Section 6: The Basic Lan

66.LAN Review

REVIEW:

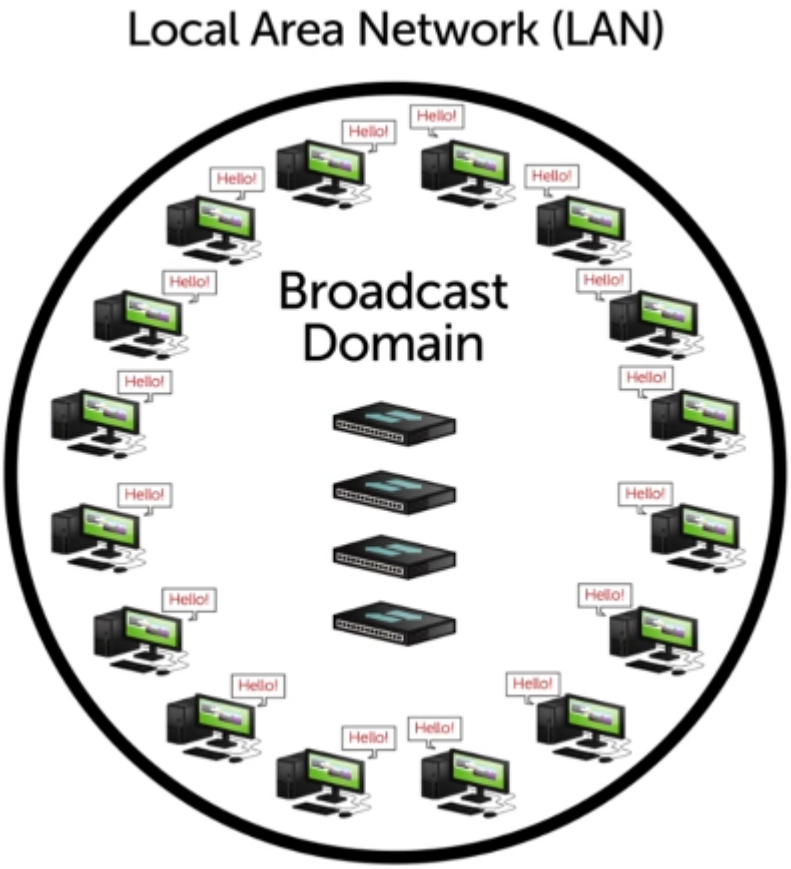
1. Switches:
    1. Filter and forward data based on MAC address
    2. Will See on the Exam:
        1. VLAN - Split one broadcast domain into multiple.(LAYER 2 SEPARATION OF NETWORKS)
            1. Assign differnt ports to different VLANs
            2. The moment you put a port on a different VLAN its like it doesn't exist (the port), The only way you can is by assigning more ports to that VLAN
        2. Flood Guarding
            1. STP (Spanning Tree Protocol) - Make sure that you enable this
            2. Prevents loop floods
2. Routers:
    1. Filter and forward data based on IP (LAYER 3) - Often routers can be referred to as a "layer 3 switch"
    2. Act as the doorway/interface between different Network ID's
    3. 'Gateway' Router acts as the interface between your LAN and the Internet
        1. Always is running NAT (Network Address Translation)
        2. A Firewall is run here often

67.Network Topologies

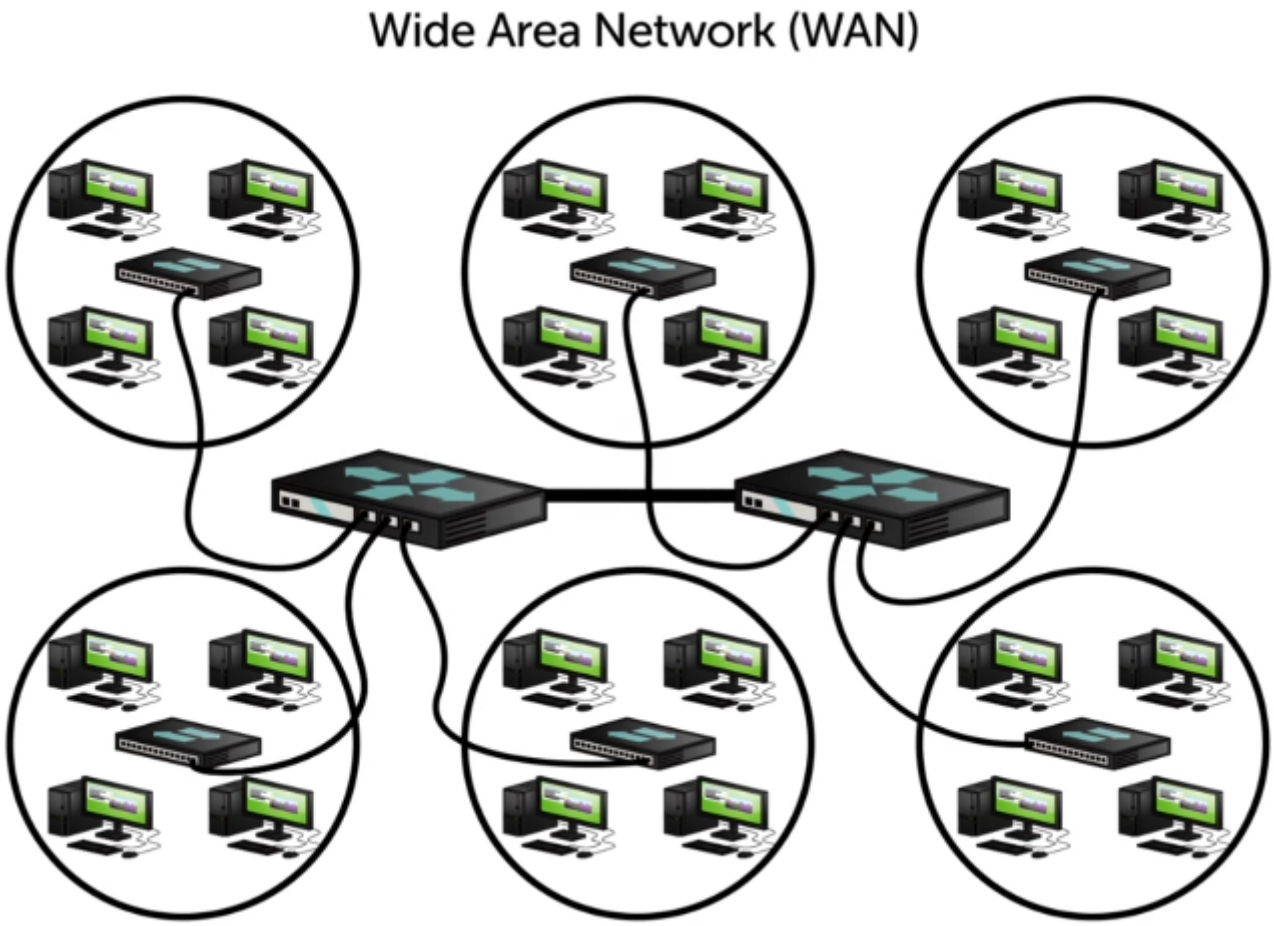
"The actual organization of a network in term of how data moves around"

REVIEW:

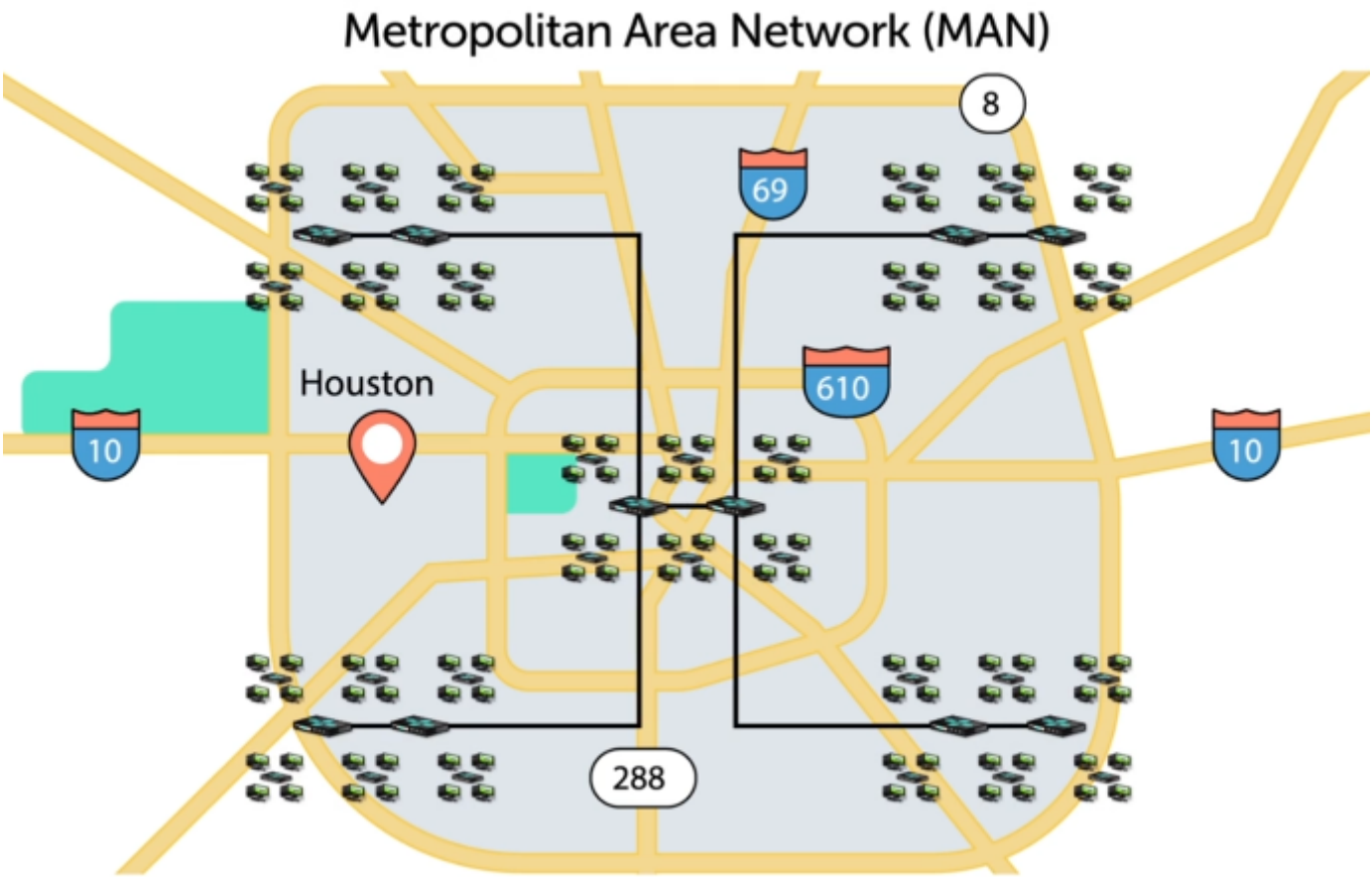
LAN:


Local Area Network (LAN)
Broadcast Domain
Hello!

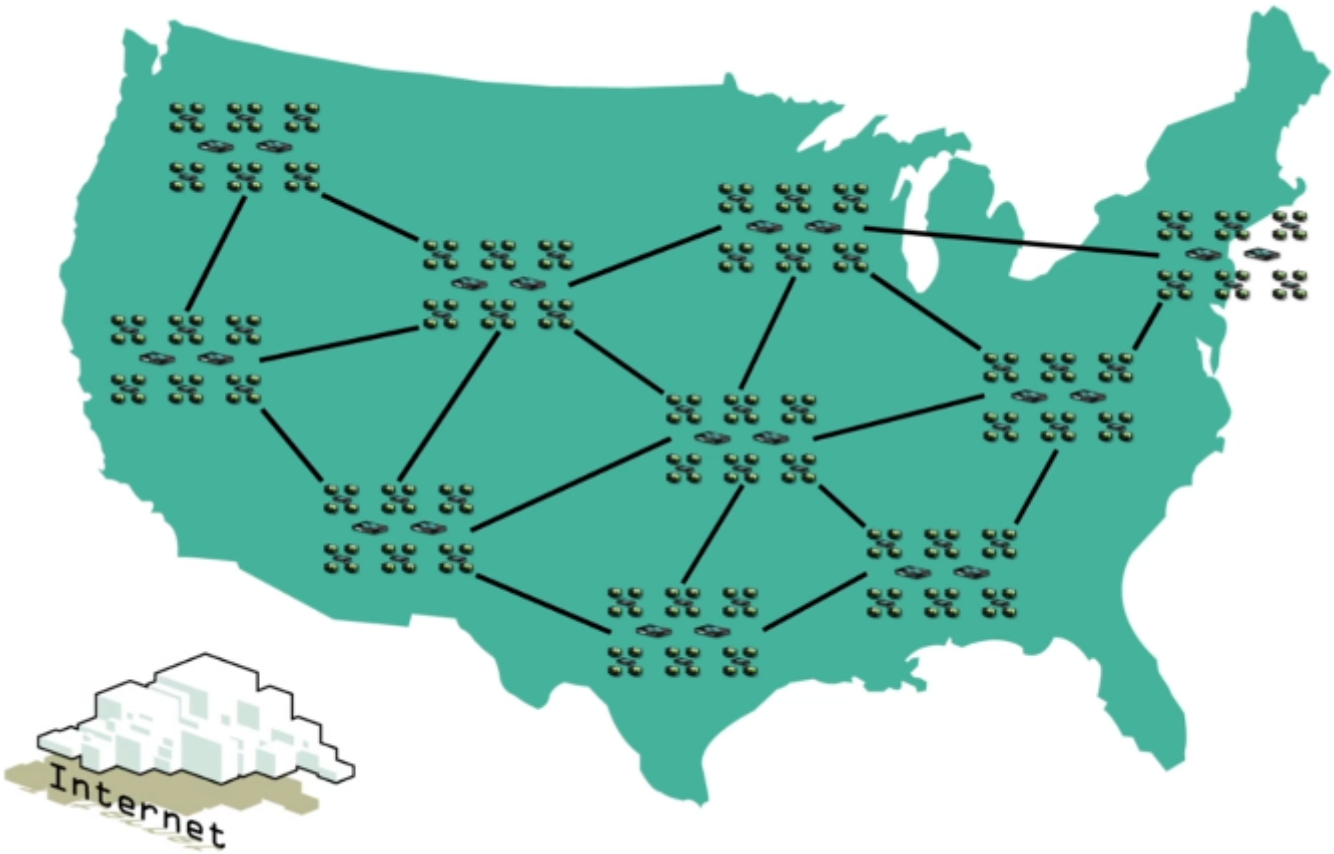
WAN:


Wide Area Network (WAN)

MAN(Spans a city):

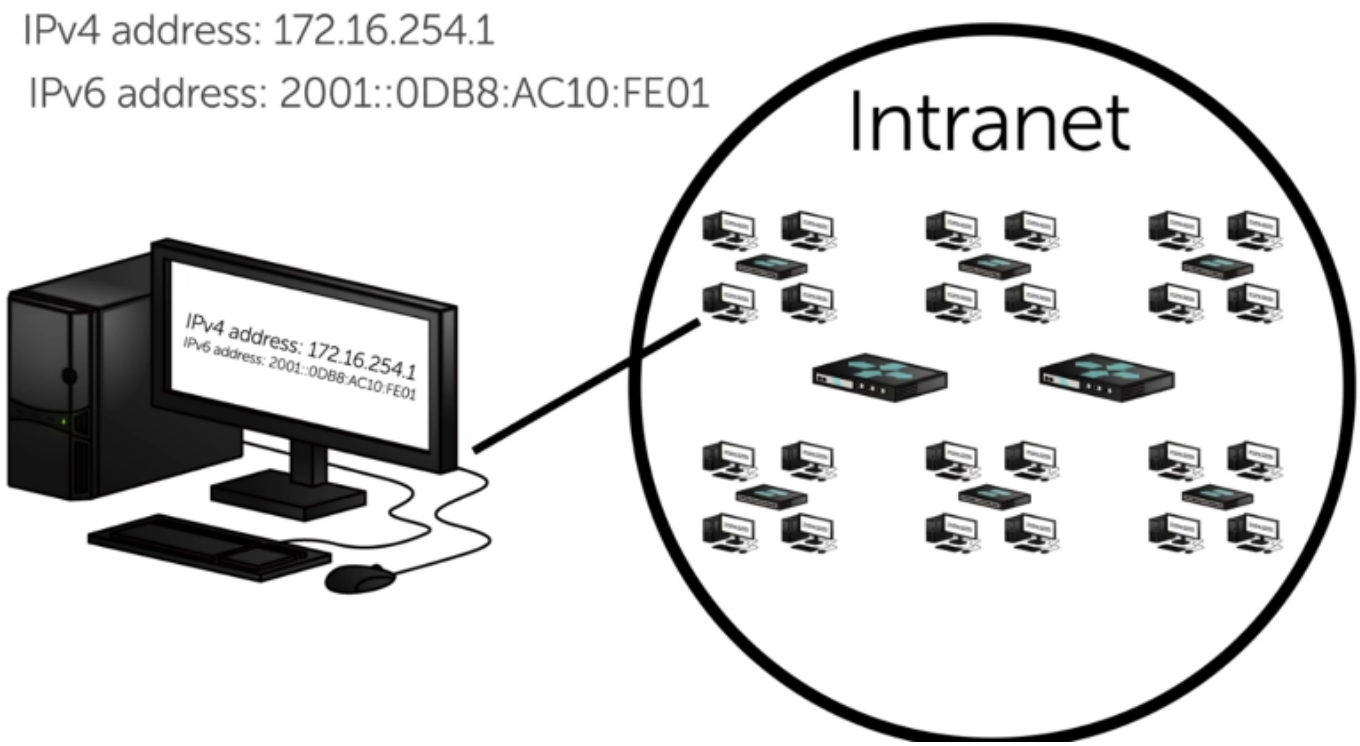


The Internet:

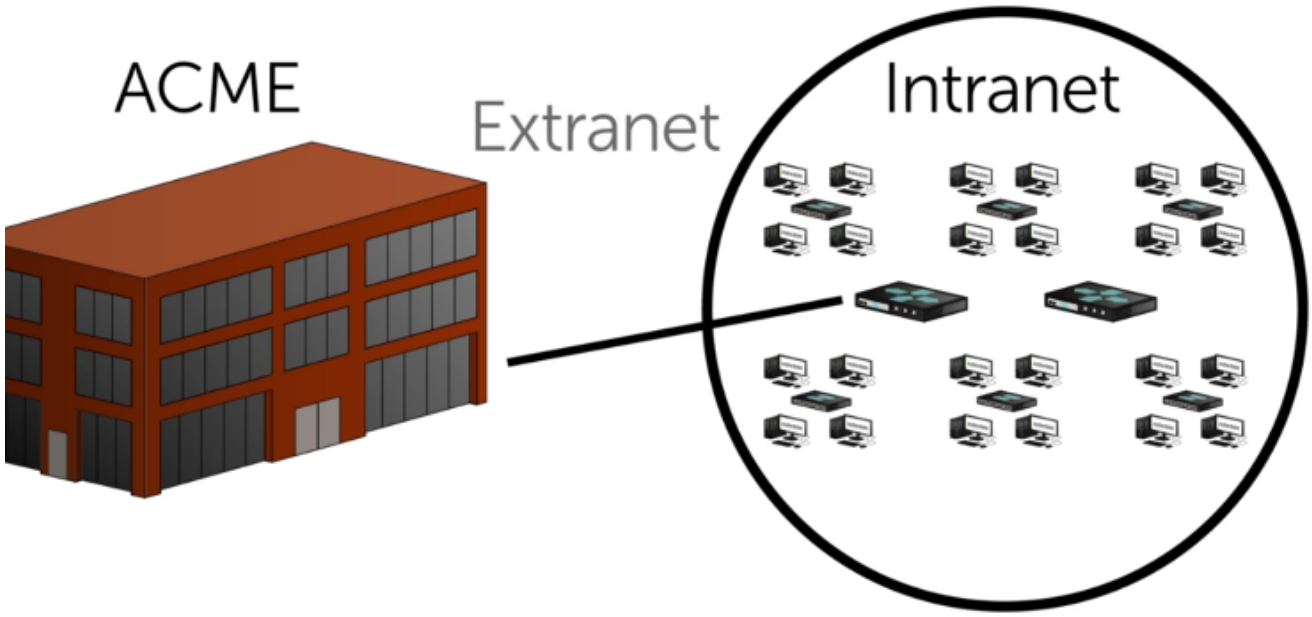


TCP/IP is the protocol which runs the internet.

IntraNet - A Private network that still runs on TCP/IP:



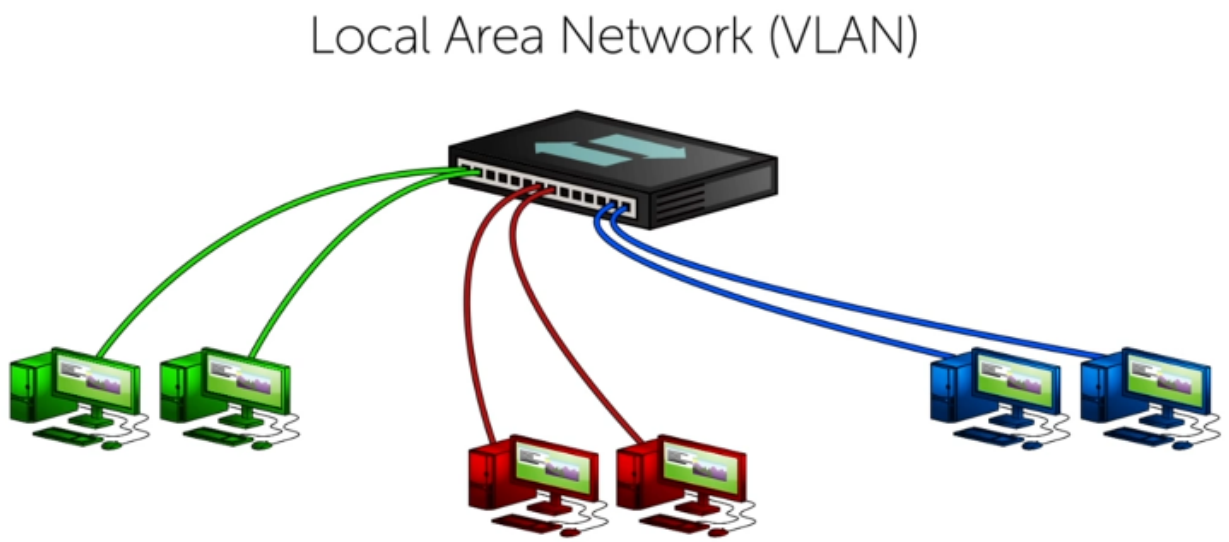
ExtraNet - Giving an outside source access to your intraNet:



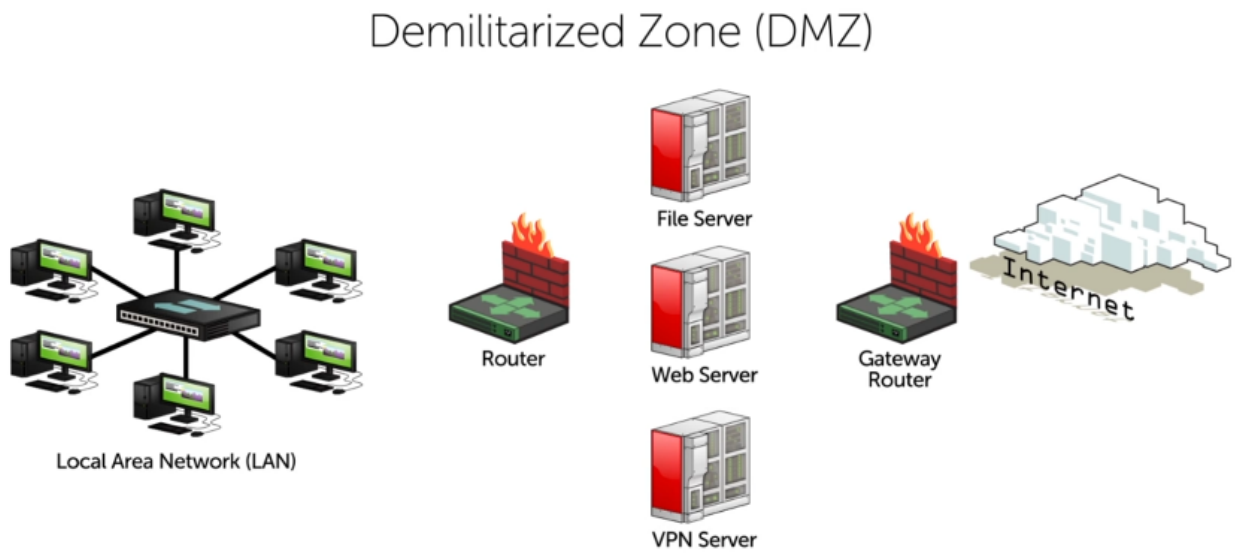
Network Zone Review

REVIEW:

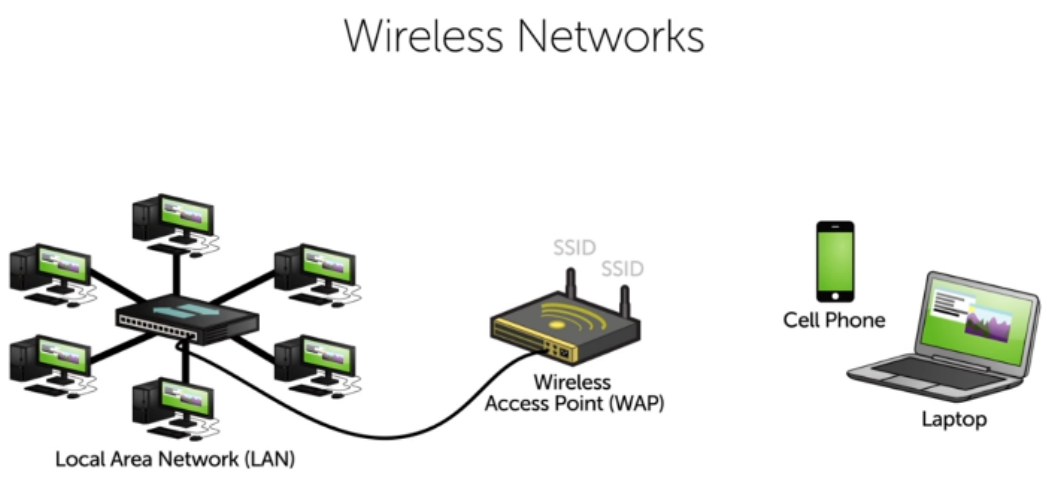
1. VLAN: Takes One or More Physical Switches and chop it up into separate Broadcast Domains



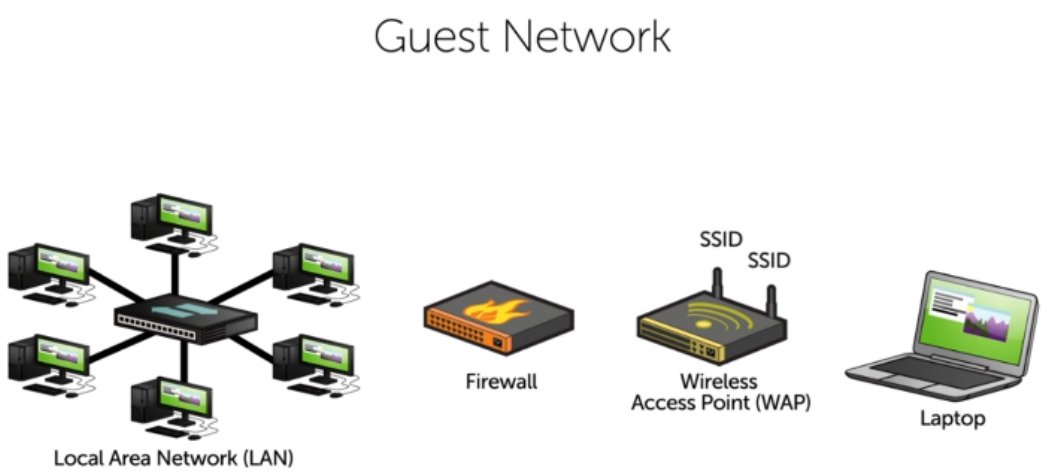
2. DMZ (Demilitarized Zone) - perfect tool for supporting web facing servers



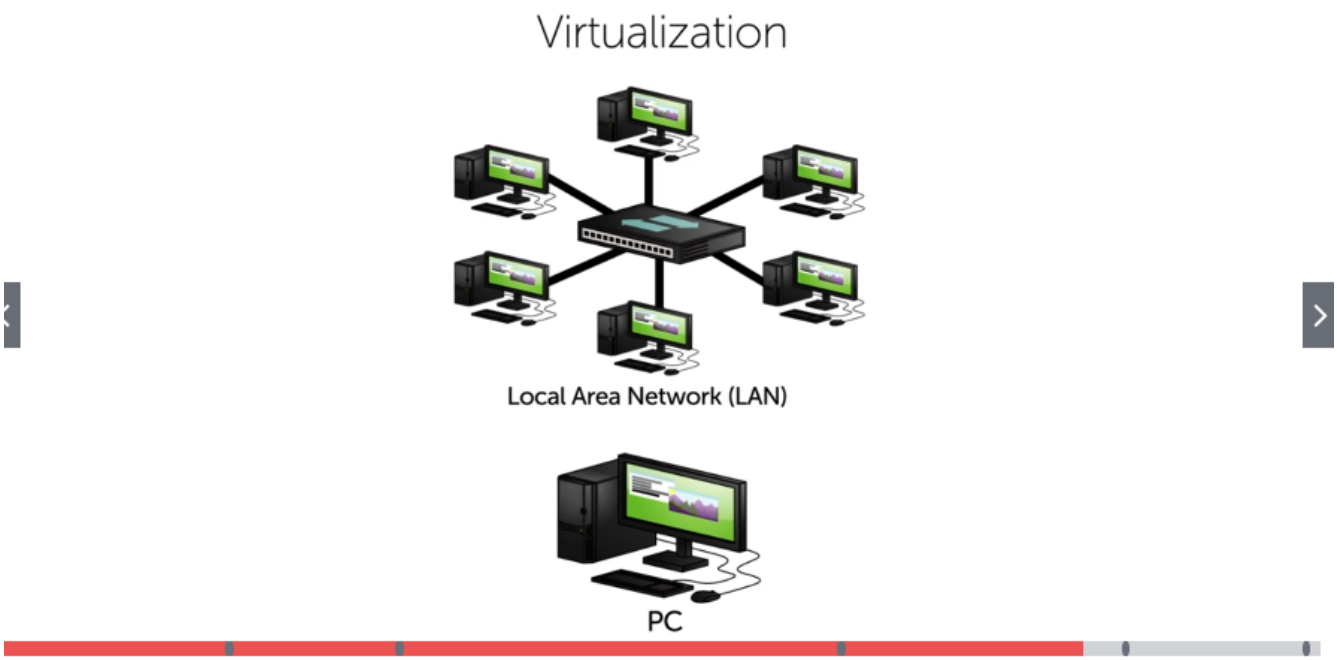
3. Wireless Networks



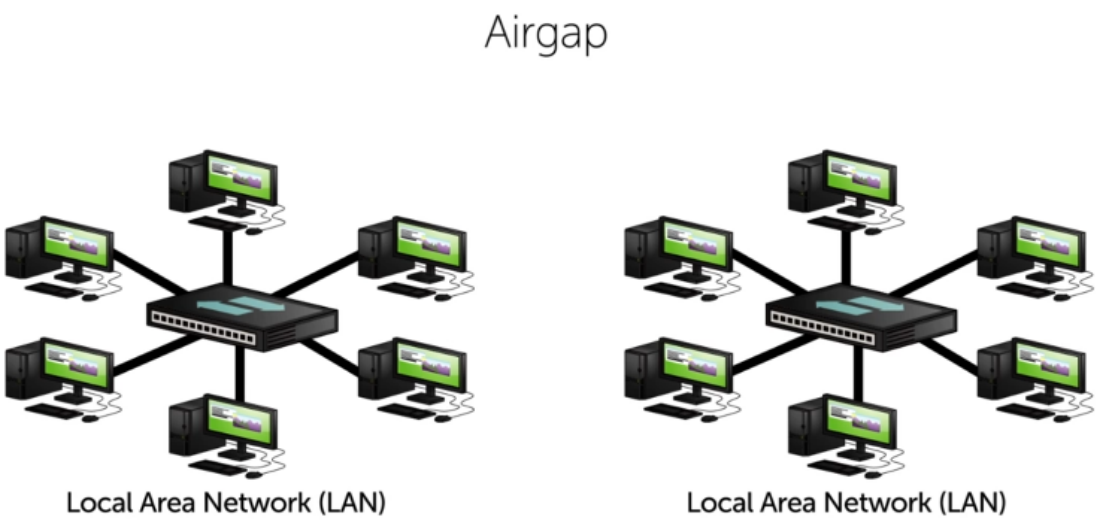
4. Guest Network



5. Virtualization Zones - Take one computer and make it look like a bunch of computers



6. Airgap - A disconnect (We unplug) two LANs from each other to provide real isolation



For the Exam: Be comfortable conceptually with the idea of "Zones"

69.Network Access Controls

NAC
1. Wireless Network
2. Remote Access
3. VPN Access

1. PPP (Point to point protocol) - Originally designed to work with dialup modems - Not used often today.
    1. Transport layer protocol

        1. initias connection
        2. Get address information
        3. Had very rudamentary authentication methods
            1. PAP (Passwords in the Clear)
            2. CHAP (Challenge handshake Authentication protolcol)\
2. EAP (Extensible Authentication Protocol) - Developed initally as an extention of PPP to handle all the authentication
    1. Types:
        1. EAP-MD5
            1. Basically MSCHAP (Microsoft CHAP)
            2. Takes those passwords and hashes them into a MD5 hash and exchanged them
        2. EAP-PSK
            1. Uses pre-determined symmetric keys
            2. Similar to WPA and WPA-2
        3. EAP-TLS
            1. Can Handle an entire TLS
            2. Needs server and client certificates
        4. EAP-TTLS
            1. Uses the TLS exchange method
            2. Only requires server certificate
3. Different Protocols that encapsulate EAP
    1. 802.1x - Authentication standard that allows us to make connections between the Supplicant and the Network (EAP over 802.11)
    2. LEAP - Ciscos High Security Wireless Standard (NO GOOD ANYMORE). Replaced by EAP-FAST
    3. PEAP - Microsofts version of EAP before EAP came along (NO GOOD ANYMORE)

When it comes to Network Access Control we will be using EAP

Quick Review:

- EAP was created as a better authentication method to PPP
- Recognize all of the EAP methods (EAP-MD5, EAP-PSK, etc)

** 70.The Network Firewall**

1. Stateful vs Stateless:
    1. Statefull: Doesn't have an ACL, but looks at whats going on and makes its own decision about what is going on (e.g. blocks a bunch of pings that are coming in.)
    2. Stateless: Filters and blocks stuff regardless of situation (Static, you set up the rules) - Stored in an ACL (Access Control List)

**Implicit Deny - Nobody can do anything unless you manually let them through

Application-based Firewall - Designed to protect applications (Set up a firewall in front of a webserver)

Quick Review:

- A stateful firewall blocking is based on behavior more than rules
- A stateless firewall blocking is based on an access control list, and defined rules
- Stateless firewalls configuration can block and unblock by defined IP address(s), port access, URL addresses

---

71.Proxy Servers

- Might need to add proxy servers to something on the exam

Proxy:
- A box/piece of software running ona computer which acts as an intermediary between two different devices having a session
- Application specific
- Web Proxy
- FTP Proxy
- VoIP Proxy
*Transparent Proxy

Two Types:

```
1. Forward Proxy Servers
        1. A traditional Forward Proxy is a dedicated box which is actually
in a business or school
        2. Caching
        3. content Filtering
        4. ![Screen Shot 2020-08-02 at 6.53.12 PM.png]
(_resources/da6ebbd42d434c33a7a798bb26764f2f.png)

        ***
        1. Usually used to do bad things
        1. ![Screen Shot 2020-08-02 at 6.57.56 PM.png]
(_resources/329bbc11bb1b4724b63f5a82a9ef3913.png)
        2. Create a VPN to the proxy
        ![Screen Shot 2020-08-02 at 6.59.18 PM.png]
(_resources/bcbd0a939ff9476bb4c9db77d09d5872.png)
        **Tools that do this: e.g. Hide.me

        *TOR (The Onion Router)
        1. ![Screen Shot 2020-08-02 at 7.02.50 PM.png]
(_resources/be5b32d0260144eb9db40089d716cf10.png)
```

```
2. Reverse Proxy Servers (Modern)
        1. Job is to protect the server
        2. High Security
        3. Handles DOS attacks
        4. used for load balancing
        5. Caching
        6. Encryption Acceleration
```

Quick Review:

- Forward vs. Reverse
- Forward hides the clients
- Reverse hides the servers

---

72. Honey Pots

- Devices that are designed to emulate a host or a network to let bad guys in and track what they are doing.

Free Honey Pot: "Honey Bot"

*Honey pots are more often then not placed in the DMZ
*Honey pots log everything, keystrokes, etc.
*Attackers often go for networks so we make a...

...HONEY NET - HONEY Net Virtual Machines

---

73. Virtual Private Networks

Remote Desktop: Emulates another desktop in that network

VPN directly connects into the network from a remote location, fully functional

Connection Options for VPN
- Lease your own line (Expensive)
- Via public network, virtualized

For the Exam they are looking for conceptual answers:

```
- Endpoints
        e.g.  (LAN (Home) ------ Computer in an airport(Needs the same IP as
the LAN))
                        ---> Create a VPN Tunnel (Connection between two VPN
endpoints)(could have a VPN Concentrator)

- Remote Access VPN - Single computer trying to phone home
- Site-to-Site VPN - A second LAN that wants to connect to a LAN
```

*A VPN is much slower than being in the LAN

- Split vs Full Tunneling

    1. Split - VPN endpoint on the laptop recognizes the traffic and sends things with the VPN endpoint IP through the tunnel and everything else outside of the tunnel.
    2. Tunneling - Sends everything through the VPN Tunnel (Avoid these)

*VPN Setup Steps
- Protocol to set up tunnel
- Protcol to handle authentication and encryption

Many Popular VPNs out there:

1. PPTP (Point to point tunneling protocol)
    1. Oldest VPN
    2. Uses PPP for tunnel
    3. Password
    4. TCP port 1723

2. L2TP (Layer 2 Tunneling Protocol)
    1. Cisco Proprietary
    2. Similar to PPTP
    3. L2TP tunnel
    4. IPsec encryption (Fast)
    5. UDP Port 500 and 4500

3. Pure IPsec
    1. Uses IPsec for the tunneling and the encryption
    2. UDP ports 500, and 4500
    3. Great for IPv6

4. SSL/TLS (Secure Socket Layer/Transport Layer Security)
    1. TCP Port 443
    2. Often works within a web browser
    3. TUN/TAP (Virtual network driver) tunnel
    4. TLS Encryption

5. OpenVPN
    1. Unique Tunnel
    2. Encryption based on SSL/TLS protocol
    3. TCP Port 1194, but can be easily changed

Remember 'Where you would use different VPNs and be comfortable with the protocols'

Quick Review:
- Two types of VPNs: remote access and site to site
- Know the VPN protocols described (PPTP, L2TP, etc)
- Know the VPN port Numbers

---

74. IPSec

```
* IPSec is a bunch of protocols that work together that come up with the
idea that you can have any 2 hosts come together and have a secure
connection.

- Used all over

Base Pieces of IPSec:

1. Transport Mode (Keeps the same IP)

        1. Authentication Headers (ONLY Provides integrity)
                1. Does an integrity check and then puts on an
Authentication header Generating an HMAC

        2. ESP (Encapsulating Security Payloads)
                1. Go through the process of encrypting and then puts on a
header

2. Tunnel Mode (Removes original IP header and adds a new IP address)
        1. Used with ESP. Keeps the ESP and adds a new IP header to the
outside of it.


Tunneling and ESP are most common today.

*ISAKMP - creates a security association (SA) between two hosts.

IPSEC Protocol Suite:
        1. Uses negotiation protocol ISAKMP
                1. Inital authentication
                        1. Certificates
                        2. preshared keys
                        3. Key Exchange
```

Where we see IPSec in todays world:

1. VPNs

    1. Pure IPSec VPN (Less common)
    2. IPSec with L2TP (More common today)
        1. L2TP creates a tunnel, and then IPSec puts a tunnel within the tunnel
2. RADIUS/TACACS+
    1. Fairly Uncommon
3. IPSec with IPv6
4. Using IPSec to Encrypt Unsecured Protocols

Quick Review:

- IPSec works at the IP layer
- IPsec has a tunnel and transport mode
- Authentication headers (AH) provide integrity

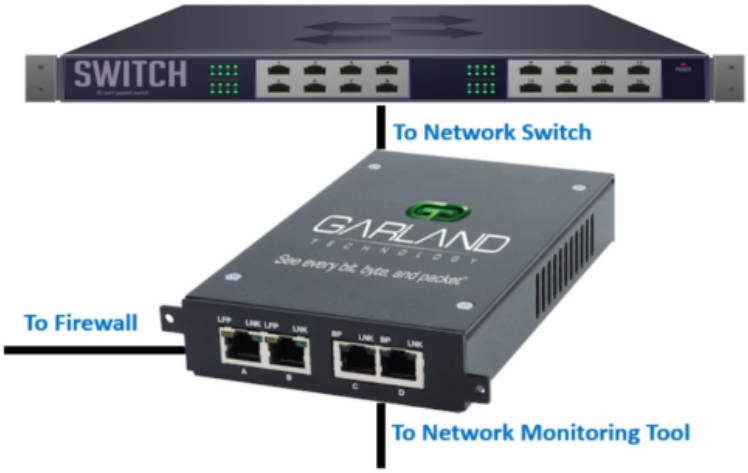
75.NIDS/NIPS

NIDS (Network Intrusion Detection Systems):
1. Passive

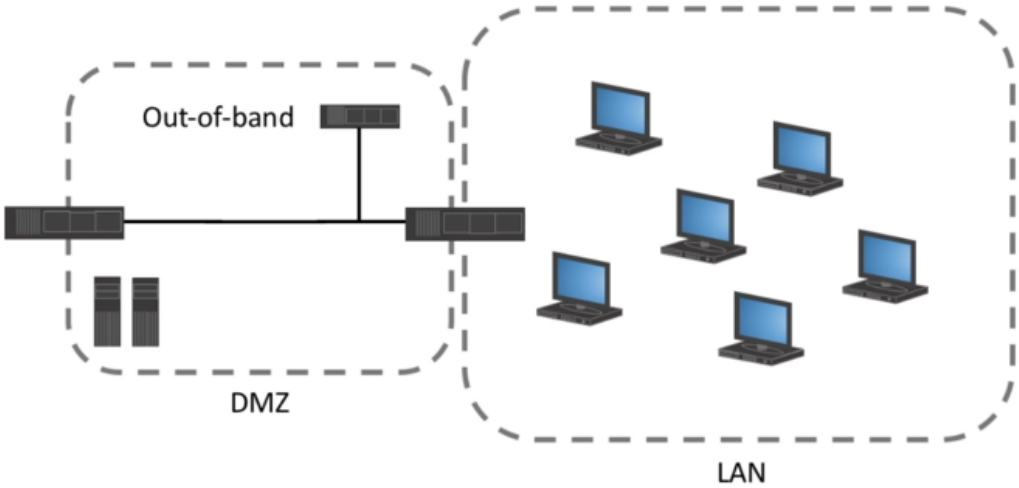
NIPS (Network Intrusion Prevention Systemss):
1. Active/Inline
1. Blocks from router
2. Detection Methods
1. Behavioral/anomaly
2. Signature-Based
3. Rule-Based
4. Heuristic
1. Combines anomaly with signature
2. Most systems today are Heuristic

To Configure NIDS/NIPS
1. Network Tap
2. Port Mirroring

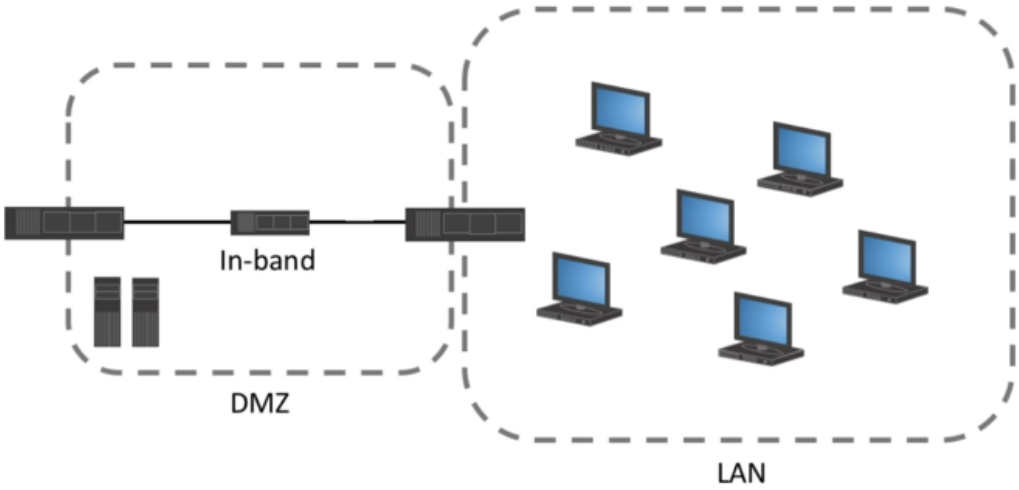
Network Tap



NIDS (OUT OF BAND)



NIPS (IN BAND)



- On larger Networks there are collectors for all the Intrusion information
- Correlation engines (Tool that does the Detection methods)

Quick Review:

- NIPS types of detection methods include; behavioral, signature-based, rule-based and heuristic
- Port Mirroring and Network Taps are tools used with NIDS and NIPS
- NIDS is most often set up as Out-Of-Band, NIPS is typically in-band

---

76.SIEM

SIEM (Security Information and Event Management) - Takes all the monitors and puts them into one package

Two things to consider when talking about SIEM:
1. Aggregation - Collecting data and storing it
1. Time Syschronization
2. Event de-duplication
3. Normalization
4. Logs -WORM (Write Once, Read Many)

```
![Screen Shot 2020-08-02 at 9.06.29 PM.png]
(_resources/eb460adaf7da420e8b1ad77d73648380.png)

![Screen Shot 2020-08-02 at 9.07.04 PM.png]
(_resources/2ef5f03a794d421fb6525e022a4759d9.png)

2. Correlation - Now that we have collected the data, lets analzye and
report it in a way that is readable.

        1. Alerts
```

```
                1. For Notification if something goes bad

        2. Triggering
                1. Exceeding Thresholds

Popular SIEM Softwares
        1. Splunk
        2. ArchSight
        3. Elk (Elastic Search, Log Stash, Cabana) - Open Source
```

QUIZ

Question 1:

What does a switch use to filter and forward data?

- IP address
- MAC address
- VLAN
- Depends on the setting

Question 2:

A WAN is the connection of which of the following?

- Two or more LANs
- Two or more interconnected PCs
- A single router connected to the Internet
- All the above

Question 3:

Which of the following will provide domain separation on a LAN behind a firewall for broadcast domains?

- (●) VLAN
- ( ) WAN
- ( ) VPN
- ( ) Proxy server

Question 4:

What was the authentication method used in Cisco environments that pre-dated EAP?

- (●) LEAP
- ( ) PEAP
- ( ) PPP
- ( ) EAP-FAST

Question 5:

A stateful firewall filters data based on?

- Rules
- Behavior
- ACLs
- Internal policies

Question 6:

Which proxy server provides protection to servers as opposed to clients?

- Forward proxy
- Transference proxy
- Reverse proxy
- Forward Web proxy

Question 7:

Where is a typical location of a honeypot or honeynet?

- With the proxy server
- In the DMZ
- Behind the firewall close to the core LAN
- On the Internet side of afirewall

Question 8:

Which of these could connect an entire LAN in one location to a LAN in another location?

- LAN-to-LAN VPN
- Office-to-office VPN
- Site-to-site VPN
- Location-to-home VPN

Question 9:

NIDS is most often configured as what type of device?

- (●) Out-of-band
- ( ) In-band
- ( ) Web server
- ( ) Print server

Question 10:

A SIEM tool provides which of the following?

- ( ) Aggregation of logs
- ( ) Alerts
- ( ) Correlation of data
- (●) All of the above