Section 12: Advanced Networking Devices

89. Understanding IP Tunneling

VNC Server - Free product

VNC Server <------unencrypted-------> VNC Client

To encrypt you could rewrite the program with encryption OR the better optinon, you can piggyback off a protocol that is already encrypted.

Tunnel:

ex. use ssh program like putty to safely send data. The SSH encrypts the information when it's sent out from the VNC Client and then the SSH at the VNC server will decrypt the information.

A tunnel starts by making an encrypted connection between two computers

The purpose of Tunneling is to provide encryption where normally there isnt.

Review:

**Very few internet protocols are encrypted
**Tunnels canencapsulate unencrypted protocols
**Tunnels are often used with remote access connections

---

90. Virtual Private Networks

*VPN (Virtual Private Network) - Tunnel connection for remote computers to get to a designated endpoint

Remote connection challenges:

-LAN often uses private IP addressing
-Remote device needs private and public IP address
--Public address to get to the network
--Private IP address to reach the LAN

VPN Types Microsoft

PPTP - Point to Point tunneling Protocol
L2TP - Layer 2 Tunneling protocol with IPsec
SSL - Secure Socket Tunneling Protocol (SSTP)
IKEv2 - pure IPsec VPN

*A Client-to-site VPN connects a remote computer to a local network

*VPN concentrator can be a dedicted device that acts as an endpoint for the network

*A site-to-site VPN connects distant networks into a single network

Review:

*know why we use VPNs and some of the technology we can choose from.
*You will see PPTP, L2TP, SSL will all be on the exam

Review:

*A VPN creates a secure tunnel so a remote machine or network can be part of a local network

*A client-to-client VPN connects a reomte computer to a local network.

*A site-to-site VPN connects distant networks into a single network.

---

91. Introduction to VLANs

VLAN (Virtual LAN) - Splits one broadcast Domain and splits it into two or more Broadcast Domains.

Two types of switches

1. Unmanaged Switches - Simple devices, Only do switching
2. Managed Switches - Offer other features (i.e. VLANs)

Managed Switches have IP addresses that enable connection and configuration

Switches run at Layer two of the OSI model

CNA (Cisco Network Assistant) - this is used to configure cisco routers

*All switches default VLAN is VLAN 0 for COMPTIA. In real life they are default at 1.

Static Access is a manual mode
VLAN Trunk Protocol - Trunk ports move traffic from all VLANs between switches

Review:

*A VLAN splits one broadcast domain into two or more broadcast domains

*A Managed switch that supports VLANS require configuration

*Trunking enables VLANs to be on more than one switch

---

92. InterVLAN Routing

A router can connect to VLANS

InterVLAN routing is a virtualization of the funtions of a router that is put into highter end switches. (Acts like one or more routers)

Review

*VLANs create separate broadcast domains
*Connect the broadcast domains with physical routers
*Broadcast domains can be connected with virtual routers using interVLAN routing

---

93. Interfacing with Managed Switches

Managed switches require configuration

Use a switches IP address to connect it

Concosole port can be used to connect to and manage a switch or router.

Rollover Cable (a.k.a Yost Cable)

PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - Telnet

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM3

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

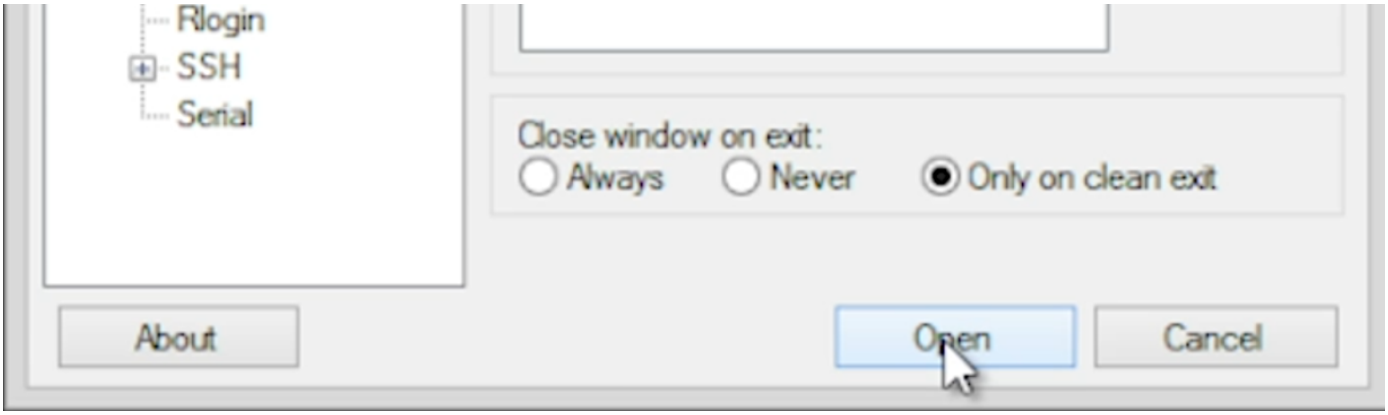
Saved Sessions

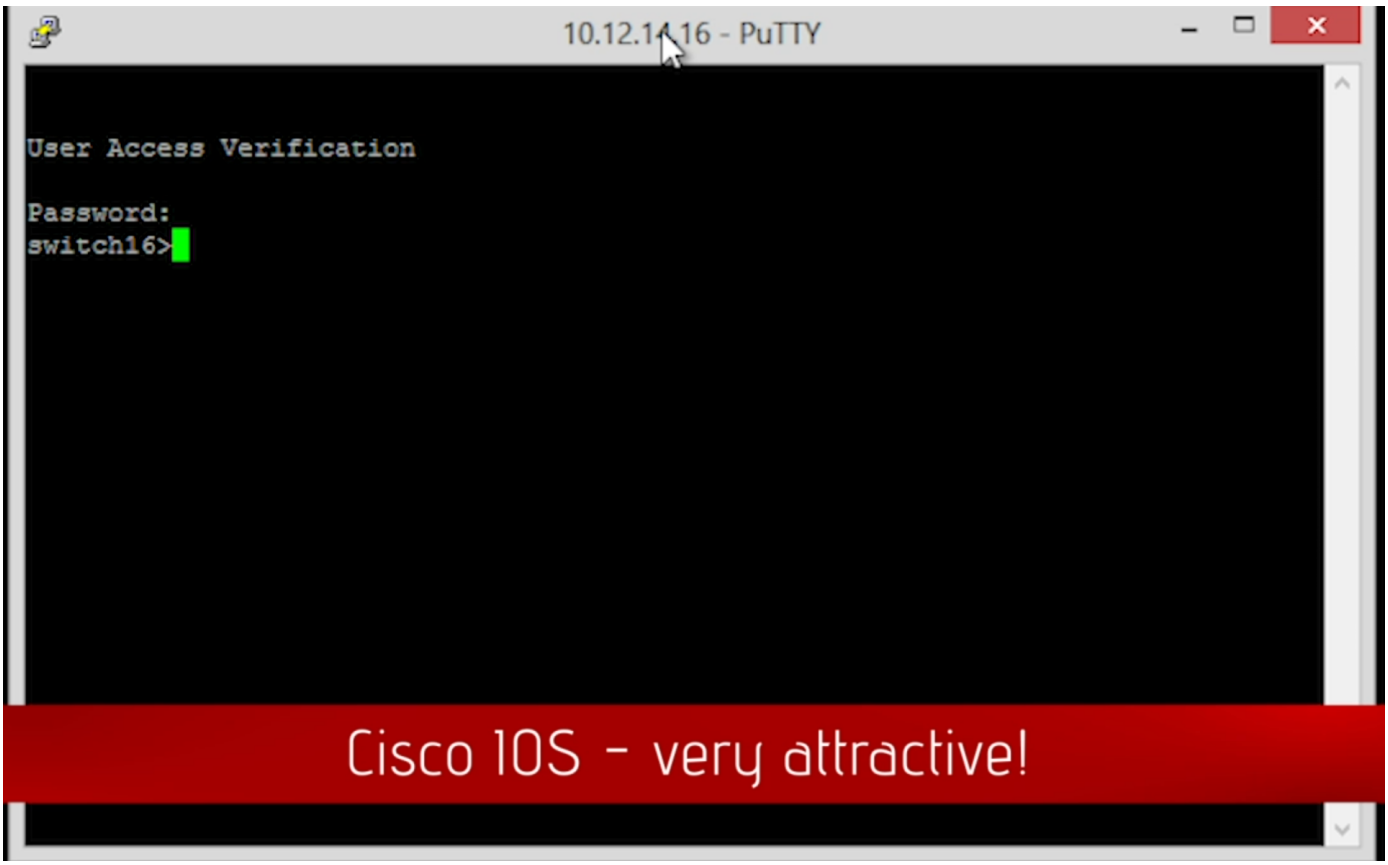
Default Settings

Load

Save

Delete





SNMP - Simple Network Management Protocol
IGMP - Internet Group Management Protocol - If doing multicasting this needs to be enabled

Review:

*managed switches require configuration
*Connect to a managed switch via an IP addres or console port
*Cisco routers and switches use a proprietary IOS

---

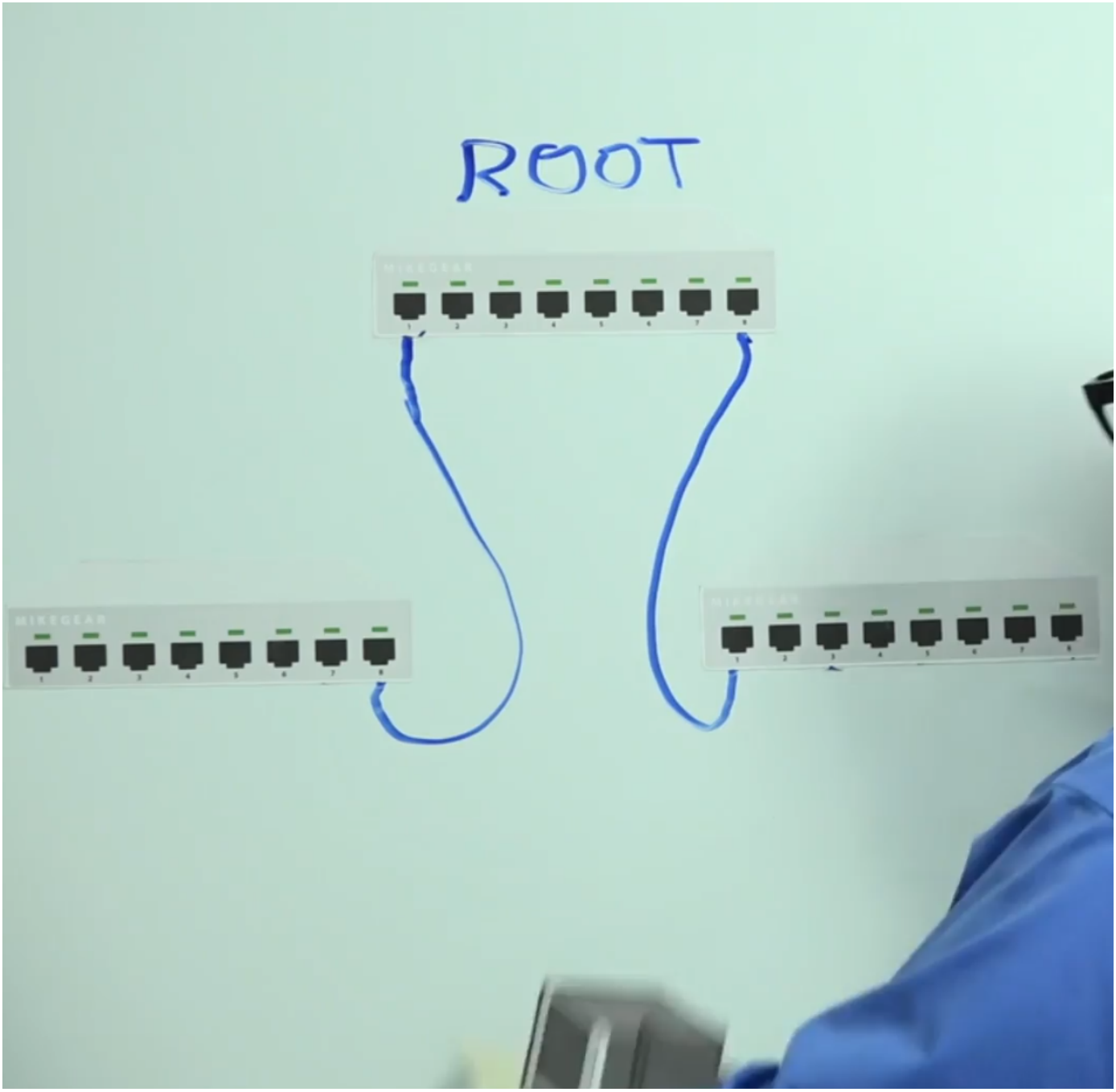
94. Switch Port Protection

Switch Port - CompTIA coined term to differenciate a regular port from a port in a switch.

STP (Spanning Tree Protocol) comes on most all managed switches - Detects bridging loops and turns off the bridged port.

Root Guard was used to combat people from plugging in their own switch and calling theirs the "root bridge".

The root bridge is the primary switch. Which all others are plugged into.



BPDU Guard (Bridge Protocol Data Units Guard) - You can configure a switch recognized that the only thing that will ever be plugged into them is a computer and NOT another switch. When a switch is plugged into one of these, they (the switch with BPDU Guard) starts sending out BPDUs and the moment that happens the port completely disables itself to eliminate any security risk.

DHCP Snooping - There should be only one DHCP Server in Any Broadcast Domain. However its easy to put in another DHCP server. So, you can configure the switches to connect to a specific DHCP server. If a rogue DHCP server is plugged in, ports start to shut down.

Review:

*Switch port do not use IP addresses or work with Layer 3
*Switch interconections use STP to detect looping by deactivating the port, if necesary
*BPDU guard is a Cisco method allowing only non-switch devices to connect to the switch

95. Port Bonding

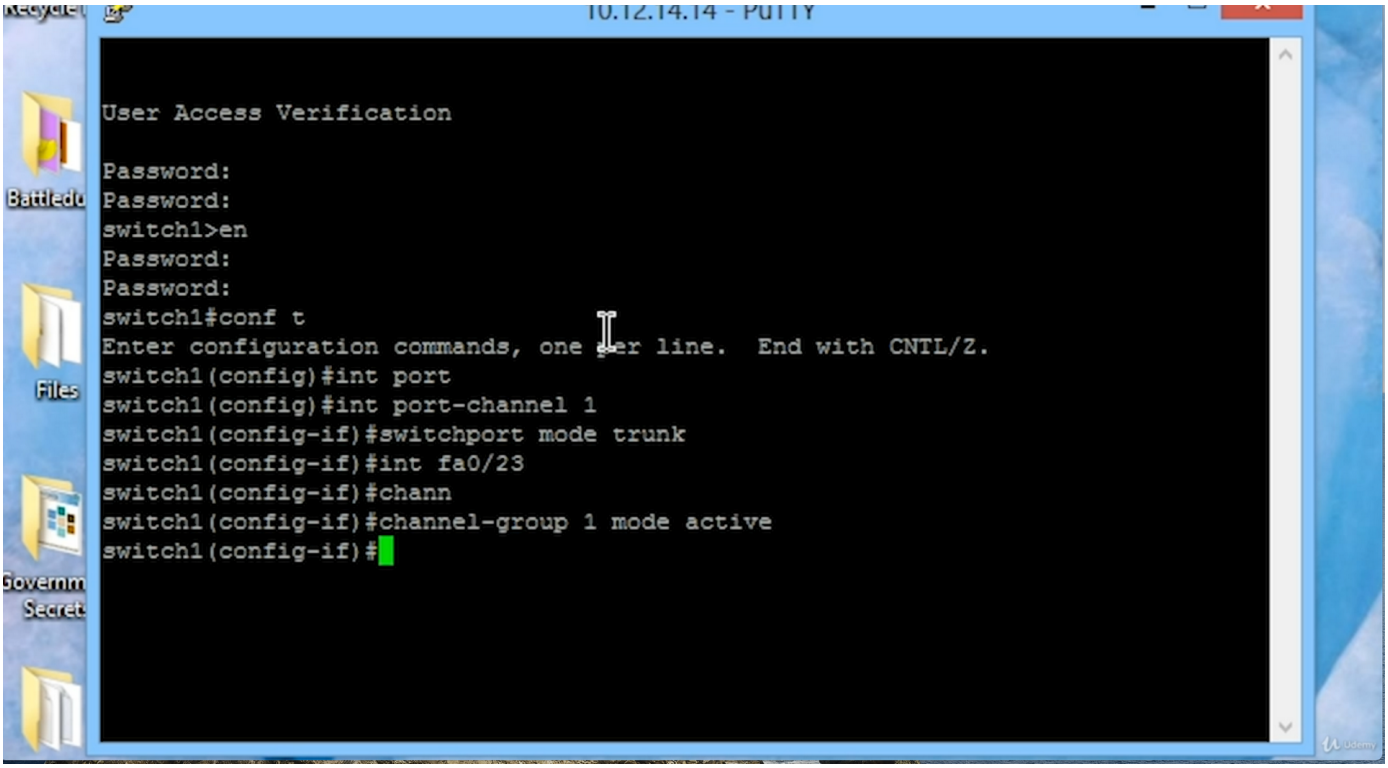
Port bonding has many names but for compTIA it is referred to as "Port Bonding" (aka NIC teaming, port aggregation)

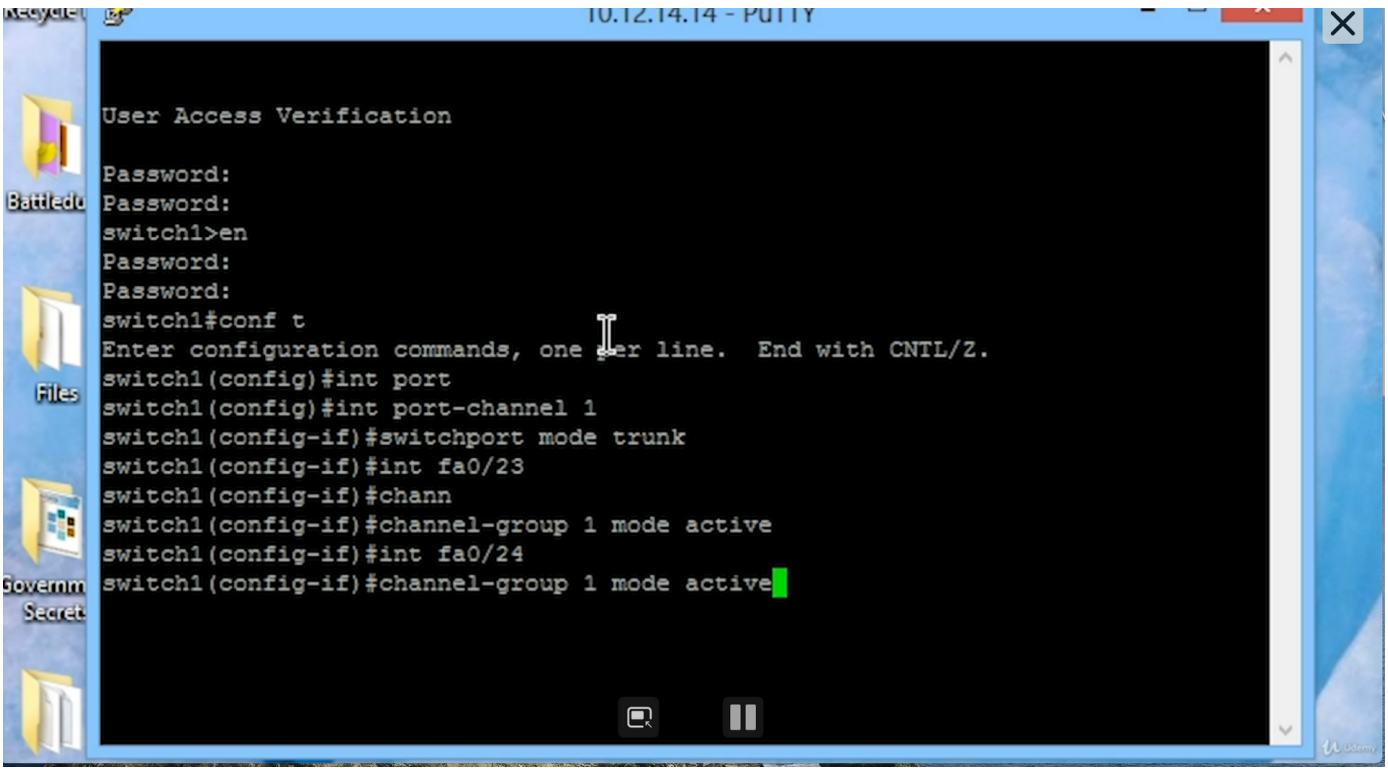
*This is taking two or more ports and bonding them together so that they will work as one higher speed port.

Two ports on each switch working together:

1. Make a group
2. assign switch ports to the group (Group ports 23 and 24)

*LACP (Link Aggregation Control Protocol)
Group = Port Channel





For the exam:

*When setting up the ports you need to set one as active and one as passive OR Both as active. If you set them both to passive it will not work.

*DO NOT go into configuration and pull out one of the ports before pulling the actual cable out of the port. YOU MUST pull the cable out first before pulling the port out using configuration settings.

Review:

- Port Bonding links switchports to increase bandwidth
- Use LACP for the trunking protocol

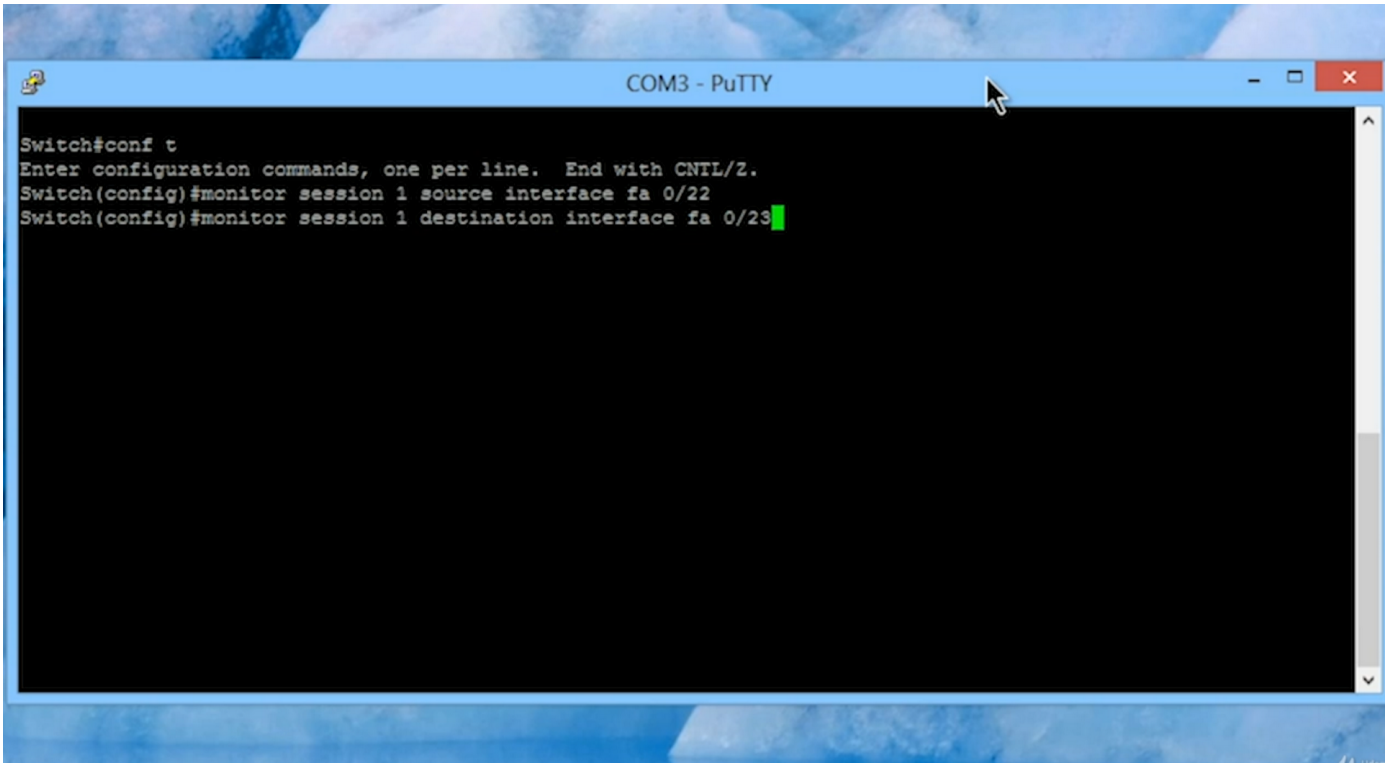
- Set ports to active

---

96. Port Mirroring

Monitoring IP traffic remotely (port sniffing)

use PuTTY to create a sniffing session and add a destination (Cisco Devices)



Review:

- Port Mirroring enables the traffic flowing through one port to be monitored on another port
- This feature enables administrators to remotely inspect traffic from a suspicious machine
- Port Mirroring is configured on a switch by providing a source port and a destination port.

---

97. Quality of Service

Traffic Shaping - controlling traffic based on all types of things. (Based on IP, MAC address, ports, activity, etc.)

Most common way to do traffic shaping is using Quality of Service (QoS)

Review:

- Quality of Service (QoS) controls help better manage available bandwidth
- One type of QoS control is Traffic Shaping
- Simple QoS on SOHO routers allows priority setting for different protocols

---

98. IDS vs IPS

IDS (Intrusion Detection System) - can be a computer or device with specialized IDS software. Using this computer or device is in the network and monitors the network for bad things. If the IDS detects something on the network the IDS lets someone know.

IDS out-of-band does monitoring and alerts

"Active IDS" it old terminology for IDS software that with do something about a found intrusion

Active IDS is now referred to as IPS (Intrusion Prevention System)

IPS is usually right behind the router/firewall before the internal network. This allow the IPS to stop whatever is happening.

IPS in-band actively stops or rejects.

In-band (route from local network to internet)
Out-of-Band (In the local network)

Know firewall vs. IPS vs. IPS for the Exam

Review:

- Intrusion detection systems detect and report possible attackes to the administrators
- Intrusion prevention systems run in-line with networks and act to stop detected attacks
- a firewall filters
- an IDS notifies
- An IPS acts to stop

---

99. Proxy Servers

Beware of questions on the exam where you may have to add proxy servers to particular situations.

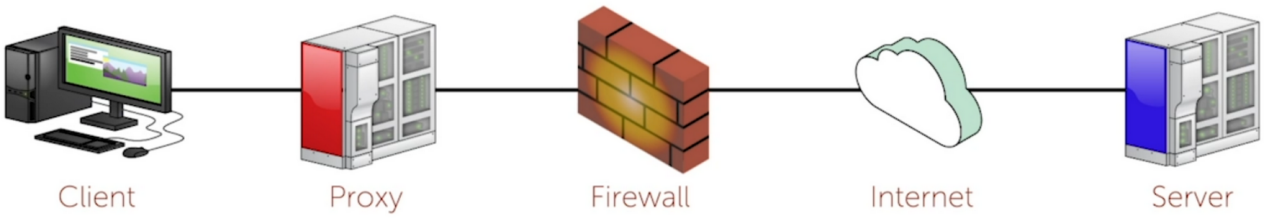
*What we need to know about proxy servers:
-They are application specific (e.g. Web Proxy, FTP proxy, VoIP proxy)

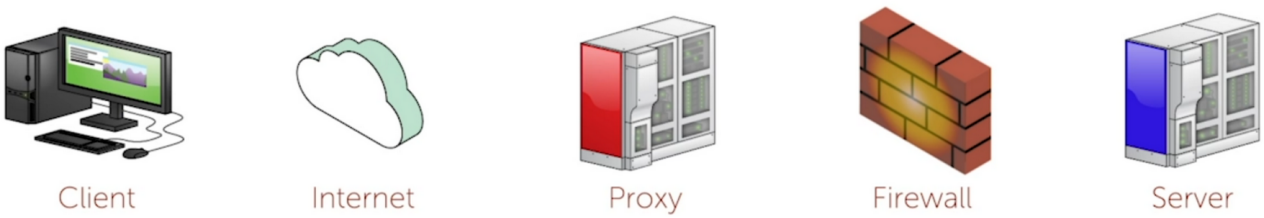
*Transparent proxy - has to be inline between the network and the web.

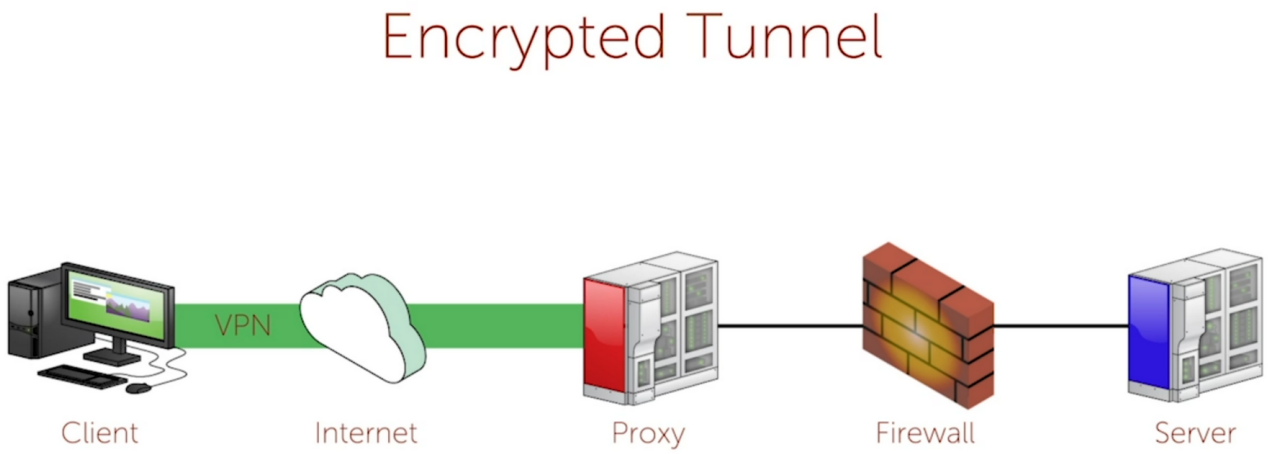
Two kinds of proxies:

1. Forward Proxy Server (Old school/Traditional)
   Represents the client
   Dedicated box or software that is in an organization (e.g. Schools)
   Provides Caching
   Provides content filtering
   Acts like a firewall

Forward Proxy

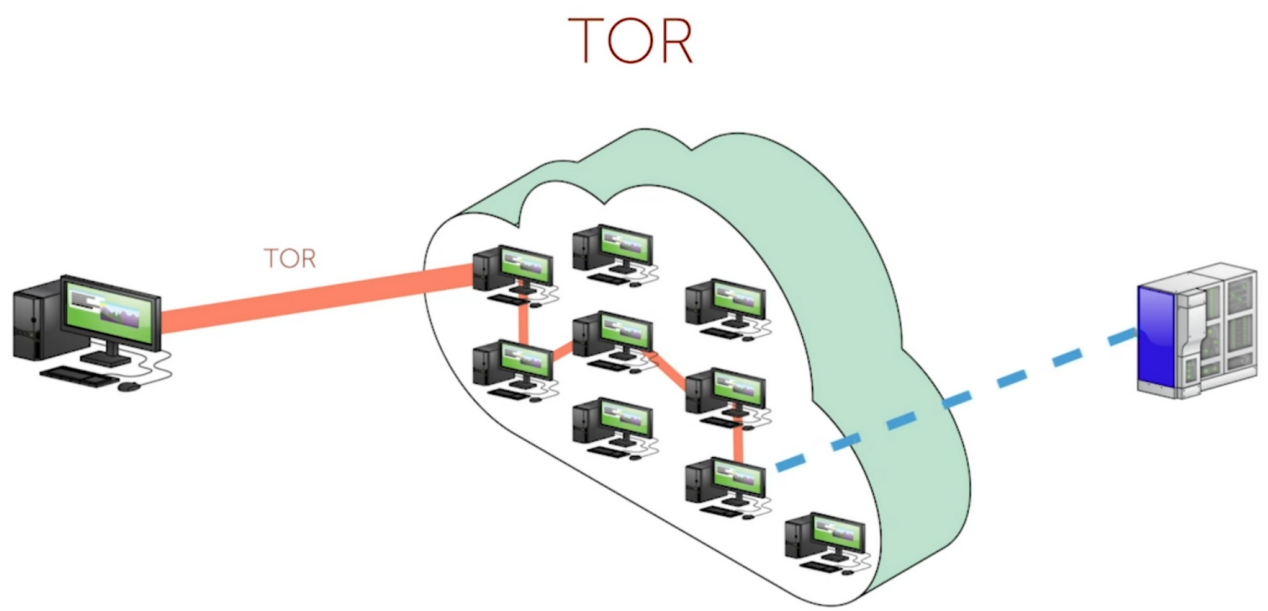






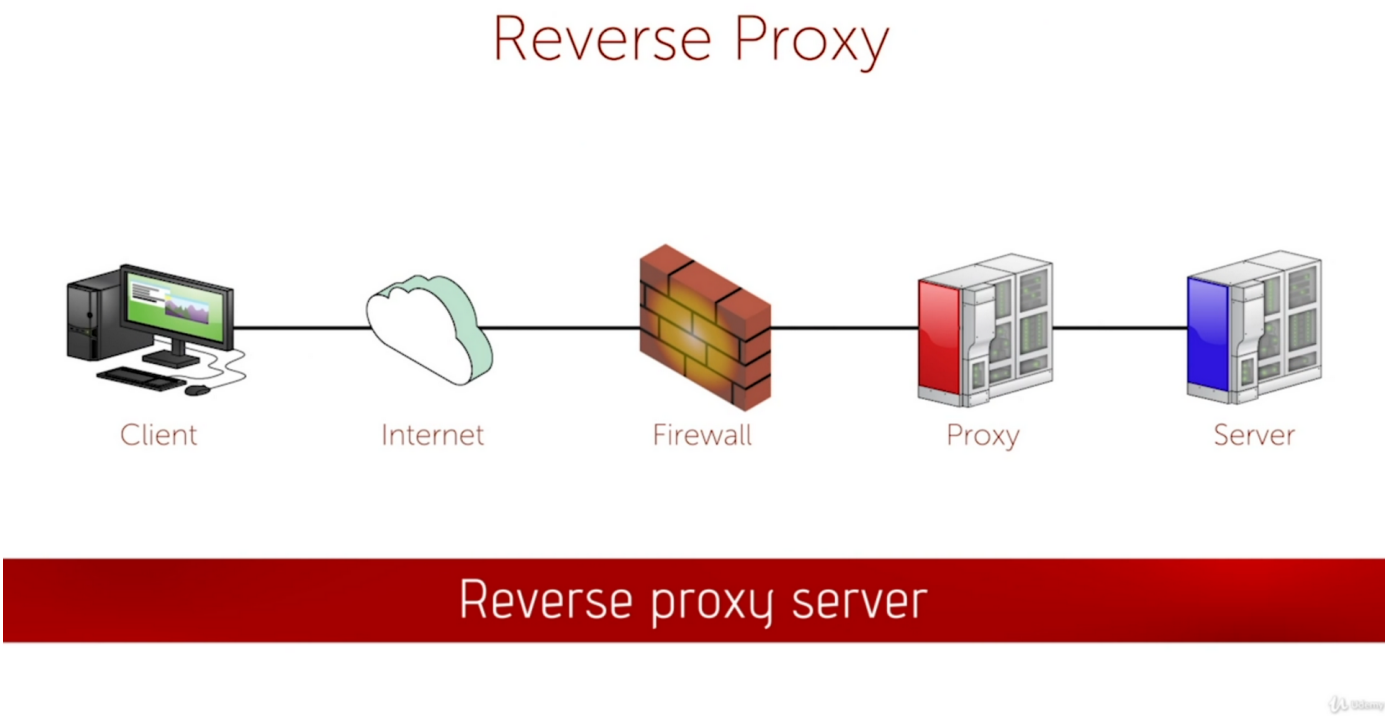
hide.me (proxy server)

VPN's still point back to you even though people cant see what you're doing. But things like TOR use a bunch of VPNs randomly before connecting you to a proxy server.



2. Reverse (Modern/used for bad stuff)
   The proxy server represents the web server (not the client)
   High Security
   Handle DoS attackes
   load balancing

caching
Encryption Acceleration



Review:

*Be confortable with a forward vs a reverse proxy server
*Forward Hide the clients from the server by forwarding the message to the server
*Forward Proxy servers can be configured for caching, content filtering, and firewall capability.
*Reverse proxy servers hide the servers, and can provide load balacing and caching for high activity pages.

---

100. Load Balancing

Load Balancing - is the ablitiy To be able to have lots of servers giving out the same thing in a smooth (nice) way and not overload them.

Ways to do this:

1. Use a DNS Server (on the exam) -

Round Robin via DNS: sets a look up zone If you have three servers running the same web page, each time a request comes in to visit the webpages the DNS passes it to the next server. So a request comes in and it passes it to server 1, then another comes in and it passes it to server 2, etc. Then the server caches the IP address to remember the visitor.

2. Delegation via DNS: Sets up a reverse look up zone to find the closest DNS server to the web server.
3. Server-side Load Balancing: involves a smart devices running smart software that is PHYSICALLY AT THE LOCATION of the servers.

-Benefits to having them at the same location: you can do "Clustering"
-Clustering is when you have your servers in a local network and they share information.
-The smart box (load balancer) can talk to each server and query to see which server is not busy and remove a load and transfer it to another server etc
-Modern load balancers and servers are all software based and not physical devices.

Review:

Two things to be comfy with:

1. DNS Solutions
2. Server-side solutions

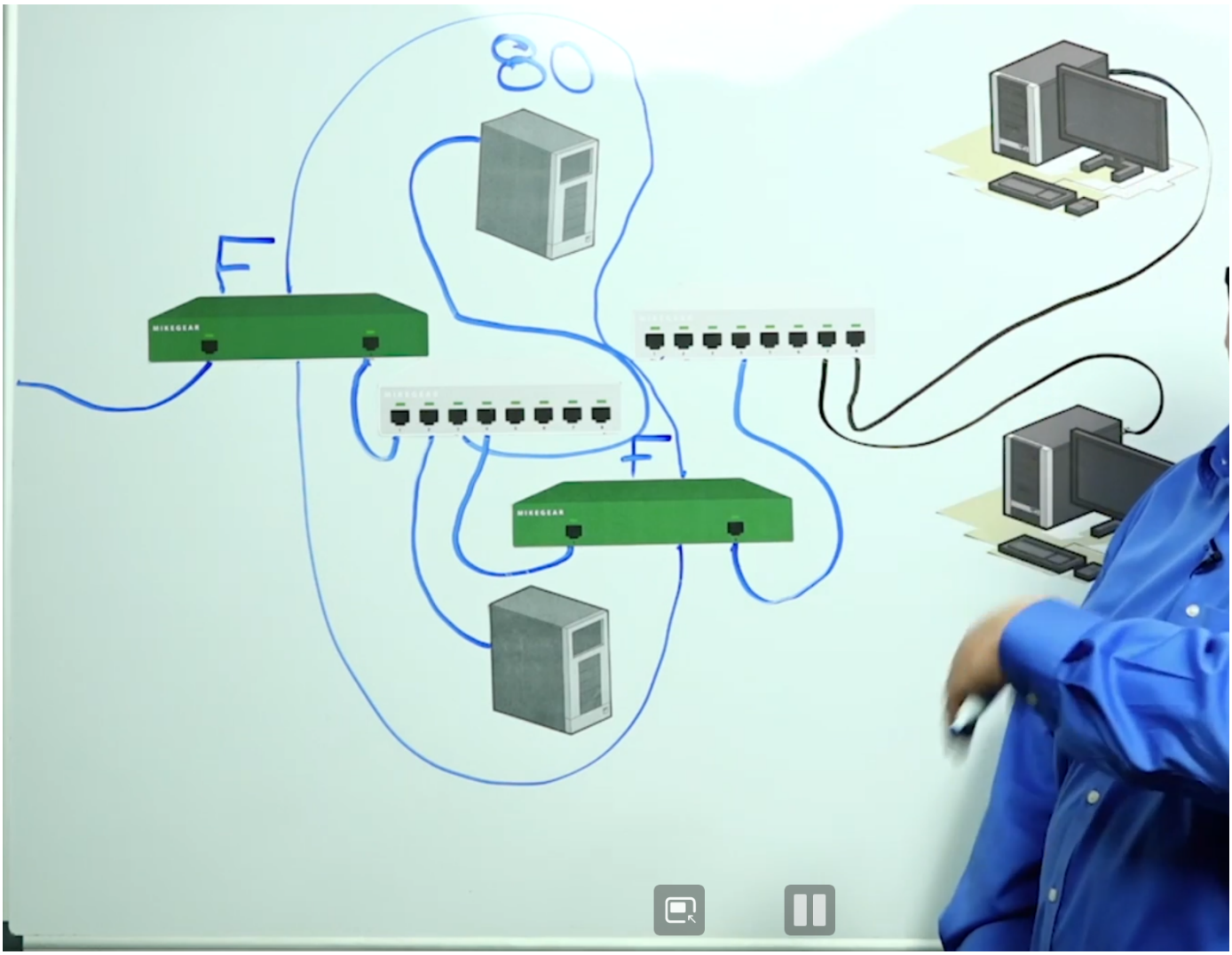
*Load balancing can be configured as client-side or server-side and provides high availability
*Load balancing can route to the most available server, either by a configured list (round robin) or by least response time
*Server-side load balancing uses a sophisticated hardware device that is located within the server.

---

101. Device Placement Scenarios

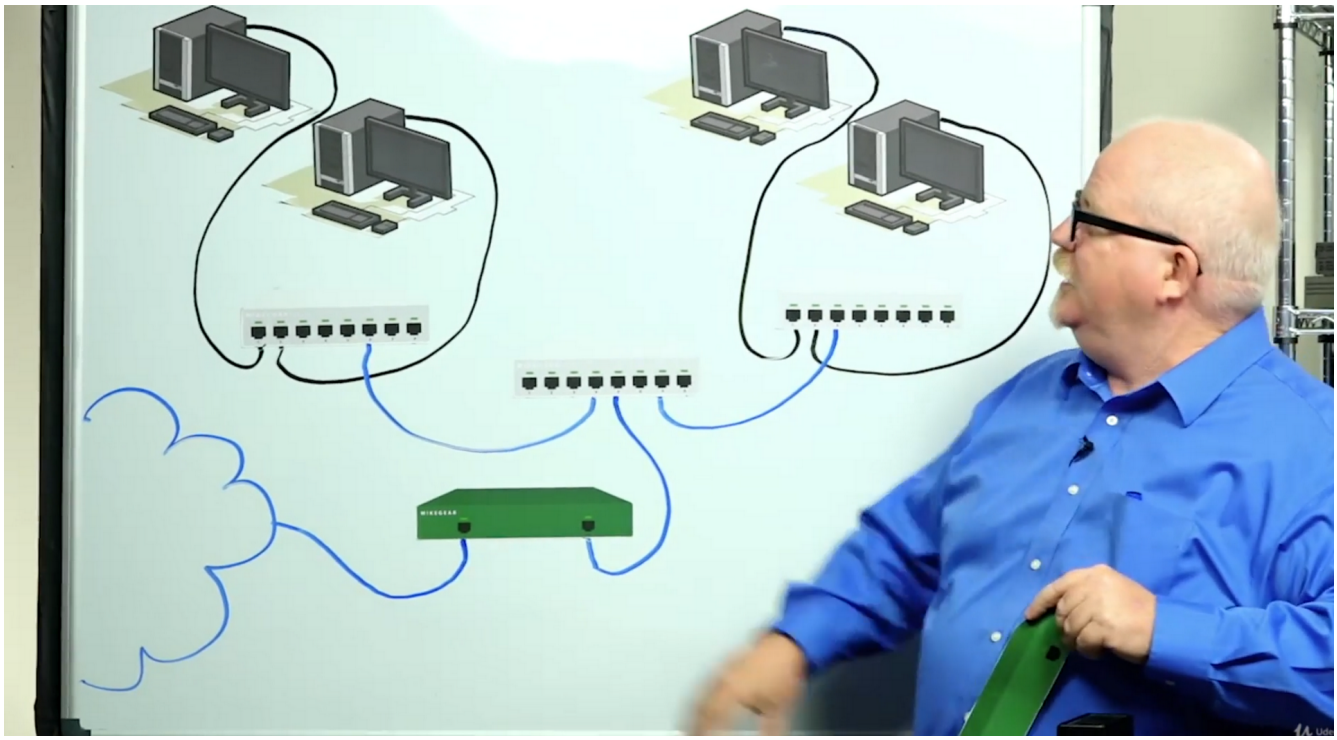
Four scenarios that you may see on the exam:

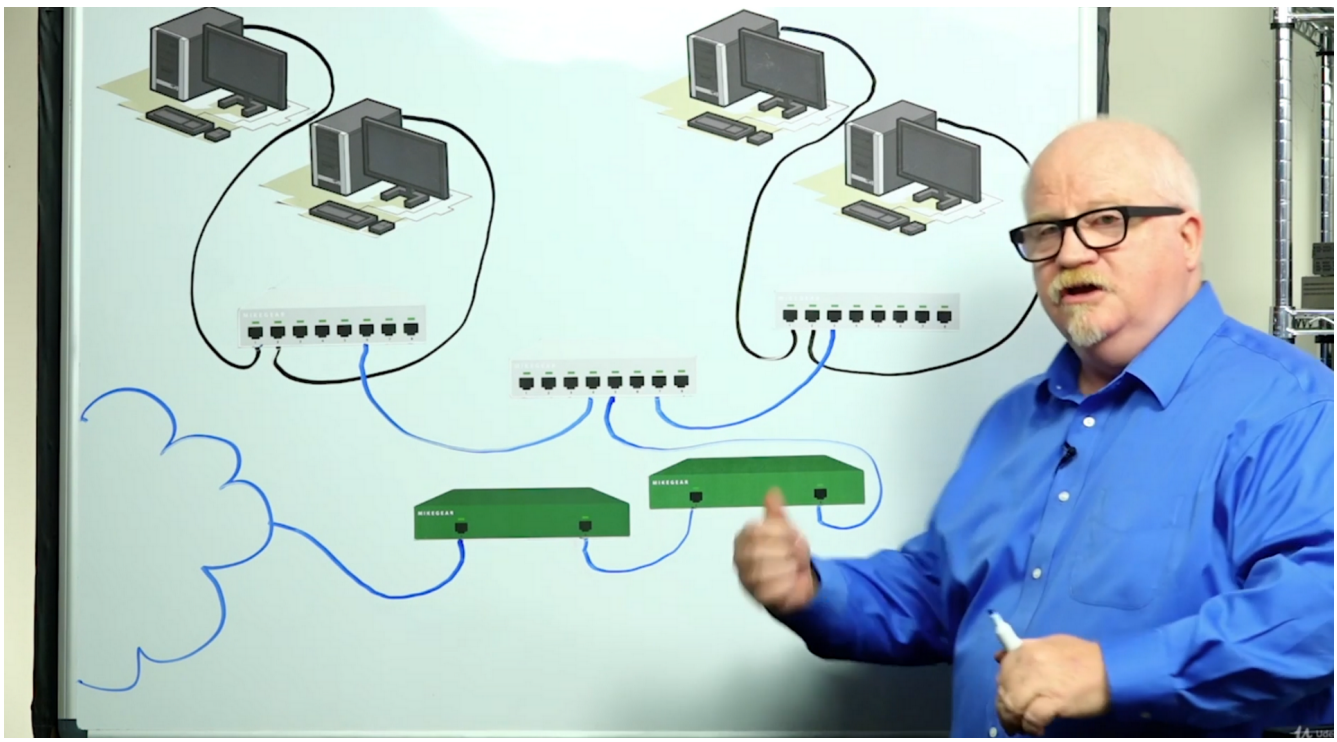
1. Demilitarized Zone (DMZ):
   "Edge Firewall" router for web servers and then the other "interior firewall" to protect our local network.



2. IDS vs. IPS:

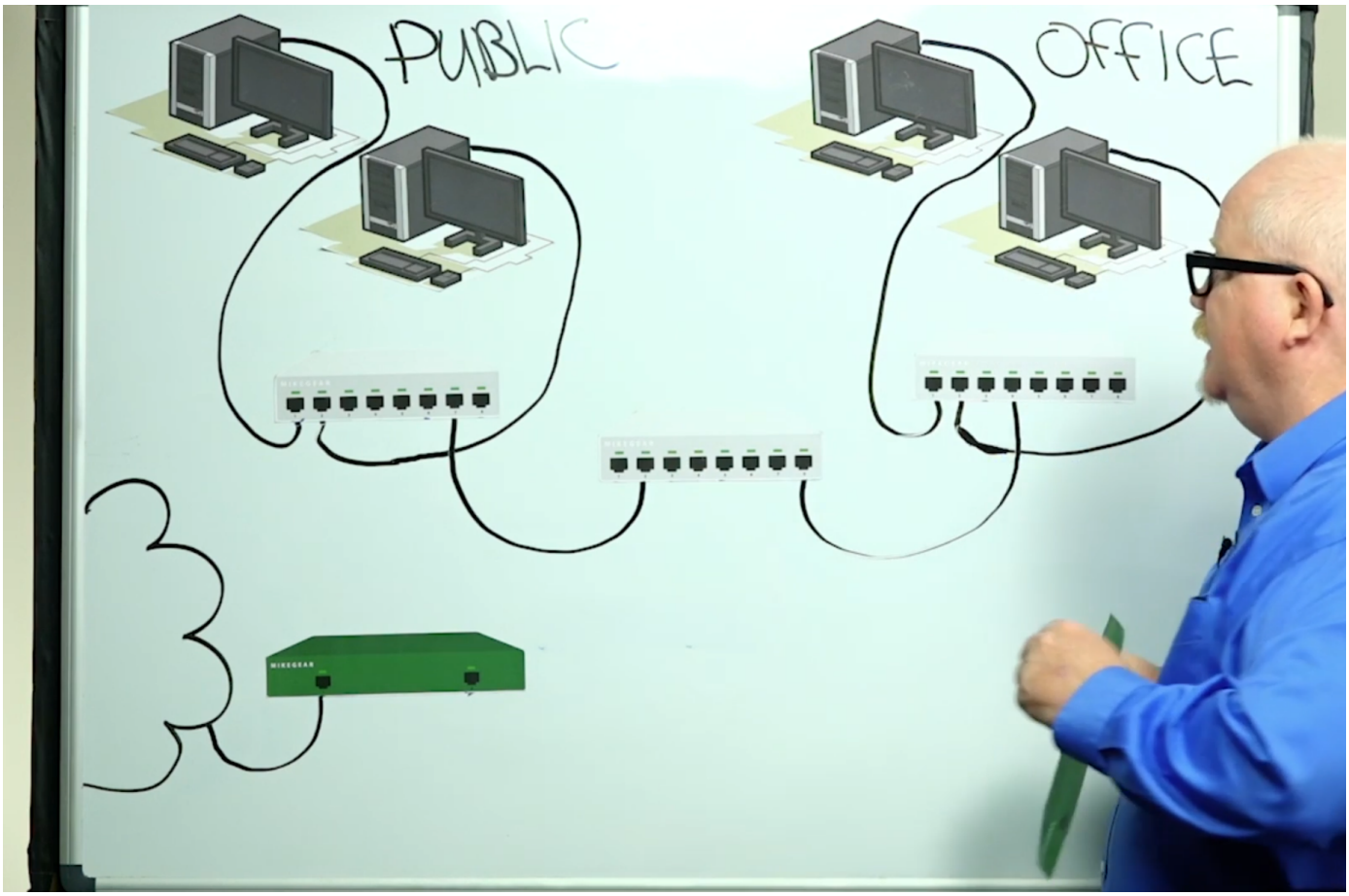
   question example: "In order to monitor all incoming and outgoing VLAN traffic where to place the IPS" - In-band (any trunked port)

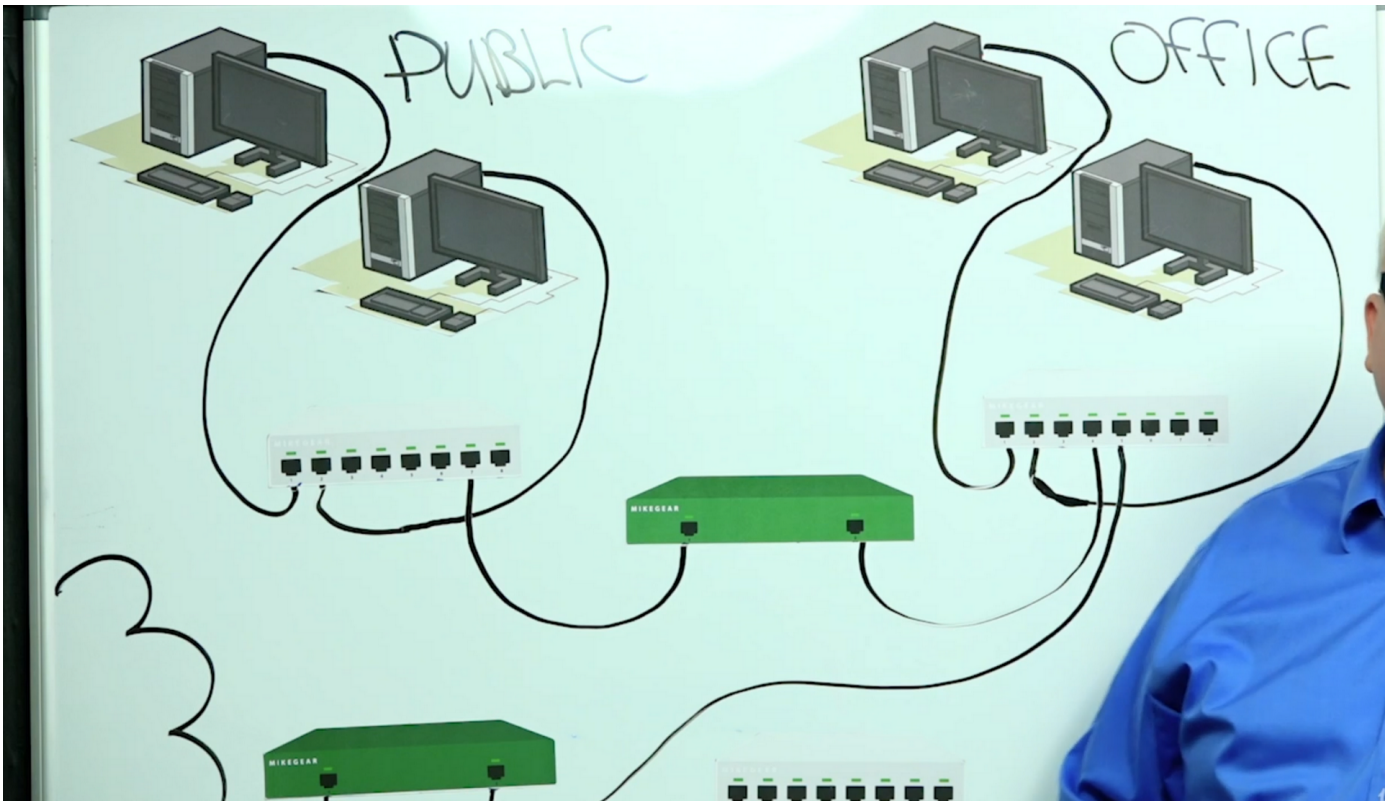




3. Firewall Placement:

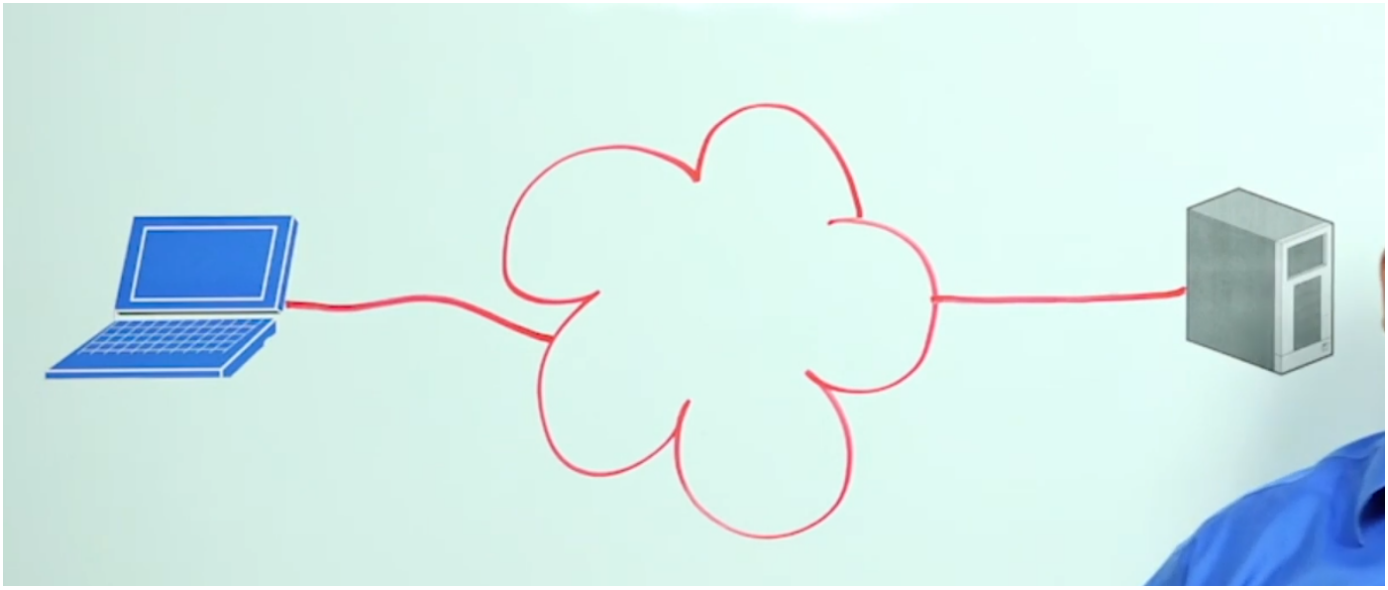
Internal Firewall:



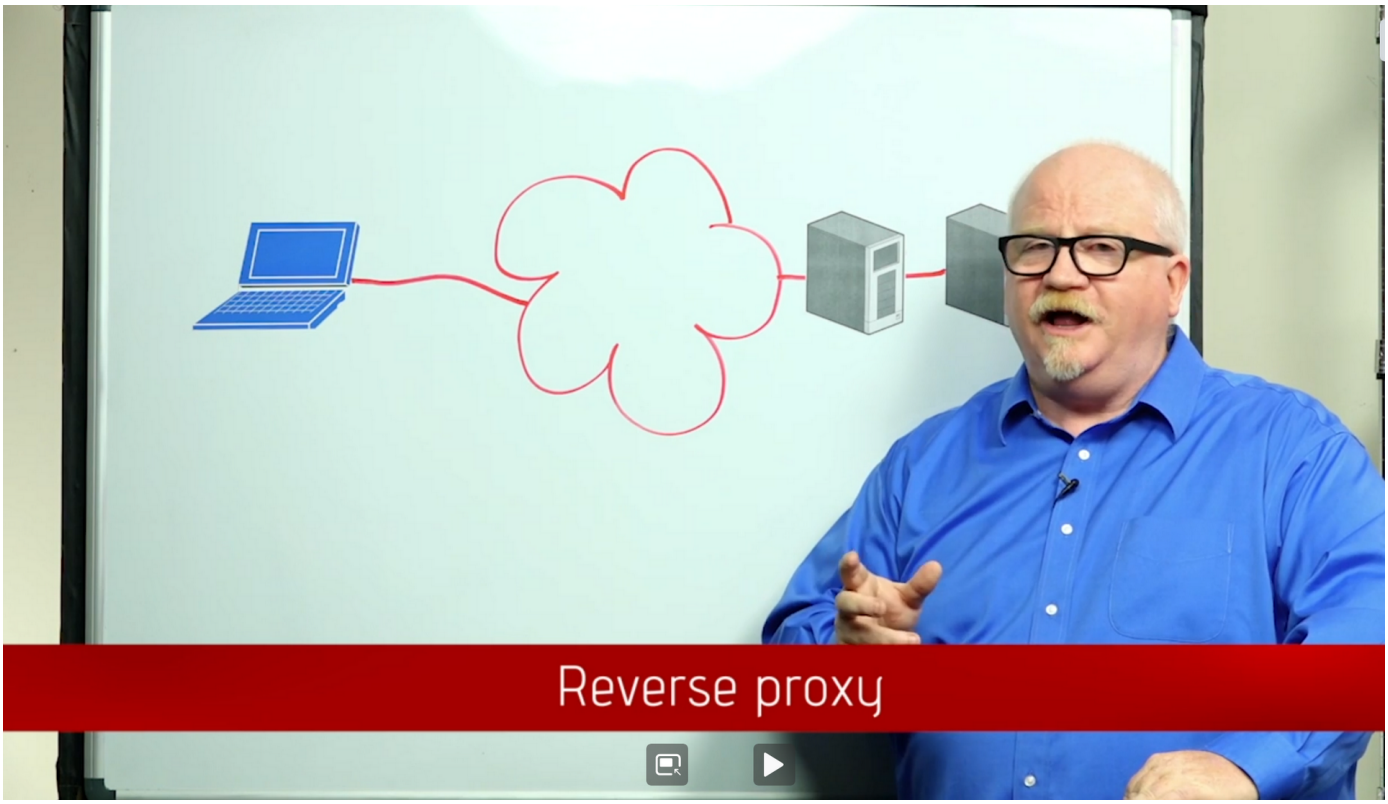


4. Proxy Servers:

Example Question: Where do place a proxy server such that the server is obscured from the client?



Reverse Proxy



Exam has lot of scenario questions.

Review:

*DMZs are used to protect public-facing servers by creating an isolated area for those devices

*Two Firewalls are used in a DMZ: one allowing usolicited traffic to the public server(s), and the second maintaining isolation of the private network.

*Internal firewalls can be used to block specific acces for areas that may need additional restrictions but, still function with the main domain.

QUIZ

1. Which would be the best solution to make an encrypted tunnel using SSH?
   a. Recode an unencrypted tunneling program to support SSH encryption**
   **b. Piggyback an exisiting tunnel program onto SSH
   c. Set up a tunnel using PPTP
   d. Set up a tunnel using L2TP/ipsec
2. Which statement is true of VLANs?
   a. VLANs enable remote stations to connect to the LAN from across the internet
   b. VLANs break up broadcast domains into multiple, smaller broadcast domains
   c. VLANs use SSH tunnes for cross-VLAN traffic
   d. VLANs can only be implemented on specified ports on a router
3. Which statement is true of inter-VLAN routing?
   a. InterVLAN routing calls for connecting each VLAN to a port on a router so that data can pass between the VLANs
   b. Inter-VLAN routing is implemented within switches to enable communication between VLANs
   c. Inter-VLAN routing encrypts and decryptes traffic between VLANs
   d. Inter-VLAN routing enables remote VLANs to connect over a public network, such as the internet.
4. Which port on a switch is used to manage the switch?
   a. Rollover port
   b. Console Port
   c. Yost port
   d. Layer-three port
5. When operating multiple, duplicate servers such as web servers, which method is best to take advantage of the full power of all the servers?
   a. HSRP
   b. DNS Server
   c. Round Robin Server
   d. Server Side Load Balancer
6. What is the Cisco protocol to perform port bonding?
   A. LACP
   b. HSRP
   c. CARP
   d. Inter-VLAN Routing
7. What does port mirroring accomplish?
   a.Enables inbound and outbound traffic from switch ports to be duplicated at the mirrored port.
   b. Double switch-port bandwidth by bonding a specified port to the mirrored port
   c. Redirects an inbound traffic to the mirrored port to another, specified port
   d. Redirects an outbound traffic from the mirrored port to a host with a specific IP address.

8. What does QoS provide?
   a. Higher performance of selected traffic
   b. Blocking of specified traffic types
   c. Redirection of low priority traffic to slower router interfaces
   d. Prioritized throughput of different traffic types
9. Which statement is true of IPS and IDS systems?
   a. passive IDS is the same as IPS
   b. IPS responds to threats with a notification to a specified staff
   c. IPS detects then attempts to defend against a threat
   d. Passive IPS is the same as IDS
10. Which statement is not true of a forward proxy?
   a. Forward proxy servers are connected in-line between the front-end router and the LAN and they do not require hosts to be configured
   b. Forward proxy servers funtion between the local network and the front-end router
   c. Forward proxy servers are application specific
   d. Hosts must be configured to access the forward proxy server
11. Which is the BEST device to dole out requests to duplicate servers to ease congestion?
   a. DNS server
   b. Round Robin Server
   c. Server Side Load Balancer
   d. Cluterer