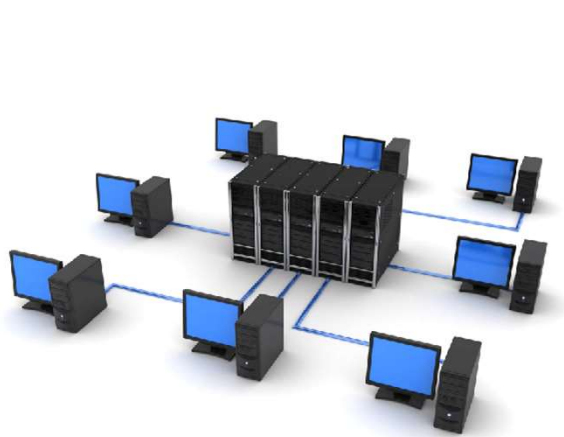


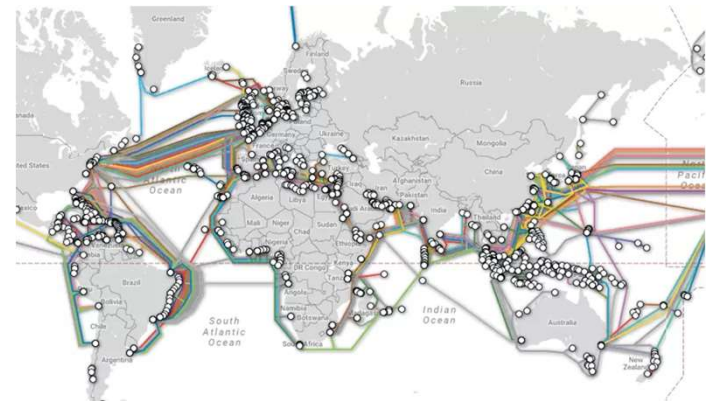
Cyber Defense Organization

Fall 2020 - Intro to Networking!!!



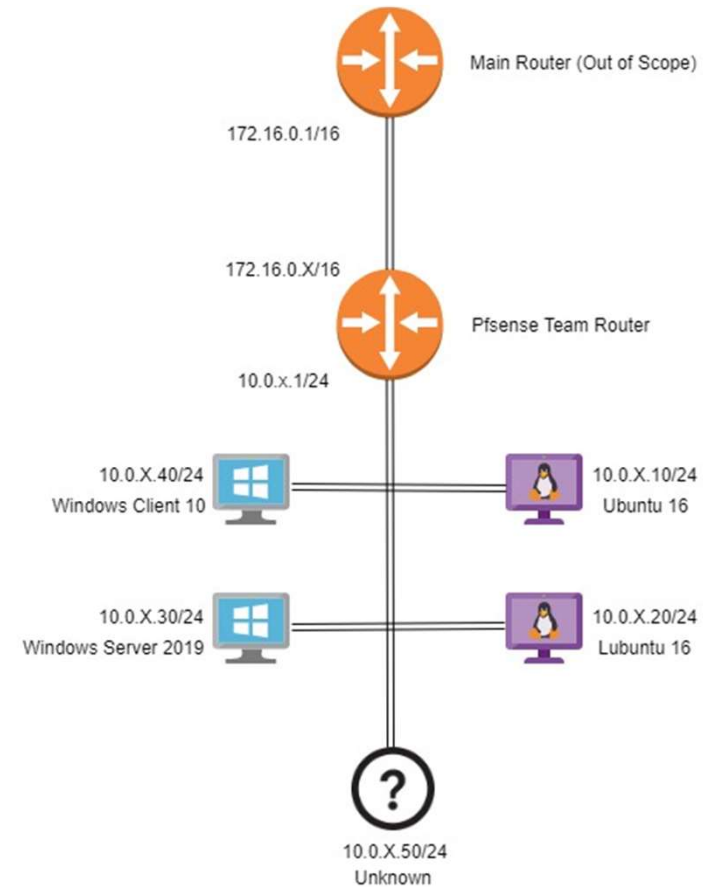
What is Computer Networking?

- Getting computers to talk to each other.
- Started with connecting tiny offices together to connecting the entire world.
- Without networking there would be no internet!
- Today's internet is just a series of connections around the world monitored and controlled by various Internet Service Providers (ISP).
 - ISP's bought giant blocks of IP addresses and are now give them out.



Network Topologies

- Topologies or network diagrams are how network architects design and manage networks.
- Many programs to build them...
 - Lucidchart
 - Visio
 - Etc.
- Without network topologies you would have to do network scans to know what's going on on each network.
- Topo from GDDC! ➔

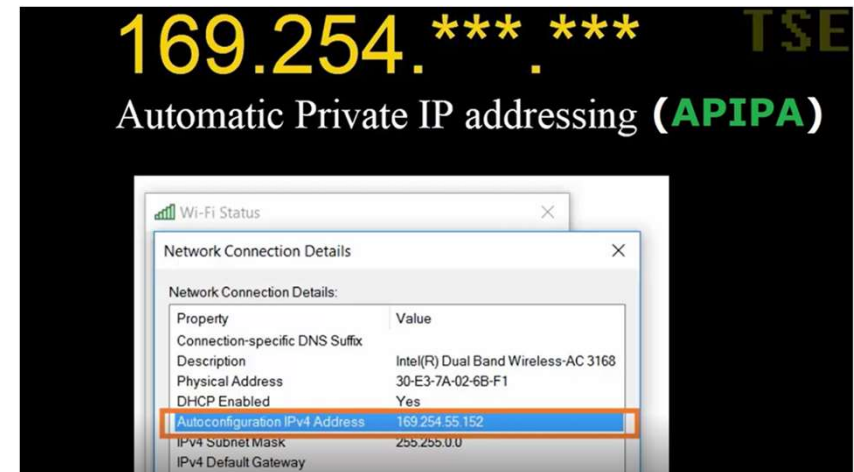


OSI Model

- While there is also a TCP model... networking people use OSI
- 7 Layers
 - Application - Bringing networking to actual services! (Next Generation Firewalls!)
 - Presentation - Encryption & Decryption
 - Session - Communications are given session IDs
 - Transport - TCP or UDP & Port Numbers!
 - Network - Packets & IP addressing & Routers!
 - Data Link - Frames! MAC Addresses! Switches!
 - Physical - Cabling, Ethernet
- Application, Presentation, and Session layers are bundled up in the TCP/IP model, because they aren't super important in networking.
- Focus on those bottom 3 layers!

IP Addressing!

- Network layer of the OSI model!
- IPv4 v. IPv6
 - IPv4 - 192.168.1.1
 - Already out of addresses!
 - IPv6 - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
 - People are afraid of this, but we are going to need it!
- Public v. Private
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- Addresses you might see
 - Local address - 127.0.0.1
 - APIPA - 169.254.0.0/16



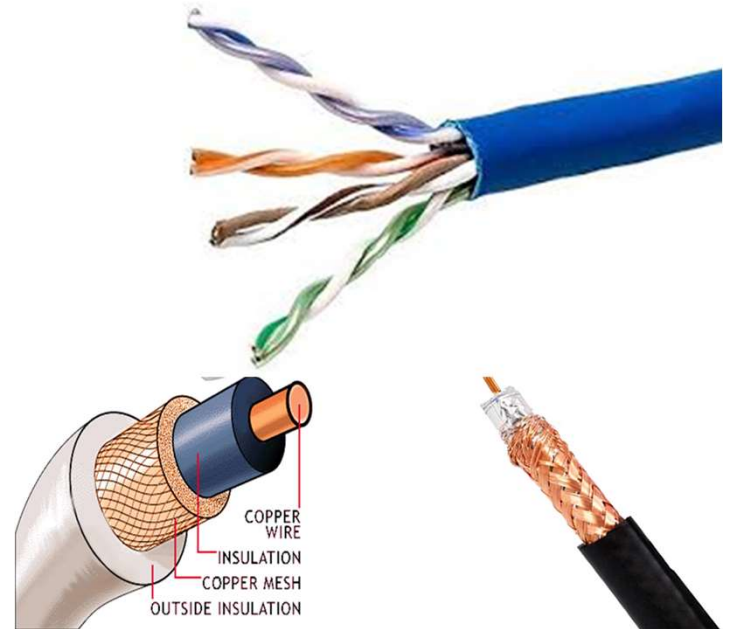
Subnetting!

- At first glance this is the scariest part of networking.
- Uses binary to separate networks.
- What you will actually use...
 - 255.255.255.0 | /24 | 254 Hosts
 - 255.255.255.128 | /25 | 126 Hosts
 - 255.255.255.192 | /26 | 62 Hosts
 - 255.255.255.224 | /27 | 30 Hosts
 - 255.255.255.240 | /28 | 14 Hosts
 - 255.255.255.248 | /29 | 6 Hosts
 - 255.255.255.252 | /30 | 2 Hosts
- There are 2 /24's in a /25
 - There are 4 /24's in a /26
 - There are 8 /24's in a /27

	Addresses	Hosts	Netmask	Amount of a Class C
/30	4	2	255.255.255.252	1/64
/29	8	6	255.255.255.248	1/32
/28	16	14	255.255.255.240	1/16
/27	32	30	255.255.255.224	1/8
/26	64	62	255.255.255.192	1/4
/25	128	126	255.255.255.128	1/2
/24	256	254	255.255.255.0	1
/23	512	510	255.255.254.0	2
/22	1024	1022	255.255.252.0	4
/21	2048	2046	255.255.248.0	8
/20	4096	4094	255.255.240.0	16
/19	8192	8190	255.255.224.0	32
/18	16384	16382	255.255.192.0	64
/17	32768	32766	255.255.128.0	128
/16	65536	65534	255.255.0.0	256

Physical Networking

- Always good to know about cabling.
- Copper Cabling
 - Cheaper
 - Max out at 10 Gbps
 - Can't run as far
 - Rj45, Coax
 - STP & UTP
 - Cat Ratings
- Fiber Cabling
 - Expensive
 - Faster!!!! 60 Tbps and beyond!
 - Can run super far!
 - LC, SC, & ST
 - Multimode v. Singlemode



Networking Vendors

In the real world a company will choose a specific vendor or two, which they use for their equipment.

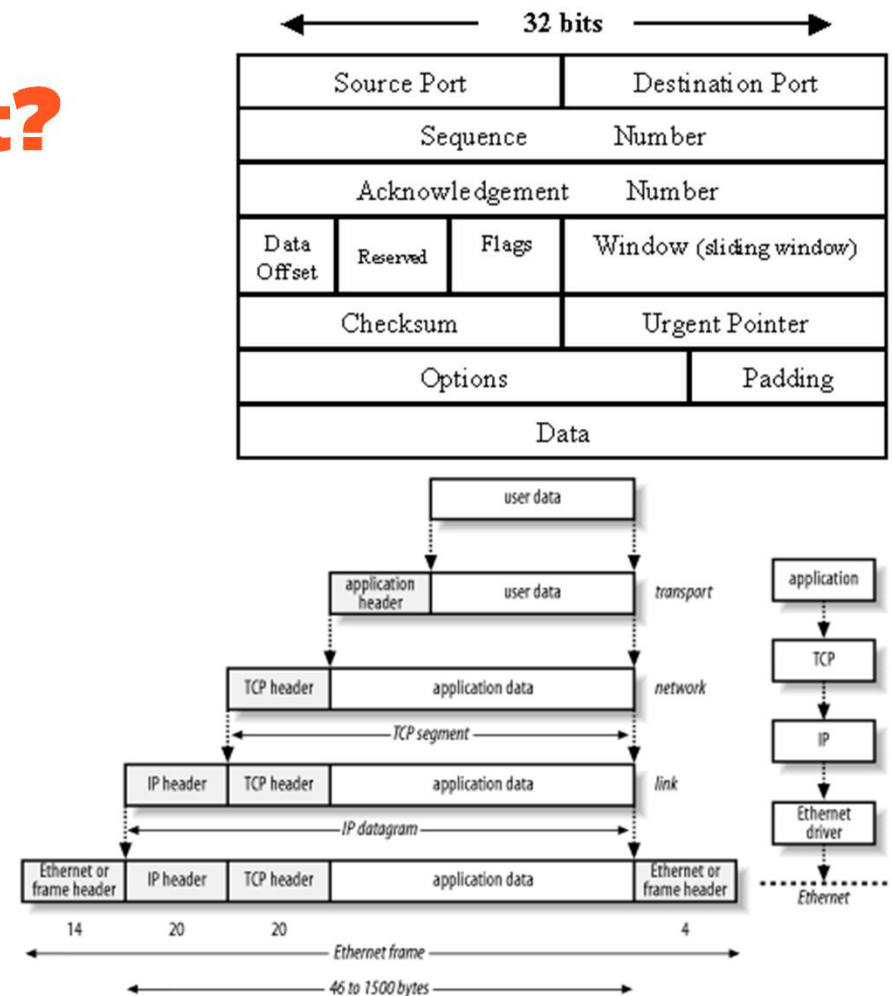
Most vendors accomplish the same goal in slightly different ways.

- Cisco
 - Routers, Switches, VPN, Certifications, & more.
- Juniper
 - Routers, Switches, VPN, & more.
- Palo Alto
 - Next generation firewall, virtual routers, certification & more.
- Pfsense
 - Open Source firewall, used in many competitions.



What Makes a packet?

- Packets are made up of bytes just like everything else on computers.
- Encapsulation
 - At the center a packet is just the data you want to send to another computer.
 - Around that data you need to put all the necessary information to get it to its destination.
- Packets are malleable!
 - They can be broken up, dissected, changed, packaged back up, inserted with new data, etc.



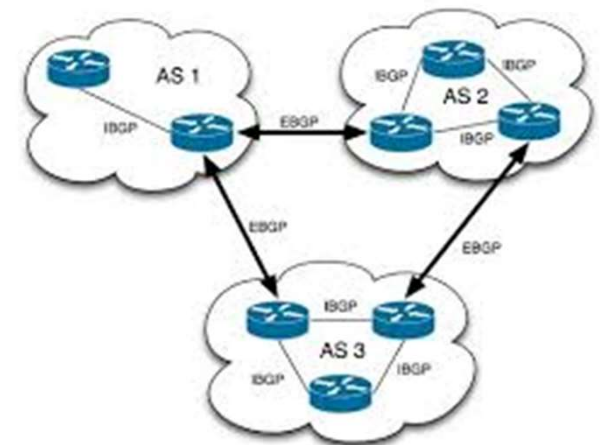
Routing Protocols!

Distance vector	Link state
sends the entire routing table	sends only link state information
slow convergence	fast convergence
susceptible to routing loops	less susceptible to routing loops
updates are sometimes sent using broadcast	always uses multicast for the routing updates
doesn't know the network topology	knows the entire network topology
simpler to configure	can be harder to configure
examples: RIP, IGRP	examples: OSPF, IS-IS

Routing protocols are used to dynamically share routes, so you don't need to statically route everything.

Routes are like directions!

- Routing Information Protocol (RIP)
- Interior Gateway Protocol (IGRP)
- Open Shortest Path First (OSPF)
- Exterior Gateway Protocol (EGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP) (What the internet is run on!)
- Intermediate System-to-Intermediate System (IS-IS)



Virtual LANs (VLANs)

VLANs are used all the time in networking to segment networks and devices.

- VLANs are two separate networks that can live on the same device.
 - To change between VLANs the packet needs to go to a router.
- Certain ports can be assigned to a VLAN.
 - Trunking is when a port is configured to transport traffic for multiple VLANs.
- IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.
 - Remember dot1q encapsulation for the hands on!

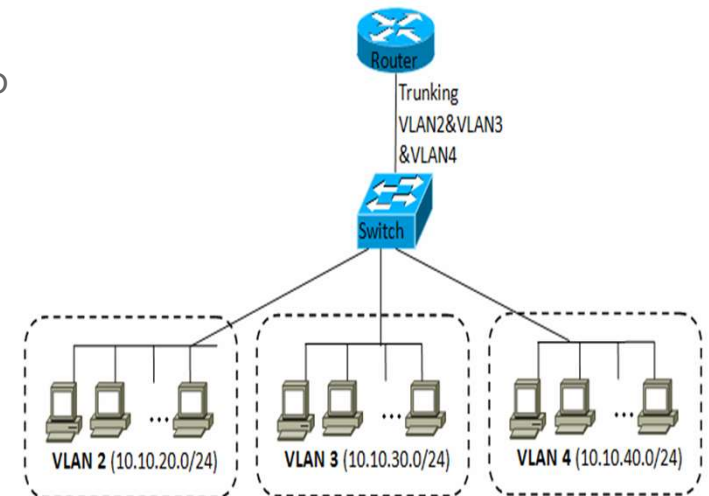
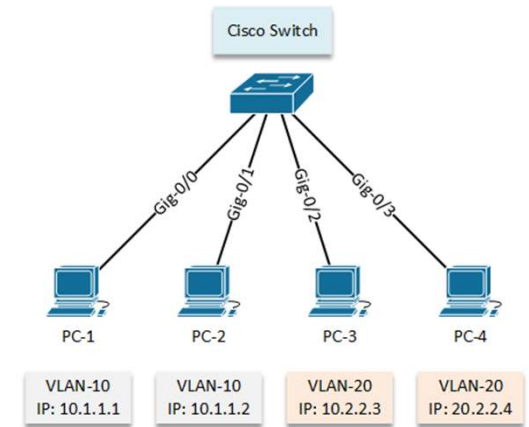
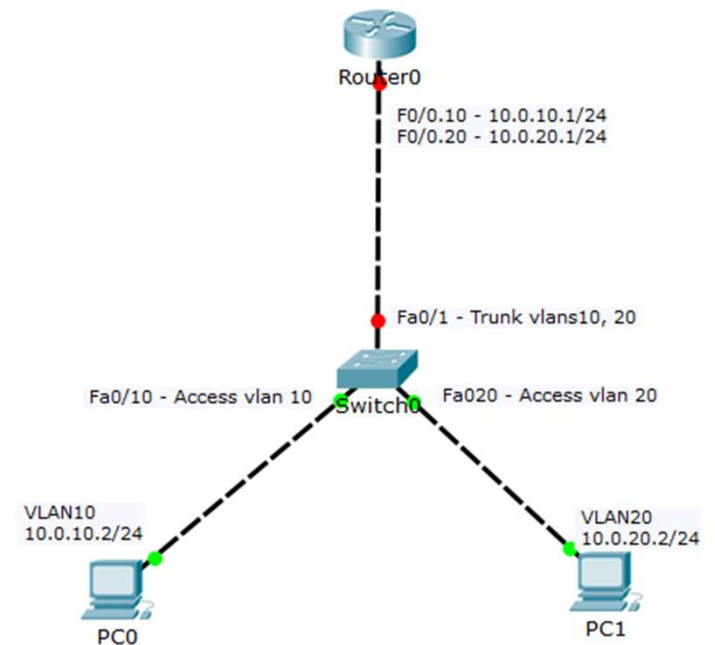


Figure 12.5. 802.1Q trunk between the router and the switch

Virtual Interfaces

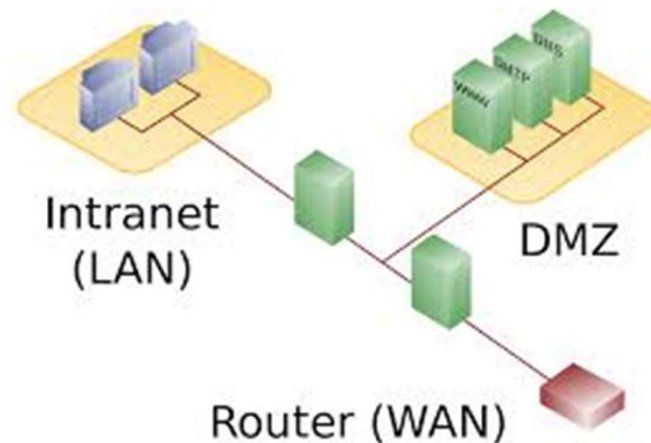
- These are interfaces that are treated like physical interfaces
- Types of Virtual Interfaces
 - Sub-Interfaces
 - Gi 0/0/0.10
 - Router on a stick!
 - (What we'll do in the hands on!)
 - Vlan Interfaces
 - Vlan 101
 - Loopback Interfaces
 - Loopback599
 - Tunnel Interfaces
 - Tunnel1



Network Security

Up to this point we have covered how networks are configured and how they run, but how do we secure our network?

- Firewall rules
- Access lists
- Next Generation Firewalls
 - Packet Inspection
 - Layer 7!
- Secure Architecture
 - DMZ
 - “Never trust, Always verify”
- VPN
 - GRE, IPsec, L2TP, PPTP, SSL & TLS, OpenVPN



Firewalls & Access Control

A lot of network security can be seen through creating different “rules” that give access to your network.

- Access control lists
 - Basic implementation of rule based policy.
 - Can be implemented with ports, but is most often used to block subnets from a device.
- Firewall rules
 - Most common implementation.
 - IP and Port based rules that allow access to different zones in a network.
 - Can fall short when services are serviced on non-standard ports or an attacker sends the wrong traffic through a port.
- Next Generation Firewalls
 - Uses Layer 7 to inspect application used in a packet.
 - AppID, Content Filtering, URL Filtering, Packet inspection, decryption, & more!

Zero Trust Model vs Perimeter Model

Secure network architecture is more than half the battle in securing your network.

- Perimeter

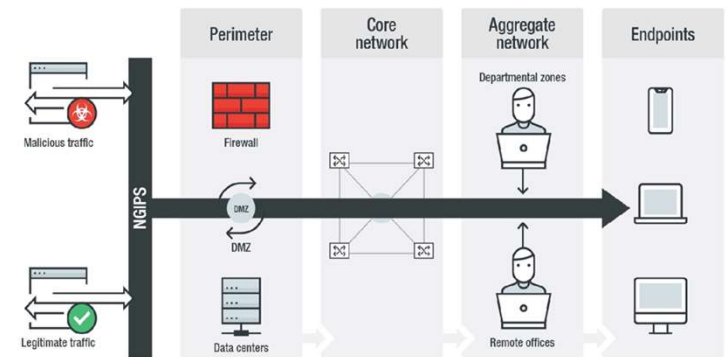
- Network architecture where firewalls are used to separate un-trusted WAN and trusted LAN with a secure DMZ thrown in.
- NOT SECURE!
- C2's and other offensive measures make getting into the LAN and privilege escalation easy.

- Zero Trust

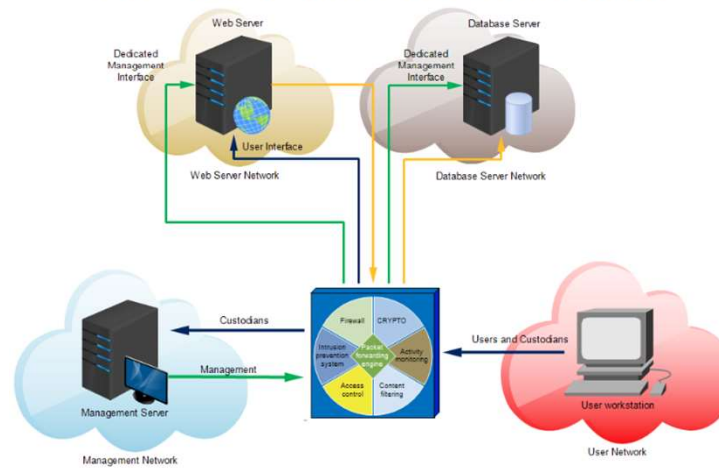
- New standard that states all actions in a network must be logged and verified.
- There should be no implicitly “trusted zone”.
- Users should be tracked.
- No admin cred that can access everything.
- “Never Trust, Always Verify”
- Every action should go through a secure network device before it moves to a different zone.

Zero Trust Model vs Perimeter Model

Perimeter →



"Zero Trust" Network Architecture



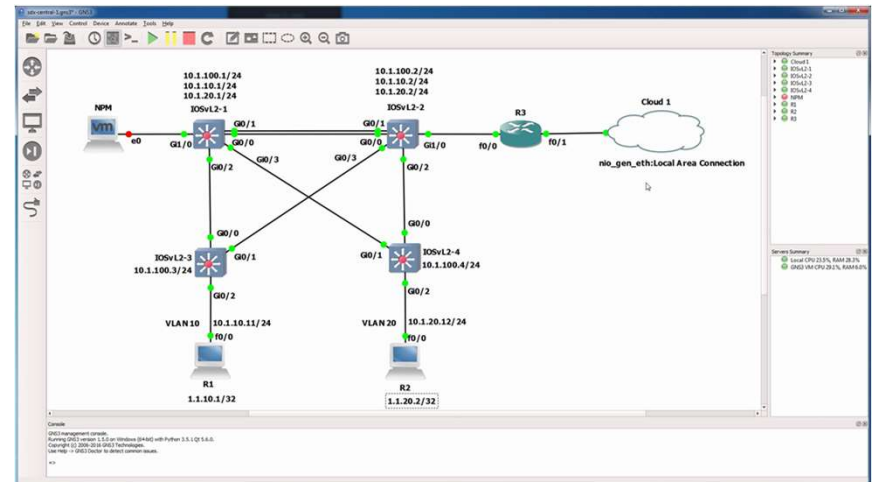
(Source: Drs. Albert Spijkers)

Zero Trust -->

How to set up your networking homelab!

Networking can be one of the hardest things to virtualize! You need a whole network to practice.

- Virtualization
 - Cisco Packet Tracer
 - GNS3
- Physical Hardware
 - Ebay!!!!!!
 - While virtualization is great, if you really want to deep dive physical hardware is great.



Networking Certifications!

- Cisco Certifications
 - CCNA
 - CCNP
 - & more!
- Palo Alto Certifications
 - PCCSA - Cyber Security Associate
 - PCNSA - Network Security Administrator
 - PCNSE - Network Security Engineer
- Comptia
 - Network +



Hands On!

CISCO Packet Tracer!

<https://tinyurl.com/net-hands-on>



Coming up next week!

Tuesday: Blue Team Practice @ 7pm

Wednesday: Security + @ 5pm

Thursday: Red Team Practice @ 7:30pm

Friday: Intro to Metasploit @ 3pm



Add us on Social Media!

Twitter: **@ualbanyCDO** 

Instagram: **ualbany_cdo** 

Myinvolvement: **Cyber Defense Org**

Twitch: UACyberDef

We have a discord!

(discord is for UAlbany Students only)

