protocol	Src. Zone	Src.	Src. Port	Dst. Zone	Dst.	Dst. Port	ID
Allow Return Traffic	Allow	Both	All	DMZ	Any	Any	Internal	Any	Any	30000
Block All Traffic	Block	Both	All	DMZ	Any	Any	Internal	Any	Any	ⓘ

DMZ (Demilitarized Zone)



You are all in the DMZ

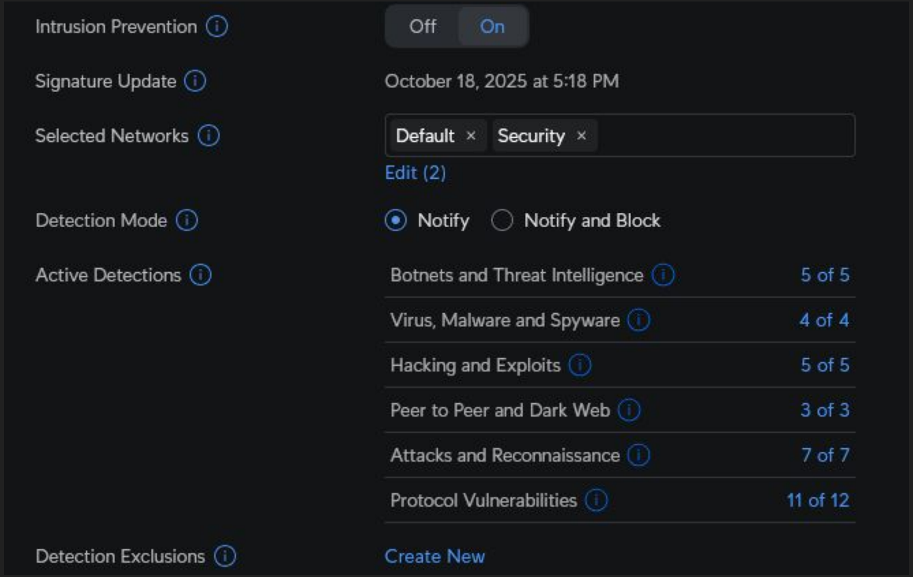
Physical or logical subnet that sits between an organization's internal trusted network and an untrusted external network (usually the internet)

I will be able to ping you all, because the firewall allows return requests from the internal network

Intrusion Detection/Prevention

An IDS monitors and analyzes network traffic or system behavior to detect suspicious activities

An IPS takes detection a step further by actively blocking threats in real-time



Intrusion Prevention: Off [✓ On]

Signature Update: October 18, 2025 at 5:18 PM

Selected Networks: Default × Security ×
Edit (2)

Detection Mode: ● Notify ○ Notify and Block

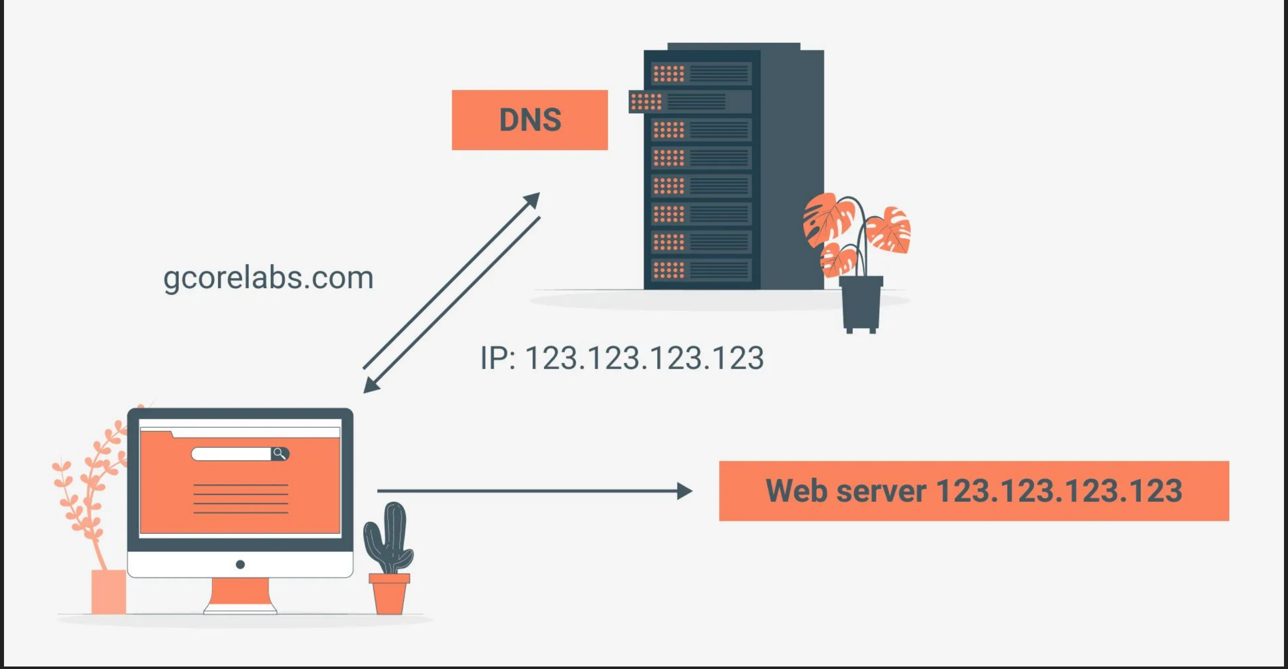
Active Detections:

Botnets and Threat Intelligence	5 of 5
Virus, Malware and Spyware	4 of 4
Hacking and Exploits	5 of 5
Peer to Peer and Dark Web	3 of 3
Attacks and Reconnaissance	7 of 7
Protocol Vulnerabilities	11 of 12

Detection Exclusions: Create New

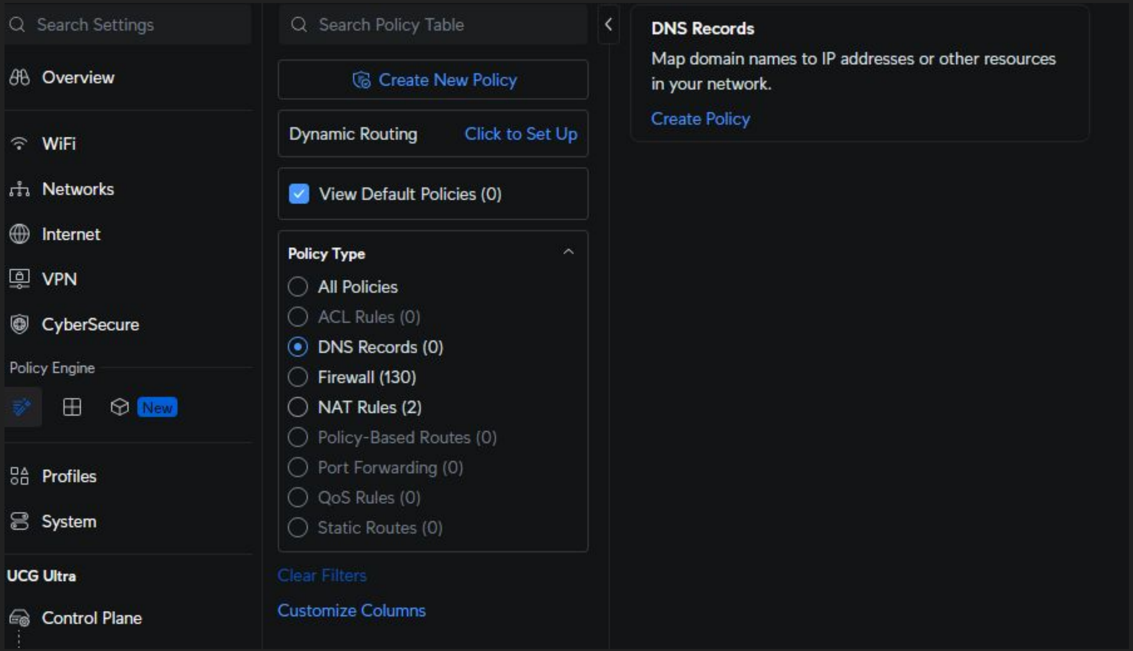
DNS

A critical component of network infrastructure that translates human-readable domain names (like "google.com") into IP addresses



Internal DNS

Large companies will have internal domain names that can only be accessed when a user is on the network



Search Settings

Overview

WiFi

Networks

Internet

VPN

CyberSecure

Policy Engine

New

Profiles

System

UCG Ultra

Control Plane

Search Policy Table

Create New Policy

Dynamic Routing Click to Set Up

☑ View Default Policies (0)

Policy Type

○ All Policies
○ ACL Rules (0)
● DNS Records (0)
○ Firewall (130)
○ NAT Rules (2)
○ Policy-Based Routes (0)
○ Port Forwarding (0)
○ QoS Rules (0)
○ Static Routes (0)

Clear Filters

Customize Columns

DNS Records

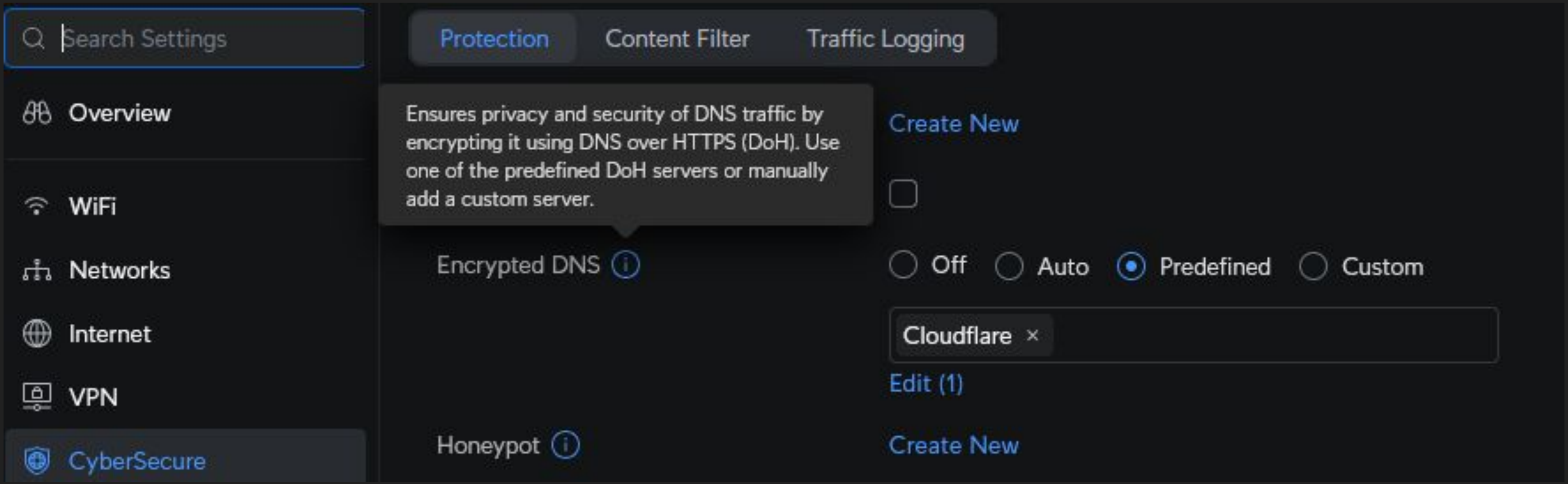
Map domain names to IP addresses or other resources in your network.

Create Policy

Encrypted DNS

Traditional DNS is sent over the network in plaintext, which is inherently insecure and can lead to eavesdropping, tampering, and manipulation

Blends in with regular web traffic, making it harder to detect or block



Ensures privacy and security of DNS traffic by encrypting it using DNS over HTTPS (DoH). Use one of the predefined DoH servers or manually add a custom server.

□

Encrypted DNS ○ Off ○ Auto ● Predefined ○ Custom

Cloudflare ×

Edit (1)

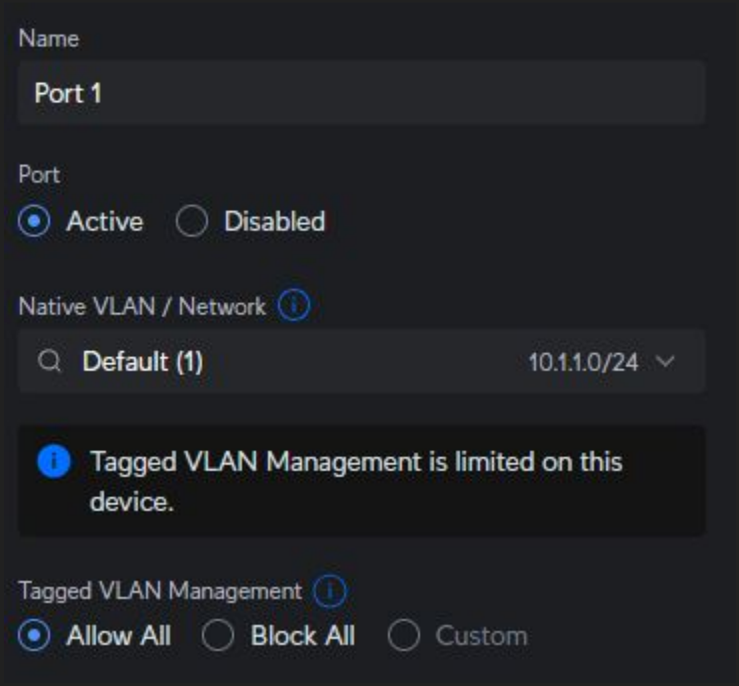
Managed vs Unmanaged Switches

Unmanaged - Plug-and-play devices with no configuration options. You simply connect cables and they start forwarding traffic immediately. BUT you can’t control how they operate or segment traffic

Managed - Configurable switches with extensive control over network behavior through a management interface (Like I will show on Unifi)

Ports

Unifi’s managed switches allow me to customize each port on each switch



Name

Port 1

Port

● Active ○ Disabled

Native VLAN / Network

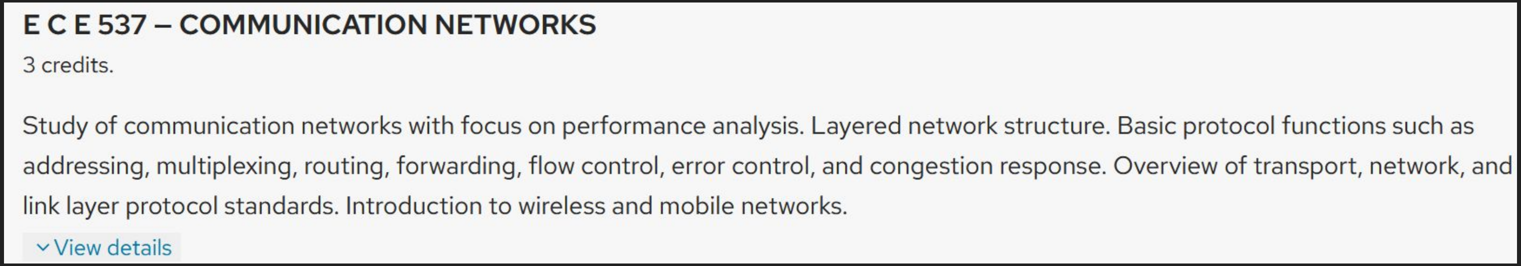
Default (1) 10.1.1.0/24

Tagged VLAN Management is limited on this device.

Tagged VLAN Management

● Allow All ○ Block All ○ Custom

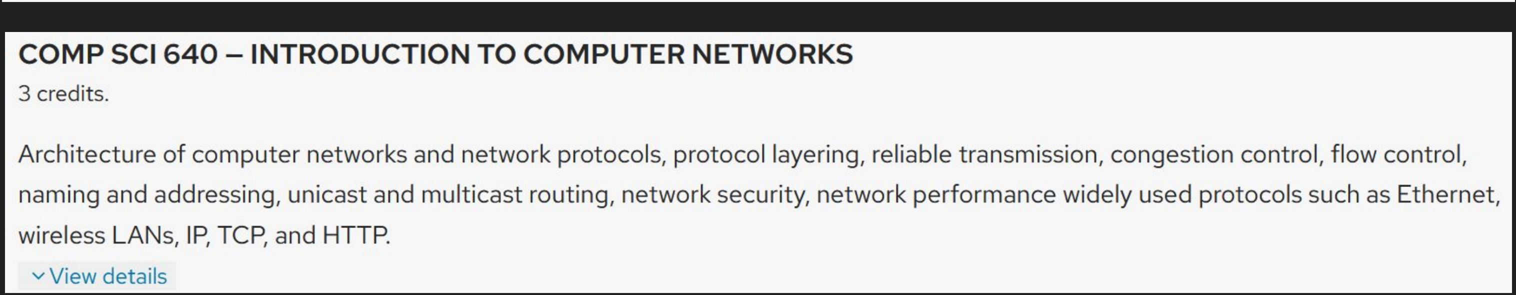
Classes



E C E 537 – COMMUNICATION NETWORKS

3 credits.

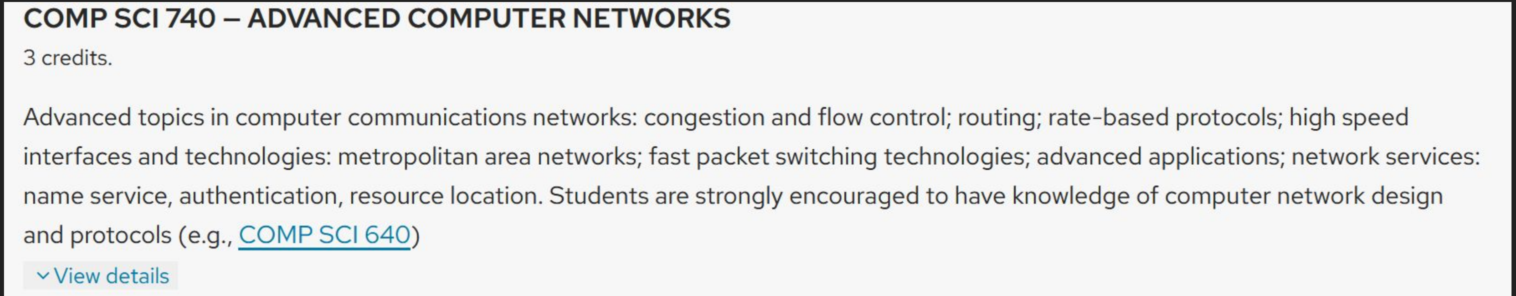
Study of communication networks with focus on performance analysis. Layered network structure. Basic protocol functions such as addressing, multiplexing, routing, forwarding, flow control, error control, and congestion response. Overview of transport, network, and link layer protocol standards. Introduction to wireless and mobile networks.



COMP SCI 640 – INTRODUCTION TO COMPUTER NETWORKS

3 credits.

Architecture of computer networks and network protocols, protocol layering, reliable transmission, congestion control, flow control, naming and addressing, unicast and multicast routing, network security, network performance widely used protocols such as Ethernet, wireless LANs, IP, TCP, and HTTP.



COMP SCI 740 – ADVANCED COMPUTER NETWORKS

3 credits.

Advanced topics in computer communications networks: congestion and flow control; routing; rate-based protocols; high speed interfaces and technologies: metropolitan area networks; fast packet switching technologies; advanced applications; network services: name service, authentication, resource location. Students are strongly encouraged to have knowledge of computer network design and protocols (e.g., COMP SCI 640)

Thank you