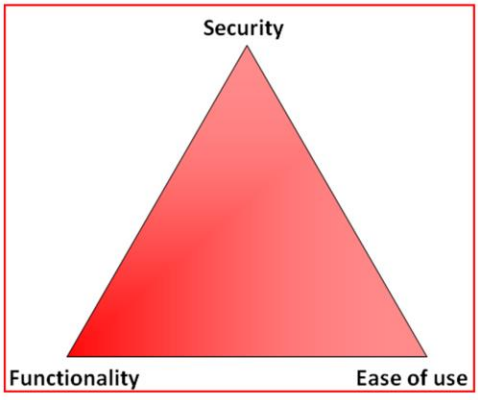
CompTIA Security+

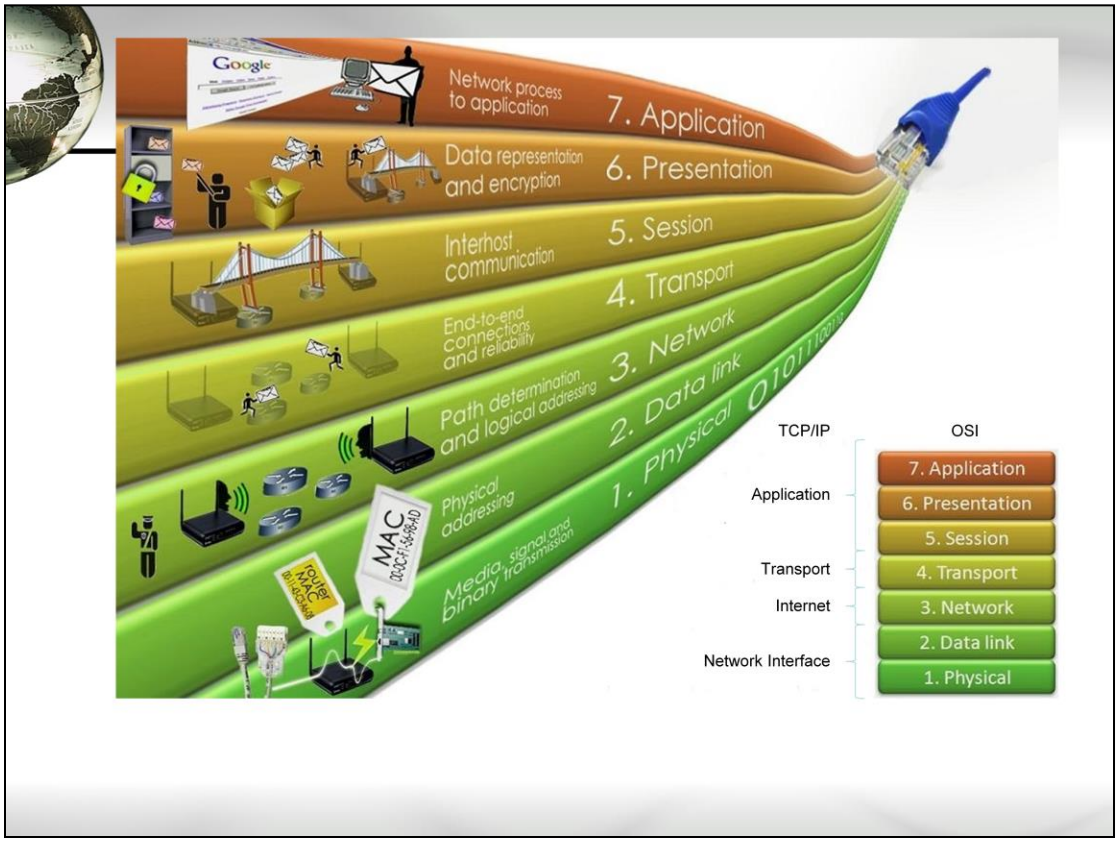
1.0 Network Security

Security

Functionality – Features
Usability – GUI
Security – Restrictions

Moving towards security means less functionality and usability.





-please

-do

-not

-throw

-sausage

-pizza

-away

Objective 1.1

- Implement security configuration parameters on network devices and other technologies

Firewall

- The first line of defense for the network
- Primary function of a firewall is to mitigate threats by monitoring all traffic entering or leaving a network
- Can be composed of hardware, software, or a combination of both
- Can be host-based or network-based

Firewall

- Packet-filtering Firewall
  - filters traffic based on source and destination
  - “Common Routers”
- Circuit-level Gateway Firewall
  - ensures that the packets involved in establishing and maintaining the circuit (a virtual circuit or session) are valid and used in the proper manner
- Application-level Gateway Firewall
  - Opens and inspects every packet on layer 7
  - “Proxy”
- Stateful-inspection Firewall
  - Keeps a state table to track every communication channel (TCP streams, UDP communication)

Firewall

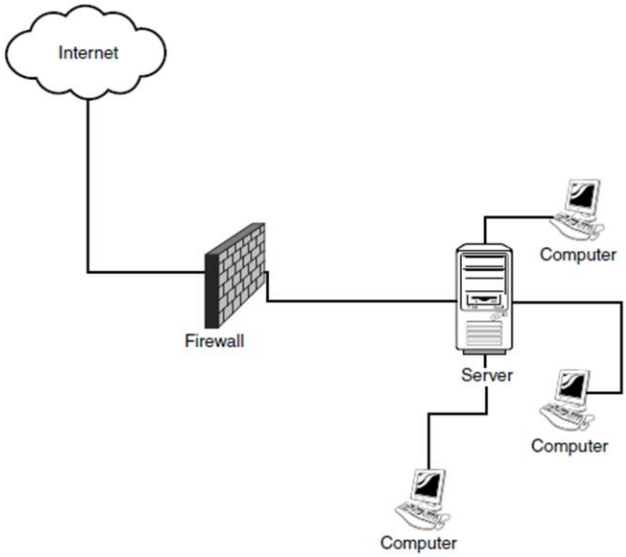


FIGURE 1.1 **A network with a firewall.**

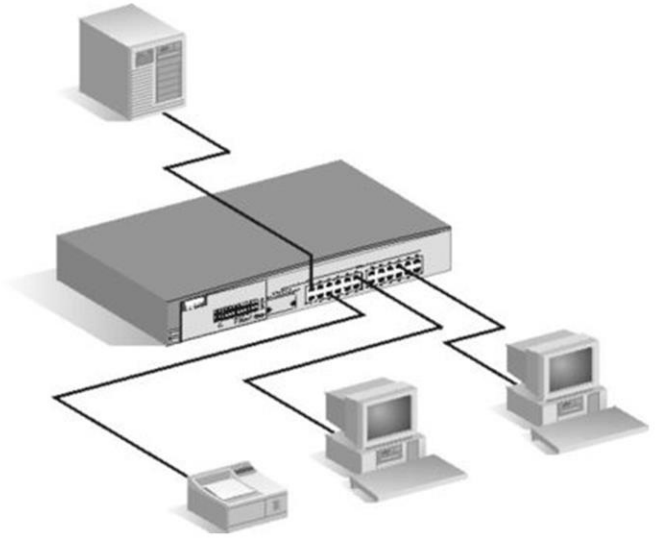
Router

- Route packets between networks
- Operate at the Network layer of the OSI model
- Routes packets based on IP addresses
- Connect diverse network types
  - LANS, WANs, copper, fiber
- Create separate broadcast domains
- Can filter network traffic (Packet-filtering firewall)

Switch

- The most common choice when it comes to interconnecting hosts within a LAN
- Operate at the Data Link layer of the OSI model
- Forwards or moves frames based on MAC addresses
- Increase the amount of bandwidth that goes to each device
- Each port creates a separate collision domains
- Prevent loops using Spanning Tree Protocol(STP)
- Can be used to create VLANs (separate broadcast domains)

Switch



Load Balancers

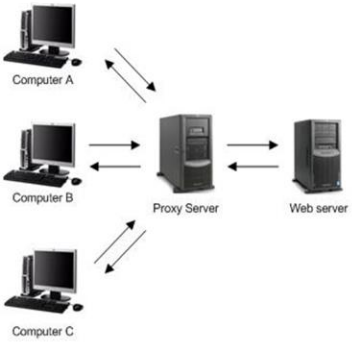
- A device that performs load balancing as its primary function
- Distributes the load over many physical servers
  - A server cluster
- Many options for load balancing
  - Distribution based on load
  - Distribution based on traffic
  - Distribution based on content

Load Balancers

Technique	Description
Random choice	Each packet or connection is assigned a destination randomly.
Round robin	Each packet or connection is assigned the next destination in order, such as 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, and so on.
Load monitoring	Each packet or connection is assigned a destination based on the current load or capacity of the targets. The device/path with the lowest current load receives the next packet or connection.
Preferencing	Each packet or connection is assigned a destination based on a subjective preference or known capacity difference. For example, suppose system 1 can handle twice the capacity of systems 2 and 3; in this case, preferencing would look like 1, 2, 1, 3, 1, 2, 1, 3, 1, and so on.

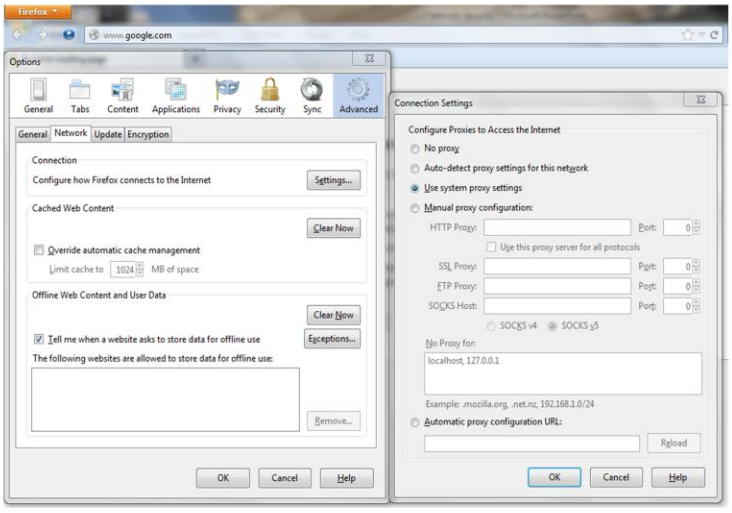
Proxy Server

- Sits between the users and the external network in the DMZ
- Receives the user request and sends the request on their behalf
- Useful for **caching content, load balancing, internet connectivity**, content filtering, and hiding private IP addresses
- Applications may need to know how to use the proxy



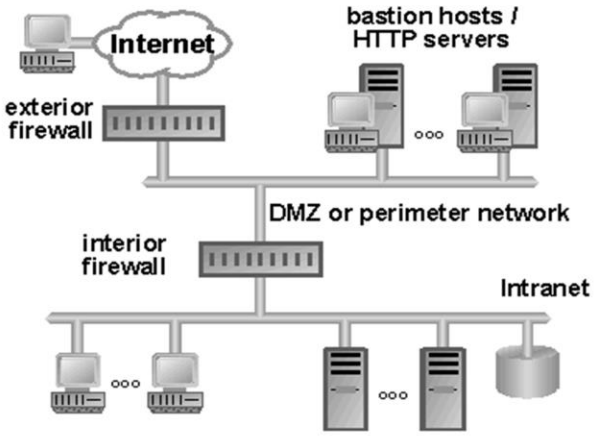
Every device with in the DMZ is called a **bastion host.**

Proxies


Firefox
www.google.com
Options
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
General
Network
Update
Encryption
Connection
Configure how Firefox connects to the Internet
Settings...
Cached Web Content
Clear Now
Override automatic cache management
Limit cache to 1024 MB of space
Offline Web Content and User Data
Clear Now
Tell me when a website asks to store data for offline use
Exceptions...
The following websites are allowed to store data for offline use:
Remove...
OK
Cancel
Help
Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy:
Port:
Use this proxy server for all protocols
SSL Proxy:
FTP Proxy:
SOCKS Host:
SOCKS v4
SOCKS v5
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
OK
Cancel
Help

Exam Alert

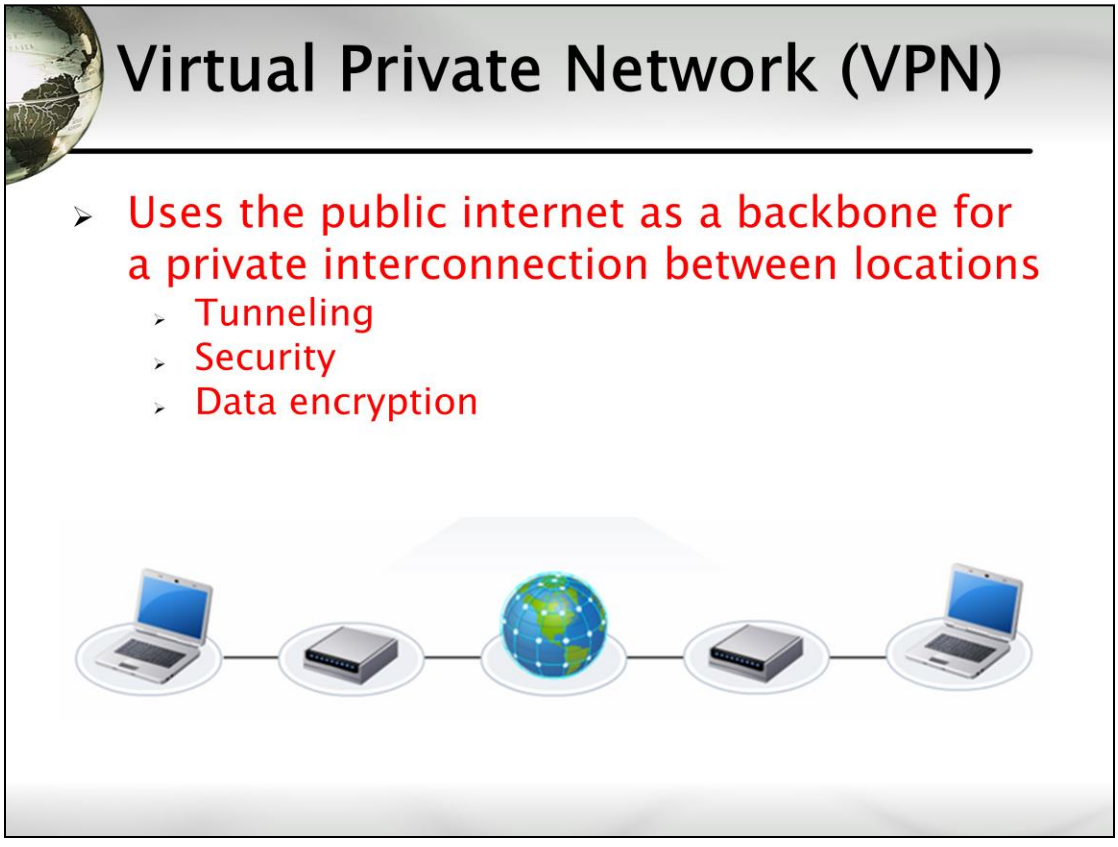
- A **bastion host** is an exposed server that provides public access to a critical service, such as a proxy, web, or email server



Web Security Gateway

(Fire Wall)

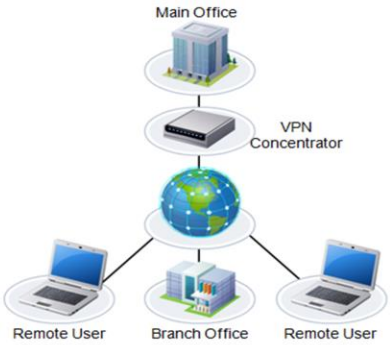
- Single point of policy control and management for web-based content access
- Used to intentionally block internal Internet access to a predefined list of websites or categories of websites, IM filtering, email filtering, spam
- Content filtering by URL
- Microsoft Forefront, Websense



Provides a secure tunnel through an unsecure internet

VPN Concentrators

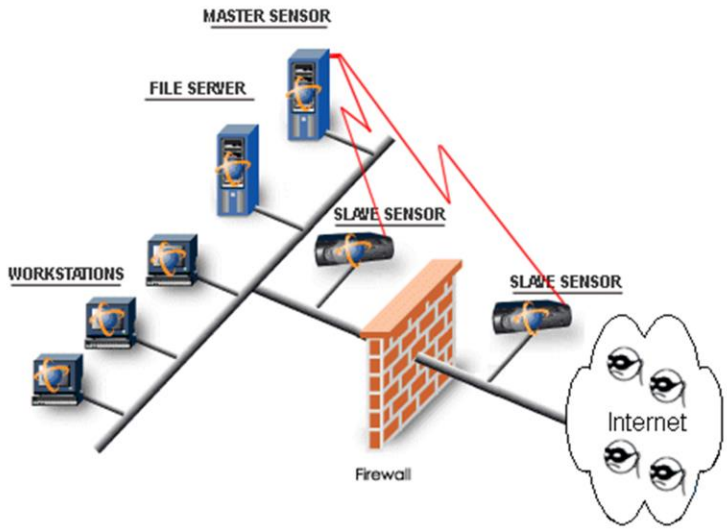
- Deployed where the requirement is for a single device to handle a very large number of VPN tunnels



Intrusion Detection System (IDS)

- Designed to analyze data, identify attacks, and respond to the intrusion (passive)
- Two basic types are:
  - **Network-based** and **Host-based**
- Software runs on either individual workstations or network devices to monitor and track network activity
- You should use NIDSs and HIDSs together to ensure a truly secure environment

NIDS

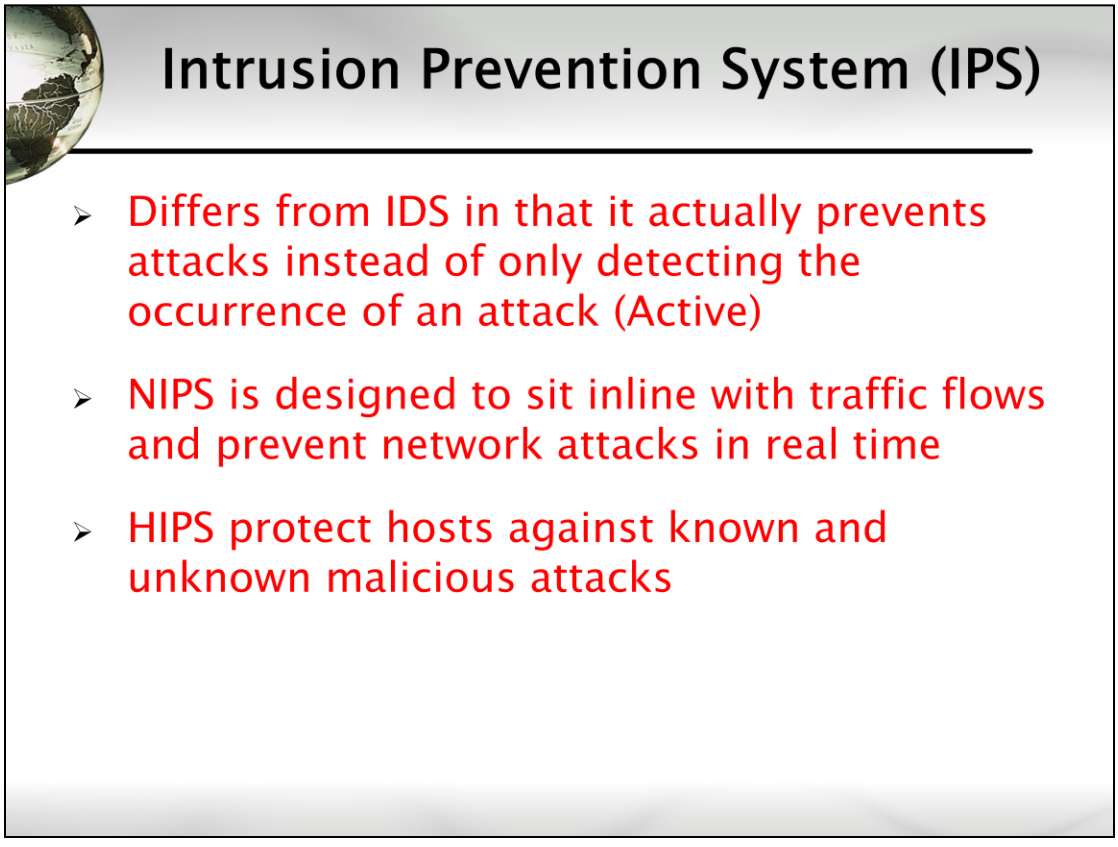

MASTER SENSOR
FILE SERVER
SLAVE SENSOR
WORKSTATIONS
SLAVE SENSOR
Internet
Firewall

NIDS

- Monitor the packet flow and try to locate packets that might have gotten through the firewall and are not allowed for one reason or another on the network
- Best at detecting DoS attacks and unauthorized user access

HIDS

- Monitor communications on a host-by-host basis and try to filter malicious data
- These types of IDSs are good at detecting unauthorized file modifications and user activity



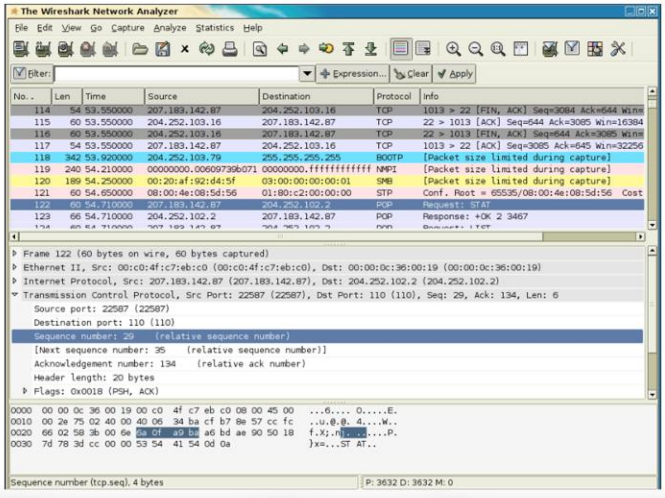
Passive while it detects active while in prevention

Types of Network Monitoring Systems

- **Behavior-based**
  - Looks for variation in behavior like unusually high traffic, policy violations, etc… **(Human based)**
- **Signature-based**
  - Evaluates attacks based on attack signatures
- **Anomaly-based**
  - Looks for anything outside of the ordinary **(Device based)**
  - A baseline must be established first
- **Heuristic (Trend Analysis)**
  - Uses algorithms to analyze network traffic over time.

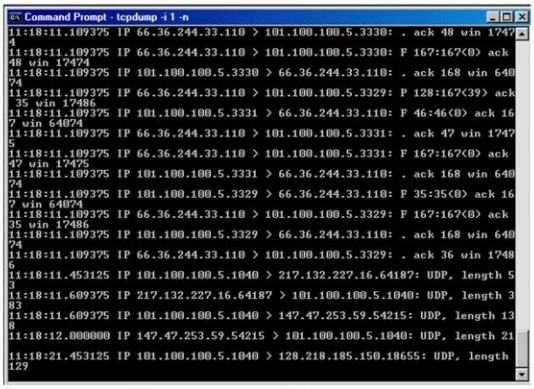
*Protocol Analyzers

- Help you troubleshoot network issues by gathering packet level information across the network



Sniffers

- Tools used to capture network traffic in the form of low-level packets
- Can be used by network administrators to troubleshoot but can also be used for malicious reasons



Unified Threat Management Device (UTM)

- All-In-One Appliance
- URL filter/Content inspection
- Malware inspection filter
- Spam filter
- Router/Switch
- Firewall
- IDS/IPS
- Slow, up to 50% loss in network performance.

Web Application Firewall (WAF)

- Not like a “normal” firewall
  - Applies rules to HTTP conversations
- Allow or deny based on expected input
- SQL injection

29

B. A Web security gateway offers a single point of policy control and management for web-based content access. Answer A is too generic to be a proper answer. Answer C is incorrect because, although an application-level gateway understands services and protocols, the requirement is specifically for webbased content. Answer D is incorrect because content filtering reports only on violations identified in the specified applications listed for the filtering application.

B. A Web security gateway offers a single point of policy control and management for web-based content access. Answer A is too generic to be a proper answer. Answer C is incorrect because, although an application-level gateway understands services and protocols, the requirement is specifically for webbased content. Answer D is incorrect because content filtering reports only on violations identified in the specified applications listed for the filtering application.

31 B. Because you want to monitor both types of traffic, the IDSs should be used together. Network-based intrusion-detection systems monitor the packet flow and try to locate packets that are not allowed for one reason or another and might have gotten through the firewall. Host-based intrusion-detection systems monitor communications on a host-by-host basis and try to filter malicious data. These types of IDSs are good at detecting unauthorized file modifications and user activity. Answer A is incorrect because a router forwards information to its destination on the network or the Internet. A firewall protects computers and networks from undesired access by the outside world; therefore, Answer C is incorrect.

32

B. Because you want to monitor both types of traffic, the IDSs should be used together. Network-based intrusion-detection systems monitor the packet flow and try to locate packets that are not allowed for one reason or another and might have gotten through the firewall. Host-based intrusion-detection systems monitor communications on a host-by-host basis and try to filter malicious data. These types of IDSs are good at detecting unauthorized file modifications and user activity. Answer A is incorrect because a router forwards information to its destination on the network or the Internet. A firewall protects computers and networks from undesired access by the outside world; therefore, Answer C is incorrect.

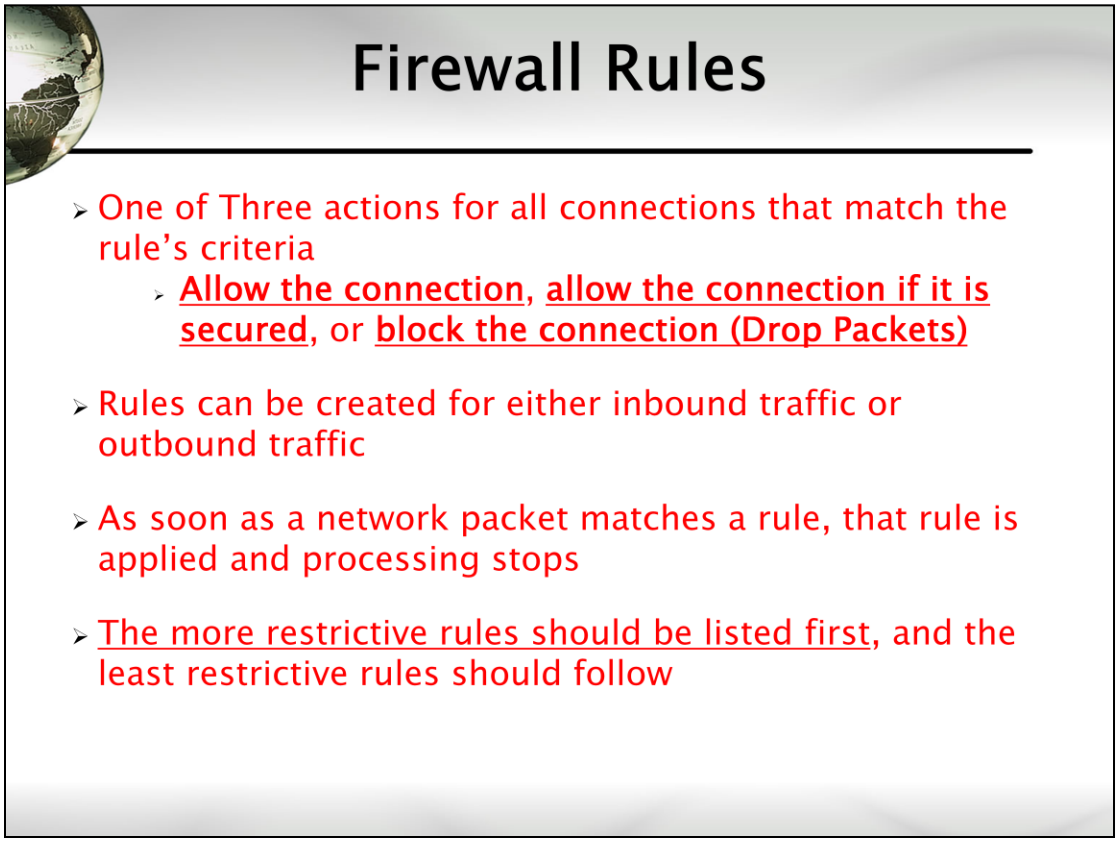
33
B, C, and D. You can place proxy servers between the private network and the Internet for Internet connectivity or internally for web content caching. If the organization is using the proxy server for both Internet connectivity and web content caching, you should place the proxy server between the internal network and the Internet, with access for users who are requesting the Web content. In some proxy server designs, the proxy server is placed in parallel with IP routers. This allows for network load balancing by forwarding of all HTTP and FTP traffic through the proxy server and all other IP traffic through the router. Answer A is incorrect because proxy servers are not used for intrusion detection.

34

B, C, and D. You can place proxy servers between the private network and the Internet for Internet connectivity or internally for web content caching. If the organization is using the proxy server for both Internet connectivity and web content caching, you should place the proxy server between the internal network and the Internet, with access for users who are requesting the Web content. In some proxy server designs, the proxy server is placed in parallel with IP routers. This allows for network load balancing by forwarding of all HTTP and FTP traffic through the proxy server and all other IP traffic through the router. Answer A is incorrect because proxy servers are not used for intrusion detection.

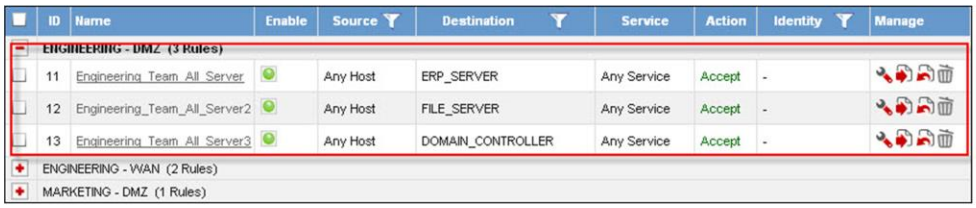
Objective 1.2

- Apply and Implement Secure Network Administration Principles

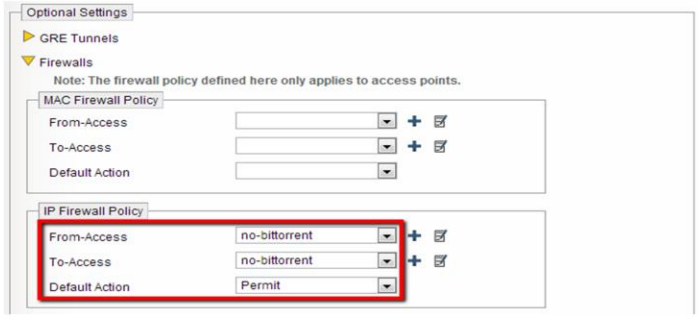


Every Firewall rule and ACL has an implicit deny.

Firewall Rules



	ID	Name	Enable	Source	Destination	Service	Action	Identity	Manage
		ENGINEERING - DMZ (3 Rules)							
	11	Engineering_Team_All_Server		Any Host	ERP_SERVER	Any Service	Accept	-	
	12	Engineering_Team_All_Server2		Any Host	FILE_SERVER	Any Service	Accept	-	
	13	Engineering_Team_All_Server3		Any Host	DOMAIN_CONTROLLER	Any Service	Accept	-	
		ENGINEERING - WAN (2 Rules)							
		MARKETING - DMZ (1 Rules)							



VLAN Management

- Provide a way to limit broadcast traffic in a switched network
- Creates a boundary and, in essence, creates multiple, isolated LANs on one switch

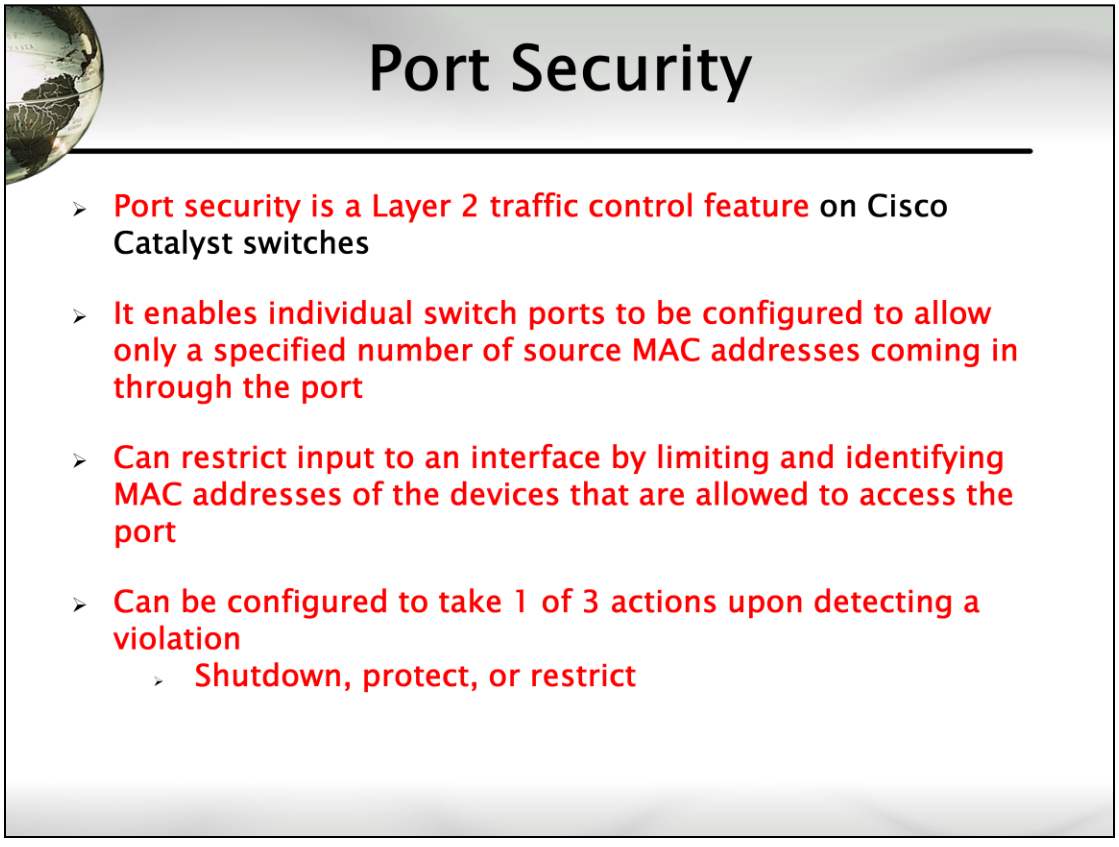
Secure Router Configuration

- Create and maintain a written router security policy
- The policy should identify who is allowed to log in to the router, who is allowed to configure and update it, and outline the logging and management practices for it
- Comment and organize offline master editions of your router configuration files. Keep the offline copies of all router configurations in sync with the actual configurations running on the routers
  - (TFTP Server)
- Implement access lists that allow only those protocols, ports, and IP addresses that are required by network users and services and that deny everything else (ACLs)
- Test the security of your routers regularly, especially after any major configuration changes

Router Access Control Lists (ACLs)

- Ability to filter packets, by source address, destination address, protocol, or port

- Standard ACLs– 1 – 99 and 1300 – 1999
- Extended ACLs – 100 – 199 and 2000 – 2699



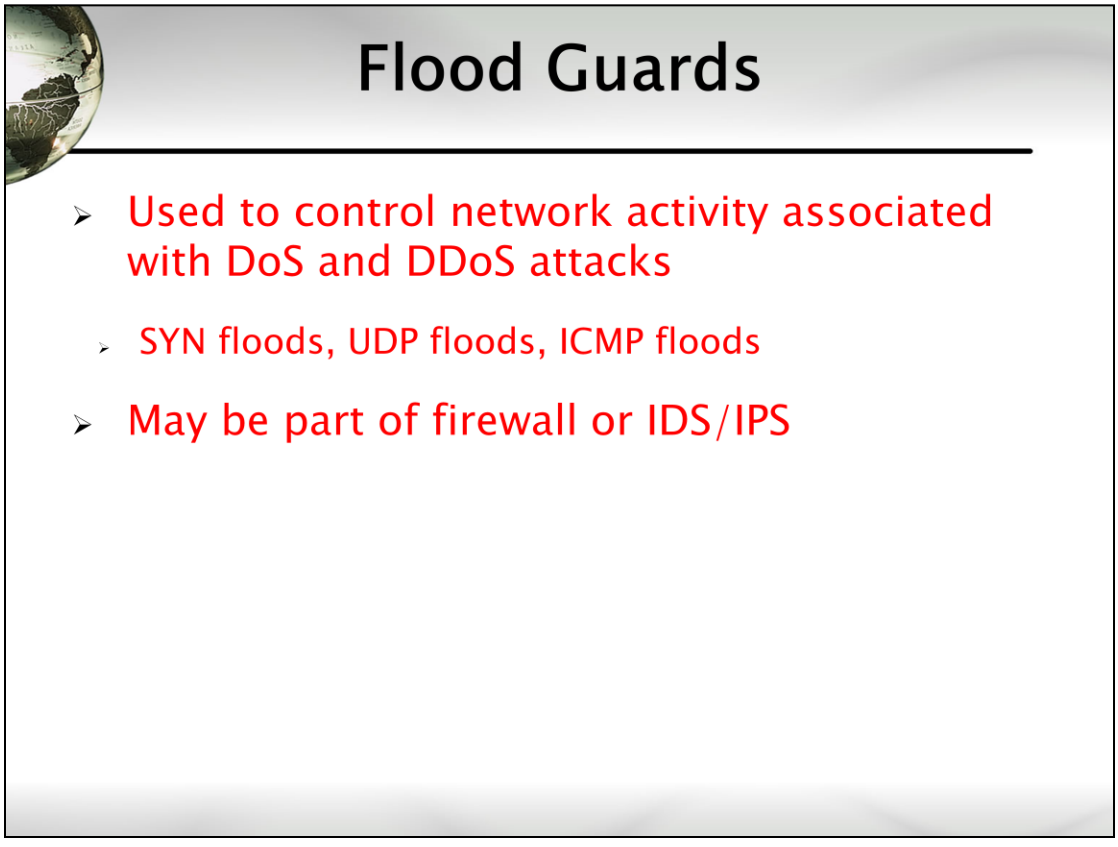
Shutdown – shuts down until admin reenables it

Protect – Shuts down unless the correct device is connected

Restrict – Shuts down after a certain number of times the incorrect device is connected

802.1X

- Provides the capability to permit or deny network connectivity, control VLAN access and apply traffic policy, based on user or machine identity
- Ideal for wireless access points and the authentication process, helps mitigate many of the risks involved in using WEP
- Keeps the network port disconnected until authentication is completed



DoS – Denial of Service – one device

DDoS – Distributed Denial of Service – two or more devices

SYN floods – continues to send Synchroniza

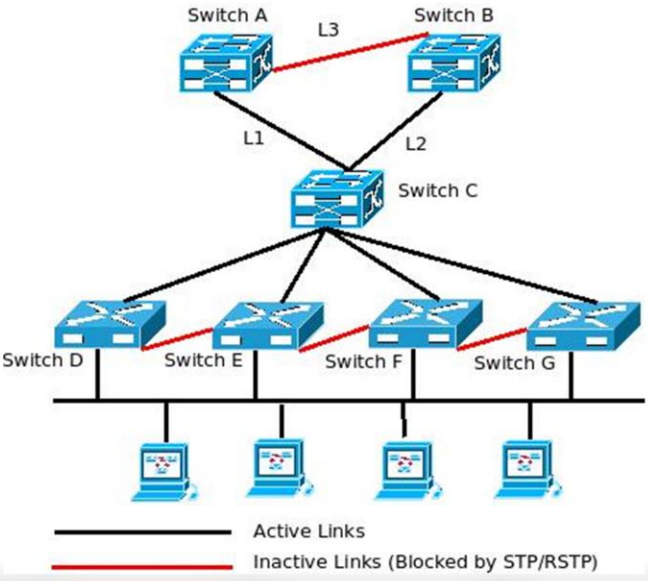
UDP floods – continues to send UDP packets

ICMP floods – continues to send ICMP packe

Loop Protection

- A major feature in Layer 2 managed switches is the Spanning Tree Protocol (STP)
- STP is a link management protocol that provides path redundancy while preventing undesirable loops in the network
- Multiple active paths between stations cause loops in the network

STP


Switch A
L3
Switch B
L1
L2
Switch C
Switch D
Switch E
Switch F
Switch G
Active Links
Inactive Links (Blocked by STP/RSTP)

Implicit Deny

- An access control practice wherein resource availability is restricted to only those logons explicitly granted access, remaining unavailable even when not explicitly denied access
- Used commonly in all networks and firewalls, where most ACLs have a default setting of "implicit deny"
- Implicit is not written in the ACL and assumed
- Explicit Deny is written in for logging purposes.

Network Segmentation

- The potential for damage greatly increases If one compromised system on the network could spread to other networks
- Networks that are shared by partners, vendors, or departments should have clear separation boundaries
  - VLANs
  - Subnetting

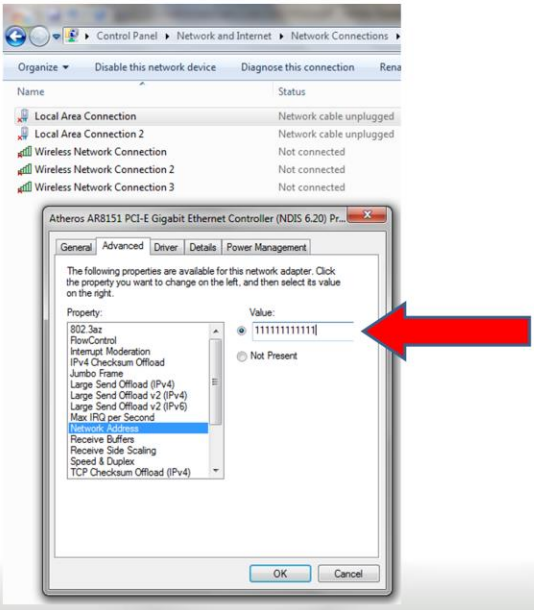
Log Analysis

- Logging is the process of collecting data to be used for monitoring and auditing purposes
- Develop standards for each platform, application, and server type to make a checklist or monitoring function
- Choose carefully what to log
- Logs take up disk space and use system resources
- Large log files could bog down the system and take a long time to audit.
- Mandate a common storage location for all logs (SYSLog Server)
- Documentation should state proper methods for archiving and reviewing logs

Exam Alert

- Although a deterrent, port security is not a reliable security feature
- MAC addresses can be spoofed, and multiple hosts can still easily be hidden behind a small router

MAC Spoofing



53
A. The loop guard feature makes additional checks in Layer 2 switched networks. Answer B is incorrect because a flood guard is a firewall feature to control network activity associated with DoS attacks. Answer C is incorrect because implicit deny is an access control practice wherein resource availability is restricted to only those logons explicitly granted access. Answer D is incorrect because port security is a Layer 2 traffic control feature on Cisco Catalyst switches. It enables individual switch ports to be configured to allow only a specified number of source MAC addresses coming in through the port.

54

A. The loop guard feature makes additional checks in Layer 2 switched networks. Answer B is incorrect because a flood guard is a firewall feature to control network activity associated with DoS attacks. Answer C is incorrect because implicit deny is an access control practice wherein resource availability is restricted to only those logons explicitly granted access. Answer D is incorrect because port security is a Layer 2 traffic control feature on Cisco Catalyst switches. It enables individual switch ports to be configured to allow only a specified number of source MAC addresses coming in through the port.

55

C. Implicit deny is an access control practice wherein resource availability is restricted to only those logons explicitly granted access. Answer A is incorrect because the loop guard feature makes additional checks in Layer 2 switched networks. Answer B is incorrect because a flood guard is a firewall feature to control network activity associated with DoS attacks. Answer D is incorrect because port security is a layer 2 traffic control feature on Cisco Catalyst switches. It enables individual switch ports to be configured to allow only a specified number of source MAC addresses coming in through the port.

56

C. Implicit deny is an access control practice wherein resource availability is restricted to only those logons explicitly granted access. Answer A is incorrect because the loop guard feature makes additional checks in Layer 2 switched networks. Answer B is incorrect because a flood guard is a firewall feature to control network activity associated with DoS attacks. Answer D is incorrect because port security is a layer 2 traffic control feature on Cisco Catalyst switches. It enables individual switch ports to be configured to allow only a specified number of source MAC addresses coming in through the port.

57

C. With interconnected networks, the potential for damage greatly increases because one compromised system on one network can easily spread to other networks. Networks that are shared by partners, vendors, or departments should have clear separation boundaries. Answer A is incorrect because logging is the process of collecting data to be used for monitoring and auditing purposes. Answer B is incorrect because access control generally refers to the process of making resources available to accounts that should have access, while limiting that access to only what is required. Answer D is incorrect because implementing a VPN does not separate the networks.

C. With interconnected networks, the potential for damage greatly increases because one compromised system on one network can easily spread to other networks. Networks that are shared by partners, vendors, or departments should have clear separation boundaries. Answer A is incorrect because logging is the process of collecting data to be used for monitoring and auditing purposes. Answer B is incorrect because access control generally refers to the process of making resources available to accounts that should have access, while limiting that access to only what is required. Answer D is incorrect because implementing a VPN does not separate the networks.

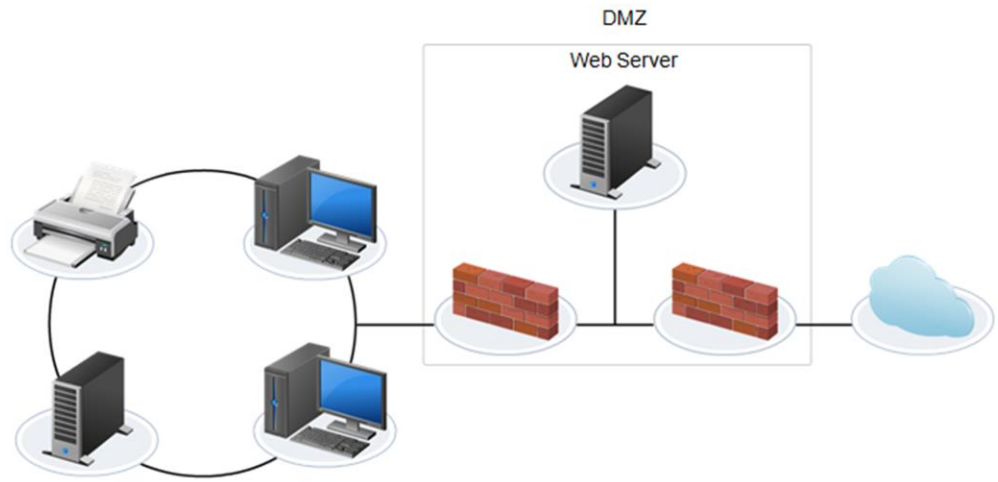
Objective 1.3

- Explain Network Design Elements and Compounds.

Demilitarized Zone (DMZ)

- A small network between the internal network and the Internet that provides a layer of security and privacy
- Often, web and mail and proxy servers are placed in the DMZ
- Because these devices are exposed to the Internet, it is important that they are hardened and patches are kept current

DMZ



Intranet

- Portion of the internal network that uses web-based technologies
- The information is stored on web servers and accessed using browsers
- If the intranet can be accessed from public networks, it should be through a VPN for security reasons

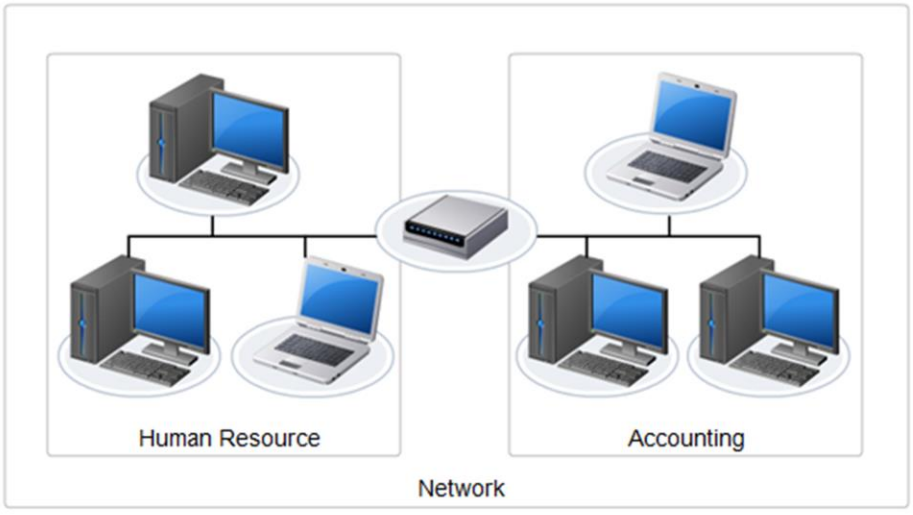
Extranet

- The public portion of the company's IT infrastructure that allows resources to be used by authorized partners and resellers that have proper authorization and authentication
- Commonly used for business-to-business relationships

Subnetting

- Makes efficient use of network address space and controls network traffic
- Allows you to arrange hosts into the different logical groups that isolate each subnet into its own mini network
- If an incident happens and you notice it quickly, you can usually contain the issue to that particular subnet

Subnetting



Subnet Mask

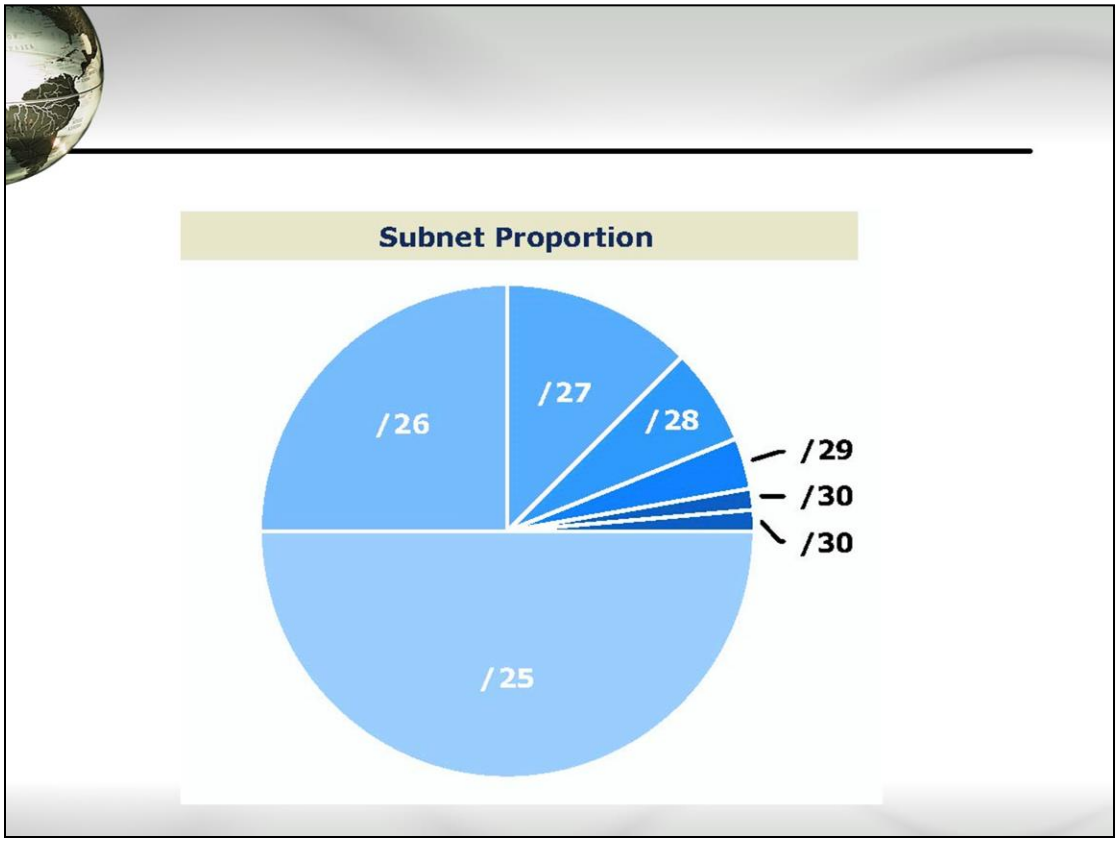
- Used to determine if IP address is local or remote
  - Default Subnet Masks
    - Class A 255.0.0.0
    - Class B 255.255.0.0
    - Class C 255.255.255.0 254 usable addresses

Classless Interdomain Routing (CIDR)

- Classful has a set Subnet Mask
- (i.e..Class A 255.0.0.0)

- Classful does not send it's Subnet Mask.

- CIDR only means the amount of bits used as the Network ID


Subnet Proportion
/26
/27
/28
/29
/30
/30
/25

Subnetting Short Cut

CIDR	/8	/9	/10	/11	/12	/13	/14	/15
Host Range	256	128	64	32	16	8	4	2
# of Subnets	1	2	4	8	16	32	64	128
Subnet Mask	0	128	192	224	240	248	252	254

255.X.0.0

CIDR	/16	/17	/18	/19	/20	/21	/22	/23
Host Range	256	128	64	32	16	8	4	2
# of Subnets	1	2	4	8	16	32	64	128
Subnet Mask	0	128	192	224	240	248	252	254

255.255.X.0

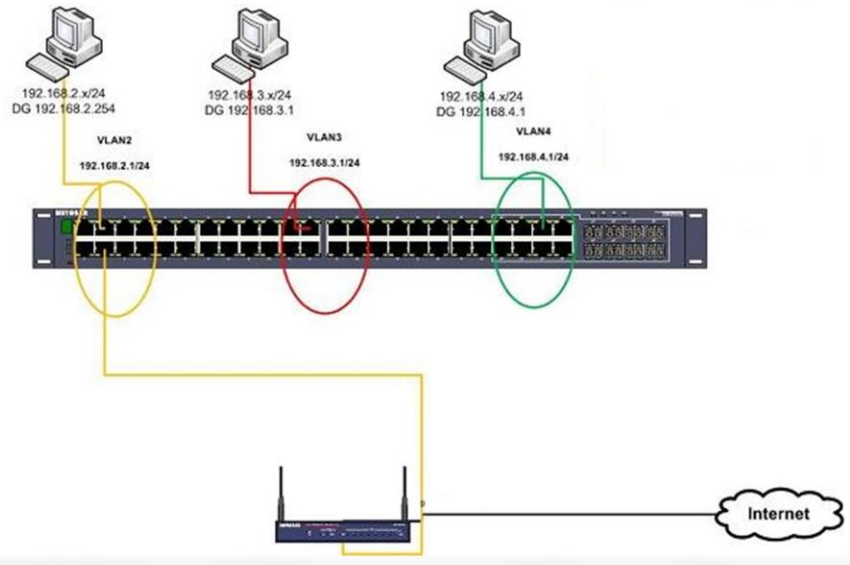
CIDR	/24	/25	/26	/27	/28	/29	/30
Host Range	256	128	64	32	16	8	4
# of Subnets	1	2	4	8	16	32	64
Subnet Mask	0	128	192	224	240	248	252

255.255.255.X

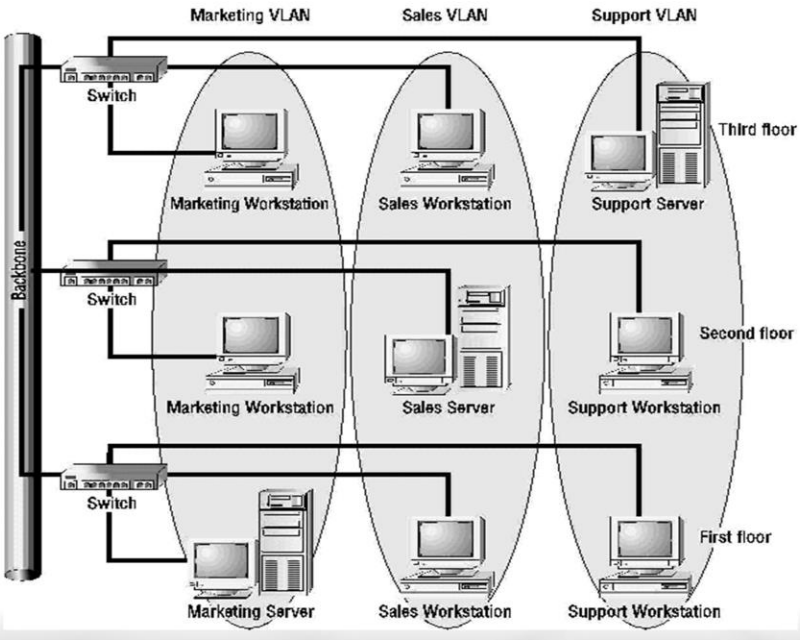
VLAN – Virtual LAN

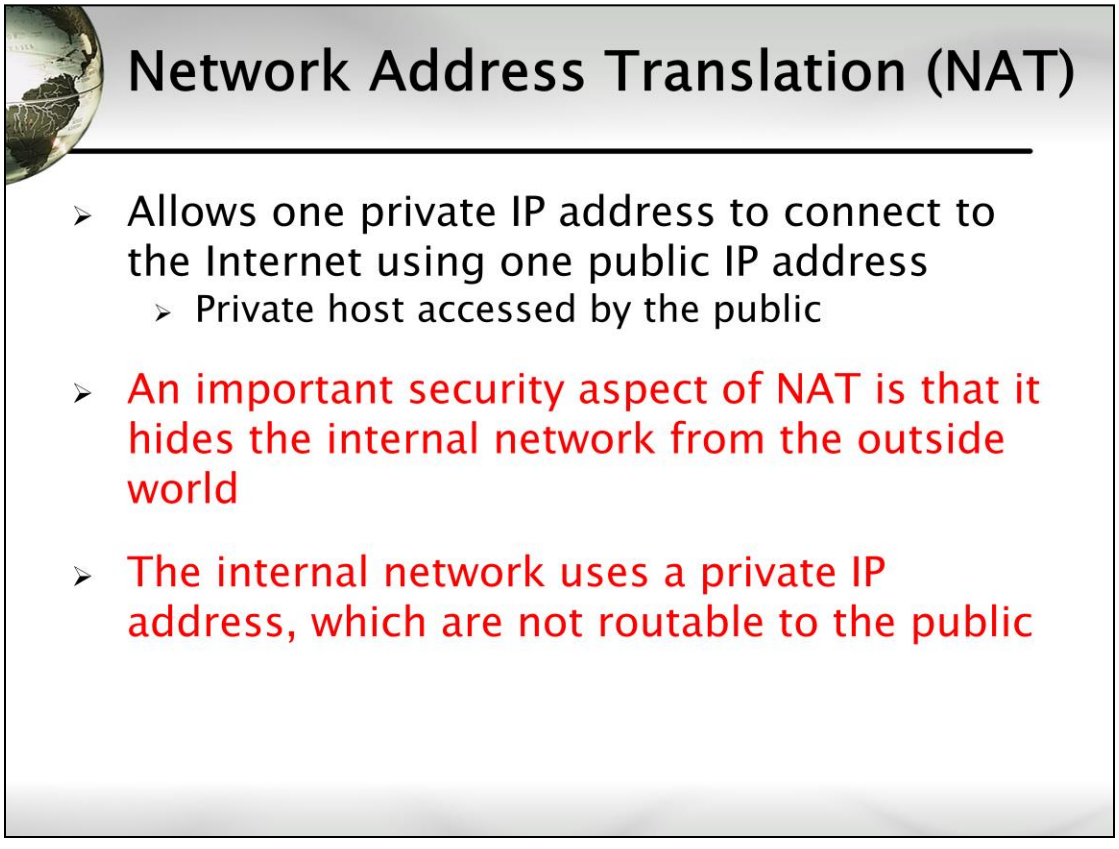
- Purpose is to unite network nodes logically into the same broadcast domain regardless of their physical attachment to the network
- Provide a way to limit broadcast traffic in a switched network
- Creates multiple, isolated LANs on one switch
- A router is required if data is to be passed from one VLAN to another

VLAN


192.168.2.x/24
DG 192.168.2.254
192.168.3.x/24
DG 192.168.3.1
192.168.4.x/24
DG 192.168.4.1
VLAN2
192.168.2.1/24
VLAN3
192.168.3.1/24
VLAN4
192.168.4.1/24
Internet

VLAN


Marketing VLAN
Sales VLAN
Support VLAN
Backbone
Switch
Switch
Switch
Marketing Workstation
Sales Workstation
Support Server
Third floor
Marketing Workstation
Sales Server
Support Workstation
Second floor
Marketing Server
Sales Workstation
Support Workstation
First floor

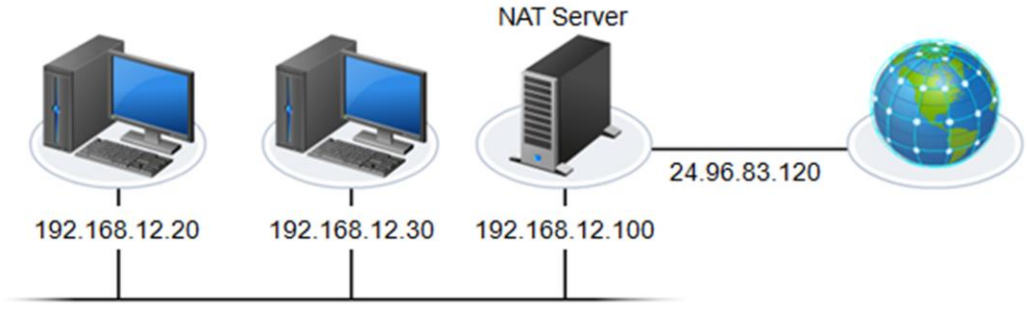


Static NAT – 1 to 1

Dynamic NAT – 1 Public to Many private, rotates usage of Public IP address pool

Port Address Translation (PAT) – Many to 1, Port Based (Also known as NAT Overload)

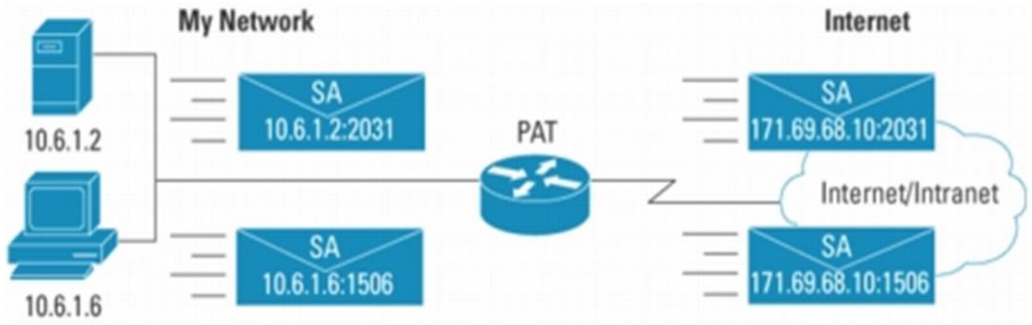
NAT



Port Address Translation (PAT)

- Extends NAT from one-to-one to many-to-one
- Allows many private IP address to connect to the Internet using one public IP address
- Also known as NAT Overloading

PAT



Port Address Translation (PAT) extends NAT from "1 to 1" to "many-to-1" by associating the source port with each flow

Exam Alert

- Another address range to keep in mind when designing IP address space is Automatic Private IP Addressing (APIPA) , Microsoft Only
- In the event that a Dynamic Host Configuration Protocol (DHCP) server is not available at the time that the client issues a DHCP lease request, the client is automatically configured with an address from the 169.254.0.1 through 169.254.255.254 range, Microsoft Only

*Remote Access

- Remote Access Services (RAS) lets you connect your computer from a remote location, such as your home or any on-the-road location, to a corporate network
- RAS is achieved primarily through VPNs using IPsec or Secure Socket Layer (SSL)
- By using a remote-access VPN, secure access to corporate resources can be provided using an encrypted tunnel over the Internet

Telephony

- The transmission of data through equipment in a telecommunications environment
- Includes transmission of voice, fax, or other data
- VoIP
  - VLANs
  - Quality of Service (QoS)
    - Dot1q
- Modems

Network Access Control (NAC)

- Offers a method of enforcement that helps ensure computers are properly configured
- Idea is to secure the environment by examining the user's machine and based on the results grant (or not grant) access accordingly
- If the user's computer patches are not up-to-date, and no desktop firewall software and Antivirus is installed, it will not be granted access

Virtualization

- Offers cost benefits by decreasing the number of physical machines required within an environment
  - Workstations, servers, firewalls, etc…
- Control of physical device is gone
  - May be difficult to apply external security components
- Updates are a concern

Cloud Computing

- A very general term which describes anything that involves delivering hosted computing services over the Internet
- The typical cloud computing provider delivers computing power, storage, and common applications online to users who access them from a web browser or portal

Platform-as-a-Service (PaaS)

- The delivery of a computing platform, **always** an operating system with associated services, that is delivered over the Internet without downloads or installation
- PaaS = OS

Software-as-a-Service (SaaS)

- The delivery of a licensed application to customers over the Internet for use as a service on demand
- SaaS vendors host an application and allows the customer to download the application for a set period of time

Infrastructure-as-a-Service (IaaS)

- The delivery of computer infrastructure in a hosted service model over the Internet
- Allows the client to literally outsource everything that would normally be in a typical IT department
- Data center space, servers, networking equipment, and software can all be leased as a service

Private Cloud

- A private cloud is a cloud service within a corporate network and isolated from the Internet
- A virtual private cloud is a service offered by a public cloud provider that provides an isolated subsection of a public or external cloud for exclusive use by an organization internally

Public Cloud

- A public cloud is a cloud service that is accessible to the general public, typically over an Internet connection
- Public cloud services often require some form of subscription or pay per use, rather than being offered for free

Hybrid Cloud

- A hybrid cloud is a mixture of private and public cloud components
- an organization could host a private cloud for exclusive internal use but distribute some resources onto a public cloud for the public, business partners, customers and the external sales force

Community

- A community cloud is a cloud environment maintained, used, and paid for by a group of users or organizations for their shared benefit, such as collaboration and data exchange

- Allows for some cost savings versus accessing private or public clouds independently

Layered security/Defense in depth

- Defense in depth is the use of multiple types of access controls in literal or theoretical concentric circles or layers
- This form of layered security helps an organization avoid a monolithic security stance.
- A monolithic mentality is the belief that a single security mechanism is all that is required to provide sufficient security

6 **The purpose of a VLAN is to unite network nodes logically into the same** broadcast domain regardless of their physical attachment to the network. Answer A is incorrect because a DMZ is a small network between the internal network and the Internet that provides a layer of security and privacy. Answer B is incorrect because a VPN is a network connection that allows you access via a secure tunnel created through an Internet connection. Answer D is incorrect because NAT acts as a liaison between an internal network and the Internet.

6. **The purpose of a VLAN is to unite network nodes logically into the same** broadcast domain regardless of their physical attachment to the network. Answer A is incorrect because a DMZ is a small network between the internal network and the Internet that provides a layer of security and privacy. Answer B is incorrect because a VPN is a network connection that allows you access via a secure tunnel created through an Internet connection. Answer D is incorrect because NAT acts as a liaison between an internal network and the Internet.

B. A DMZ is a small network between the internal network and the Internet that provides a layer of security and privacy. Answer A is incorrect. The purpose of a VLAN is to unite network nodes logically into the same broadcast domain regardless of their physical attachment to the network. Answer C is incorrect because NAT acts as a liaison between an internal network and the Internet. Answer D is incorrect because a VPN is a network connection that allows you access via a secure tunnel created through an Internet connection.

B. A DMZ is a small network between the internal network and the Internet that provides a layer of security and privacy. Answer A is incorrect. The purpose of a VLAN is to unite network nodes logically into the same broadcast domain regardless of their physical attachment to the network. Answer C is incorrect because NAT acts as a liaison between an internal network and the Internet. Answer D is incorrect because a VPN is a network connection that allows you access via a secure tunnel created through an Internet connection.

Objective 1.4

- Implement and Use Common Protocols

Internet Protocol Security (IPsec)

- Authentication and encapsulation standard is widely used to establish secure VPN communications
  - VPN Tunnels
  - IPv6
- Secures transmissions between servers and clients
- Functions within the network layer

IPsec Services

- The asymmetric key standard defining IPsec provides Two primary security services
  - **Authentication Header (AH)**
  - Provides authentication of the data's sender, along with **integrity and nonrepudiation**
  - **Encapsulating Security Payload (ESP)**
  - Supports authentication of the data's sender and encryption of the data being transferred along with **confidentiality and integrity protection**

IPsec Modes of Operation

- Transport Mode
  - Only the **payload** of the IP packet is encrypted and/or authenticated
- Tunnel Mode
  - The **entire** IP packet is encrypted and/or authenticated

IKE (Internet Key Exchange)

- IKE ensures the secure exchange of secret keys between communication partners in order to establish the encrypted VPN tunnel.

ISAKMP

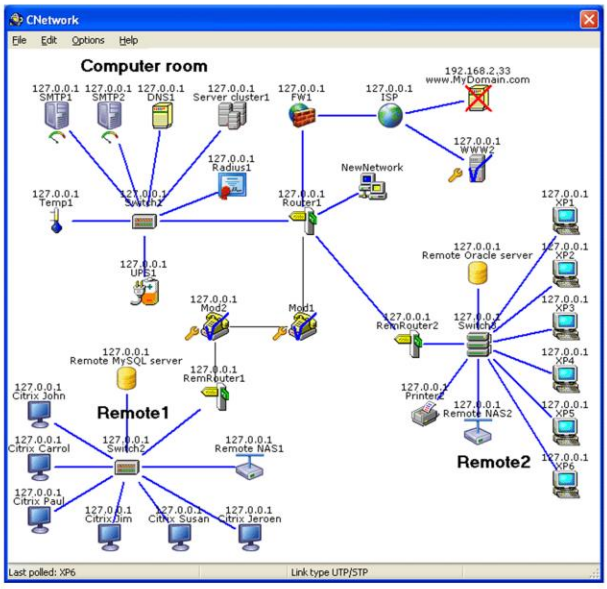
- ISAKMP (Internet Security Association and Key Management Protocol)
  - used to negotiate and provide authenticated keying material (a common method of authentication) for security associations in a secured manner

  - Authentication of communications peers
  - Threat mitigation
  - Security association creation and management
  - Cryptographic key establishment and management

Simple Network Management Protocol (SNMP)

- An application layer protocol whose purpose is to collect statistics from TCP/IP devices
- Used for monitoring the health of network equipment, computer equipment, and devices such as uninterruptible power supplies (UPSs)
- SNMPv1 and v2 had security holes in the "community string"
- SNMPv3 added security in the form of authentication and encryption
- Ports 160,161,162

SNMP Network Map



Secure Shell (SSH) Connections

- A more secure replacement for the common command-line terminal utility Telnet
- Requires encryption of all data, including the login portion
- SSH runs on TCP port 22
  - Also SFTP (Secure FTP)and SCP (Secure Copy)
- Only used for the encrypted configuration of a router or switch

Unix based SSH

Domain Name Service (DNS)

- Allows hosts to resolve hostnames (FQDN) to IP addresses
- Critical service that must be protected
- DNS troubleshooting tools
  - Nslookup
  - Dig
- Uses TCP/UDP Port 53

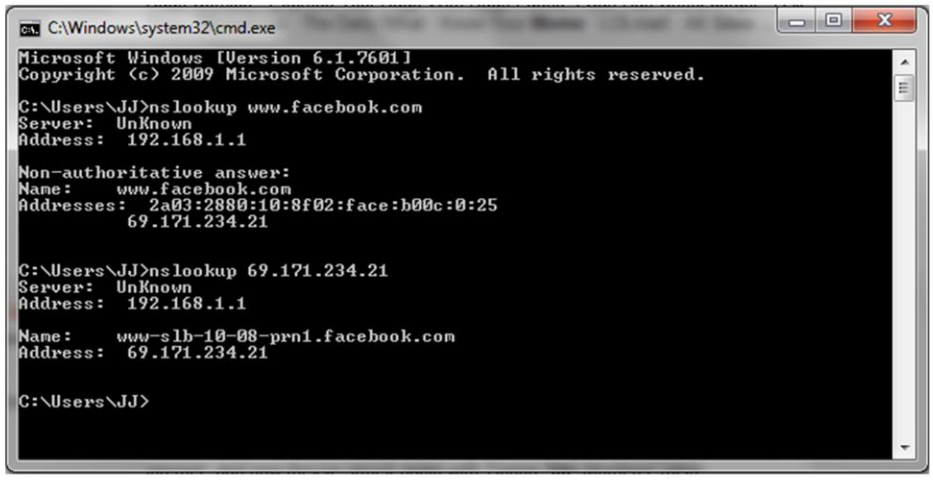
DNS record keeping

- DNS records are kept in various places depending on the application

Record	Type	Description
A	Address record	Links a FQDN to an IPv4 address
AAAA	Address record	Links a FQDN to an IPv6 address
PTR	Pointer record	Links an IP address to a FQDN (for reverse lookups)
CNAME	Canonical name	Links a FQDN alias to another FQDN
MX	Mail exchange	Links a mail- and messaging-related FQDN to an IP address
NS	Name server record	Designates the FQDN and IP address of an authorized name server
SOA	Start of authority record	Specifies authoritative information about the zone file, such as primary name server, serial number, timeouts, and refresh intervals

Nslookup

- Used to resolves web addresses to IP addresses and vice versa



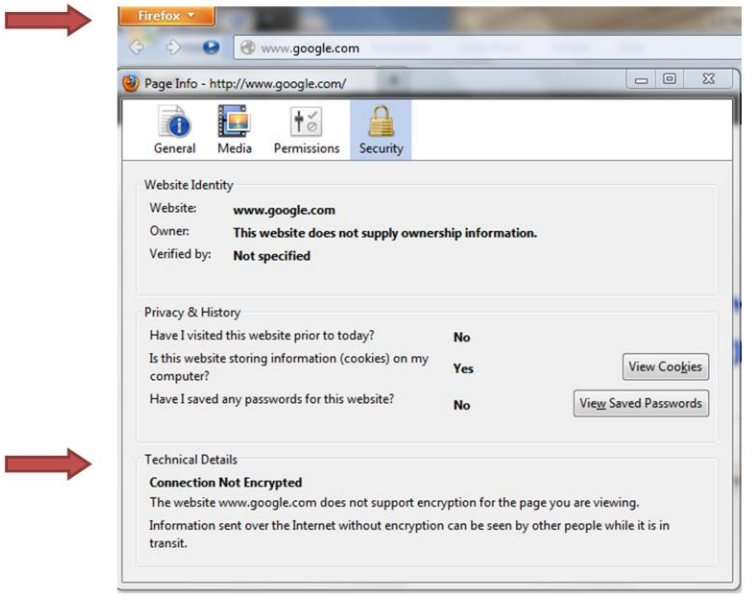
Transport Layer Security (TLS)

- The successor to SSL
- Uses stronger encryption methods
- Port 443 (https)

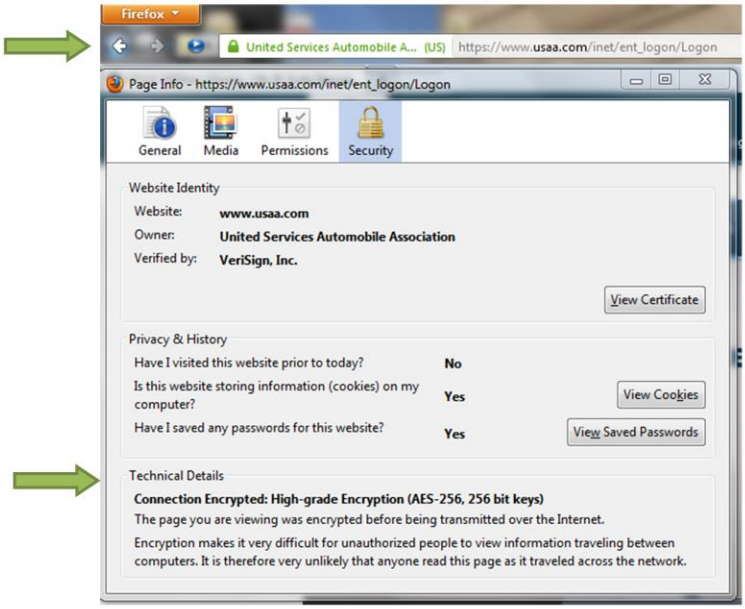
Secure Sockets Layer (SSL)

- Used by millions of websites in the protection of their online transactions with their customers
- A public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality
- Uses certificates for authentication and encryption for message integrity and confidentiality
- Connection is negotiated by a handshaking procedure between client and server
- During this handshake, the client and server exchange the specifications for the cipher that will be used for that session
- Port 443 (https)

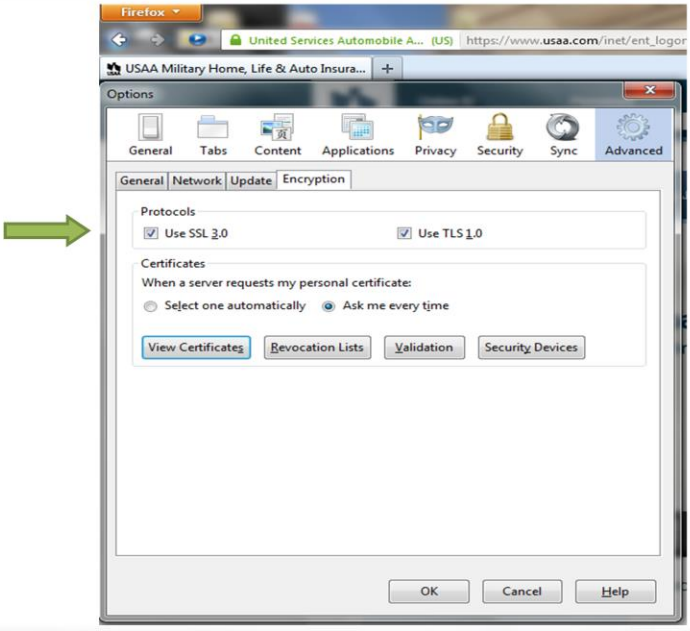
SSL and TLS


Firefox
www.google.com
Page Info - http://www.google.com/
General
Media
Permissions
Security
Website Identity
Website: www.google.com
Owner: This website does not supply ownership information.
Verified by: Not specified
Privacy & History
Have I visited this website prior to today? No
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Not Encrypted
The website www.google.com does not support encryption for the page you are viewing.
Information sent over the Internet without encryption can be seen by other people while it is in transit.

SSL and TLS


Firefox
United Services Automobile A... (US)
https://www.usaa.com/inet/ent_logon/Logon
Page Info - https://www.usaa.com/inet/ent_logon/Logon
General
Media
Permissions
Security
Website Identity
Website:
www.usaa.com
Owner:
United Services Automobile Association
Verified by:
VeriSign, Inc.
View Certificate
Privacy & History
Have I visited this website prior to today?
No
Is this website storing information (cookies) on my computer?
Yes
View Cookies
Have I saved any passwords for this website?
Yes
View Saved Passwords
Technical Details
Connection Encrypted: High-grade Encryption (AES-256, 256 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

SSL and TLS


Firefox
United Services Automobile A... (US)
https://www.usaa.com/inet/ent_logor
USAA Military Home, Life & Auto Insura...
Options
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
General
Network
Update
Encryption
Protocols
Use SSL 3.0
Use TLS 1.0
Certificates
When a server requests my personal certificate:
Select one automatically
Ask me every time
View Certificates
Revocation Lists
Validation
Security Devices
OK
Cancel
Help

TCP/IP

- Comprised of **four** main protocols
- Internet Protocol (IP)
  - Responsible for providing essential routing functions for all traffic on a TCP/IP network
- Transmission Control Protocol (TCP)
  - Provides connection-oriented communication
  - 3-way handshake
  - Reliable and uses sequence numbers
- User Datagram Protocol (UDP)
  - Provides connectionless communications
  - Unreliable
  - VOIP uses UCP
- Internet Control Message Protocol (ICMP).
  - Provides administrative services to TCP/IP networks
  - PING, Traceroute, Multicast

TCP/IP

TABLE 2.1 **OSI and TCP/IP Model Comparison**

OSI Reference Model	TCP/IP Reference Model
Application Presentation Session	Application
Transport	Transport
Network	Internet
Data Link Physical	Network Access

File Transfer Protocol over SSL (FTPS)

- FTP passes the username and password in a plain-text form, allowing packet sniffing of the network traffic to read these values, which may then be used for unauthorized access to the server
- FTPS is an FTP extension that adds support for TLS and SSL
- Port 989 (Data) and 990 (Control)

Hypertext Transport Protocol Secure (HTTPS)

- Basic web connectivity using Hypertext Transport Protocol (HTTP) occurs over TCP port 80, providing no security against interception of transacted data sent in clear text
- HTTPS is an alternative that involves the use of TLS and or SSL
  - Operates on port 443

Exam Alert

- An alternative to HTTPS is the Secure Hypertext Transport Protocol (S-HTTP), which was developed to support connectivity for banking transactions and other secure web communications
- S-HTTP supports DES, 3DES, RC2, and RSA2 encryption, along with CHAP authentication, but was not adopted by the early web browser developers (for example, Netscape and Microsoft) and so remains less common than the HTTPS standard

Secure Copy Protocol (SCP)

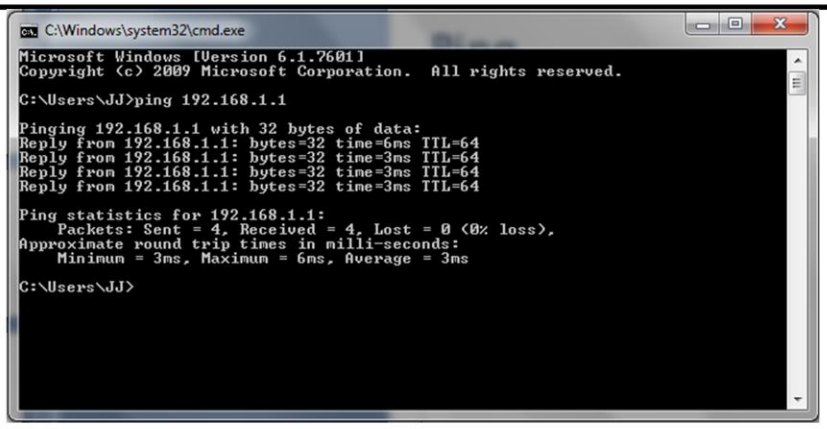
- Network protocol that supports file transfers
- Uses SSH protocol to perform authentication and encryption
- SCP runs on port 22 and protects the authenticity and confidentiality of the data in transit

Internet Control Message Protocol (ICMP)

- A protocol to test for connectivity and search for configuration errors in a network
  - Ping
  - Tracert

ICMP Type	Description
0	Echo request
8	Echo reply
11	Time exceeded
3	Destination unreachable
5	Redirect

Ping



- Ping -t
  - Continuous ping
  - Ctrl-C

Tracert

- Tracert- Microsoft
- Traceroute- Cisco and linix command
- An ICMP command used to measure latency and “hops” between each device in route to the targeted IP address.

- Can be useful in troubleshooting network issues

IPv4 versus IPv6

- Due to the increased demand of devices requiring IP addresses, IPv4 was not able to keep up with such an expansive demand
- As a result, a new method was needed to address all the new devices requiring IP addresses
- IPv4- 32 bit, 4 octets
- IPv6 -128 bit, 8 segments

IPv4 versus IPv6

TABLE 2.2 **IPv4 and IPv6 Comparison**

IPv4	IPv6
Addresses are 32 bits (4 bytes) in length.	Addresses are 128 bits (16 bytes) in length.
Header includes a checksum and options.	Header does not include a checksum, and all optional data is moved to IPv6 extension headers.
ARP uses broadcast request frames to resolve an IP address to a link-layer address.	Multicast Neighbor Solicitation messages are used to resolve IP addresses to link-layer addresses.
IPv4 header does not identify packet flow for QoS.	IPv6 header identifies packet flow for QoS.
IPsec support is optional.	IPsec support is required.
IPv4 limits packets to 64-KB of payload.	IPv6 has optional support for jumbograms, which can be as large as 4-GB.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.

iSCSI

- Internet Small Computer System Interface (iSCSI) is a **networking storage** standard based on IP
- This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public Internet connections.
- iSCSI is often viewed as a low-cost alternative to Fibre Channel

Fibre Channel

- Fibre Channel is a form of network data-storage solution (storage area network [SAN]) or network-attached storage [NAS]) that allows for high-speed file transfers at upward of 16Gbps

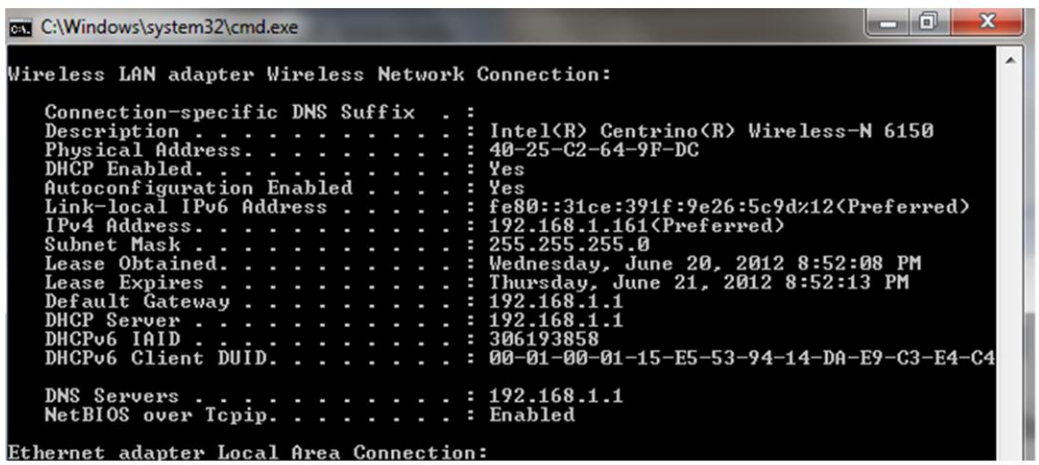
Fibre Channel communication over Ethernet (FCoE)

- FCoE is used to encapsulate Fibre Channel communications over Ethernet networks
- Typically requires 10 Gbps Ethernet in order to support the Fibre Channel protocol
- With this technology, Fibre Channel operates as a Network layer or OSI Layer 3 protocol, replacing IP as the payload of a standard Ethernet network

File Transfer Protocol (FTP)

- This protocol is often used to move fi les between one system and another either over the Internet or within private networks
- FTP is an in-the-clear file-exchange protocol
- Supported by any computer system that uses TCP/IP
- FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, and it then often uses a randomly selected higher port (above 1023) for file transfers.

Ipconfig /all



Ipconfig – Microsoft
Ifconfig - Linix

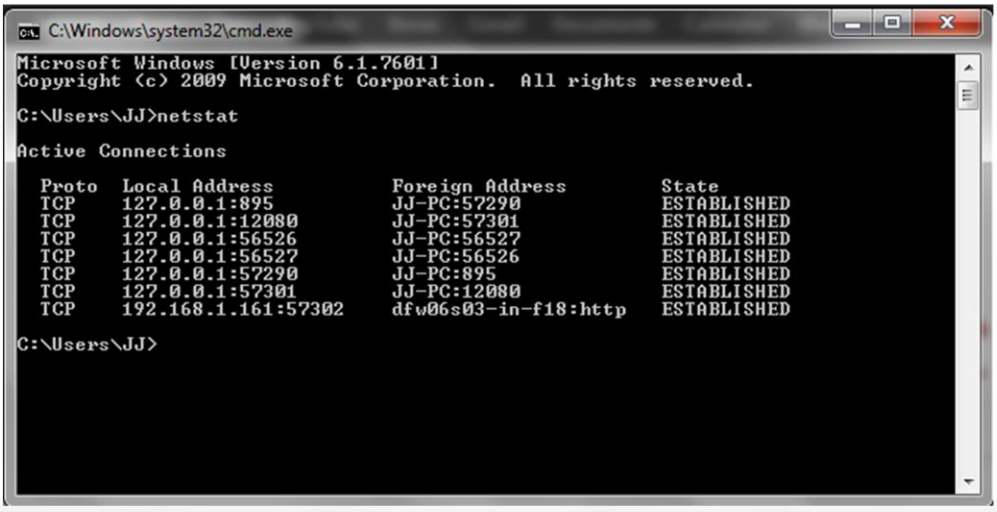
Ipconfig /release – releases DHCP

Ipconfig /renew – renews DHCP

Ipconfig /flushdns – deletes DNS info on device

Netstat

- Microsoft
- Who you are connected to and who is connected to you
- Used to display network connections (incoming and outgoing)



SSH FTP (SFTP)

- SFTP, or secure FTP, is a program that uses SSH to transfer files
- Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network
- Port 22

Trivial File Transfer Protocol (TFTP)

- Simple protocol to transfer files
- Only reads and writes files (or mail) from/to a remote server
- Uses UDP port 69
- Only for the storage of config files for routers and switches

TELNET

- Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn't support transfer of files
- TCP port 23
- Because it's a cleartext protocol and service, it should be avoided and replaced with SSH

Network Basic Input/ Output System (NetBIOS)

- Allows applications on separate computers to communicate over a LAN
- Non-routable
- NetBIOS can run over TCP/IP via the NetBIOS over TCP/IP (NBT) protocol
- NetBIOS uses ports137, 138, and 139

Port Numbers

- There are 65,536 TCP and UDP ports on which a computer can communicate
- The port numbers are divided into three ranges
  - Well-known ports: The well-known ports are those from 0 through1,023
  - Registered ports: The registered ports are those from 1,024 through 49,151
  - Dynamic/private ports: The dynamic/private ports are those from 49,152 through 65,535

Ports To Know

PORT	Service/Protocol
20, 21	FTP
22	SSH, SFTP, SCP
23	Telnet
25	SMTP
49	TACACS+ (Cisco)
53	DNS
69	TFTP
80	HTTP
88	Kerberos

PORT	Service/Protocol
110	POP3
137,138,139	NetBIOS
143	IMAP
161, 162	SNMP
389	LDAP
443	HTTPS
1812	RADIUS
3389	RDP (Remote Access)

Remote Desktop Protocol (RDP)

- Remote access protocol used by many systems as a means of remotely configuring another system via GUI
- Supports full desktop emulation
- TCP Port 3389

OSI relevance

- The OSI model (ISO/IEC 7498-1) was developed over three decades ago as a conceptual reference model for describing protocols, as well as potentially to guide their design
- The most widely used protocol in the world today is TCP/IP (which is in fact a protocol suite rather than an individual protocol)
- This four-layer model is also referred to as the DARPA model or the DoD model
- On the Security+ exam, when a layer name or number is mentioned, assume that it means the OSI model, unless it specifies TCP/IP model

D. SCP runs on port 22 and protects the authenticity and confidentiality of the data in transit. Answer A is incorrect because DHCP is used to automatically assign IP addresses. Answer B is incorrect because SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. The standard port for SSL is port 443. Answer C is incorrect because in FTP, the data is not protected.

D. SCP runs on port 22 and protects the authenticity and confidentiality of the data in transit. Answer A is incorrect because DHCP is used to automatically assign IP addresses. Answer B is incorrect because SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. The standard port for SSL is port 443. Answer C is incorrect because in FTP, the data is not protected.

B. Traceroute uses an ICMP echo request packet to find the path between two addresses. Answer A is incorrect because SNMP is an application layer protocol whose purpose is to collect statistics from TCP/IP devices. SNMP is used for monitoring the health of network equipment, computer equipment, and devices such as uninterruptible power supplies (UPSs). Answer C is incorrect because SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. Answer D is incorrect because Internet Protocol Security (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications.

B. Traceroute uses an ICMP echo request packet to find the path between two addresses. Answer A is incorrect because SNMP is an application layer protocol whose purpose is to collect statistics from TCP/IP devices. SNMP is used for monitoring the health of network equipment, computer equipment, and devices such as uninterruptible power supplies (UPSs). Answer C is incorrect because SSL is a public key-based security protocol that is used by Internet services and clients for authentication, message integrity, and confidentiality. Answer D is incorrect because Internet Protocol Security (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications.

C. IPv6 increases the address size from IPv4 32 bits to 128 bits. Answers A, B, and D are incorrect because IPv6 addresses sizes are 128 bit.

C. IPv6 increases the address size from IPv4 32 bits to 128 bits. Answers A, B, and D are incorrect because IPv6 addresses sizes are 128 bit.

6. A connection using the HTTP protocol over SSL (HTTPS) is made using the RC4 cipher and port 443. Answer A is incorrect because port 21 is used for FTP connections. Answer B is incorrect because port 80 is used for unsecure plaintext HTTP communications. Answer D is incorrect because port 8,250 is not designated to a particular TCP/IP protocol.

6. A connection using the HTTP protocol over SSL (HTTPS) is made using the RC4 cipher and port 443. Answer A is incorrect because port 21 is used for FTP connections. Answer B is incorrect because port 80 is used for unsecure plaintext HTTP communications. Answer D is incorrect because port 8,250 is not designated to a particular TCP/IP protocol.

. There are NetBIOS ports that are required for certain Windows network functions, such as file sharing, which are 137, 138, and 139. Answer A is incorrect because these ports are used for email. Answer B is incorrect because these ports are used for SNMP. Answer D is incorrect because these ports are used for FTP.

. These are NetBIOS ports that are required for certain Windows network functions, such as file sharing, which are 137, 138, and 139. Answer A is incorrect because these ports are used for email. Answer B is incorrect because these ports are used for SNMP. Answer D is incorrect because these ports are used for FTP.

Objective 1.5

Implement Wireless Networks in a Secure Manner

802.11 Wireless standards

TABLE I

THE EVOLUTION OF THE 802.11 STANDARDS

Protocol	Year Introduced	Maximum Data Transfer Speed	Frequency	Highest Order Modulation	Channel Bandwidth	Antenna Configurations
802.11a	1999	54 Mbps	5 GHz	64 QAM	20 MHz	1×1 SISO
802.11b	1999	11 Mbps	2.4 GHz	11 CCK	20 MHz	1×1 SISO
802.11g	2003	54 Mbps	2.4 GHz	64 QAM	20 MHz	1×1 SISO
802.11n	2009	65 to 600 Mbps	2.4 or 5 GHz	64 QAM	20 and 40 MHz	Up to 4×4 MIMO
802.11ac	2012	78 Mbps to 3.2 Gbps	5 GHz	256 QAM	20, 40, 80 and 160 MHz	Up to 8×8 MIMO; MU-MIMO

Wireless Encryption

- Wireless NICs are radio transmitters and receivers
  - Signal can be intercepted and eavesdropped on
- Solution–Encrypt the data
- Now only people with the password can transmit and listen

Wi-Fi Protected Access (WPA)

- Developed by the Wi-Fi Alliance for a short term temporary replacement for WEP
- Uses RC4 stream cipher
  - The only stream cipher
- Uses Temporal Key Integrity Protocol (TKIP)
  - Dynamic keys
  - Every packet gets unique key
- Two different modes
  - WPA-PSK (Personal Shared Key) mode
    - Requires passphrase
  - WPA Enterprise
    - Requires use of certificates with use of radius, TACACS+, Kerberos

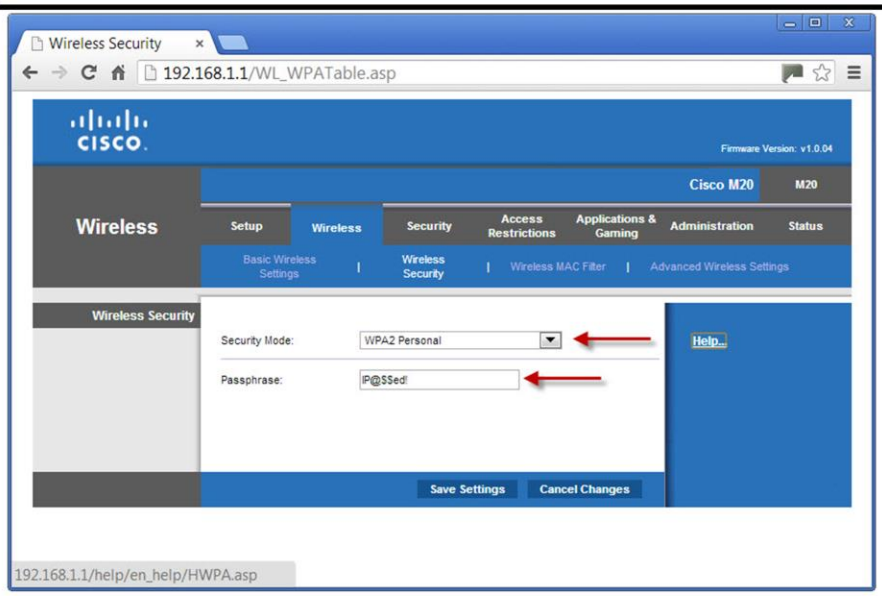
WPA2

- Two versions of WPA2
  - WPA2-Personal
    - Protects unauthorized network access via a password
  - WPA2-Enterprise
    - Verifies network users through a RADIUS, TACACS, or Kerberos server

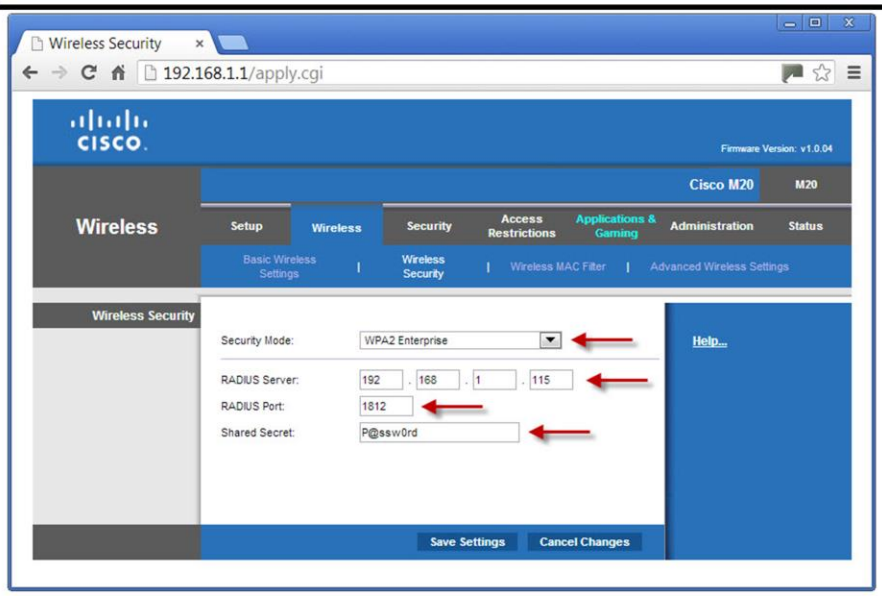
WPA2

- Uses Advanced Encryption Standard (AES) through the use of (CCMP) Chaining Message Authentication Code Protocol Cipher Block
- AES is the encryption cipher
  - Replaced RC4 stream cipher in WPA

WPA2 Personal



WPA2 Enterprise



Wired Equivalent Privacy (WEP)

- The most basic form of encryption that can be used on 802.11-based wireless networks to provide privacy of data sent between a wireless client and its access point
- The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key
- Only uses RC-4
- Do not use WEP

Wireless Authentication:EAP

- **Extensible Authentication Protocol (EAP)**
  - Never Used Alone
    - EAP is an authentication framework, not a specific authentication mechanism
    - It provides some common functions and negotiation of authentication methods called EAP methods
      - EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-IKEv2 are some of the 40 methods
    - EAP methods are used by WPA/WPA2 to authenticate
    - Can be used with smart cards, one-time passwords, and public key encryption (PKI)

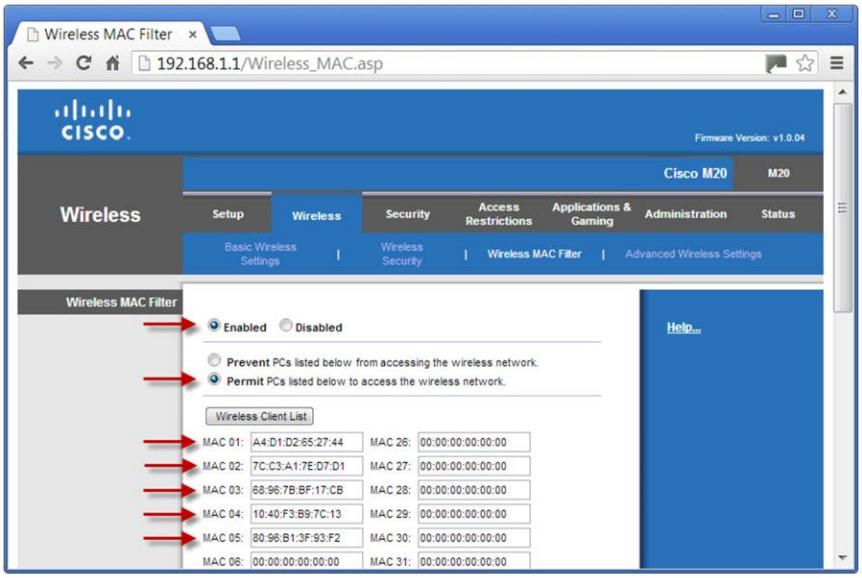
Wireless Authentication

- **Lightweight EAP (LEAP)**
  - Cisco proprietary
  - Uses password only
  - Cisco abandoned this for PEAP
- **Protected EAP (PEAP)**
  - Co-developed by Cisco, Microsoft, and RSA Security
  - Encapsulates EAP methods in a TLS tunnel
  - PEAP supports any type of EAP methods to authenticate the user including certificate

Media Access Control Filter

- MAC filtering is a security access control method whereby the MAC address is used to determine access to the network
- Vulnerable to spoofing attacks

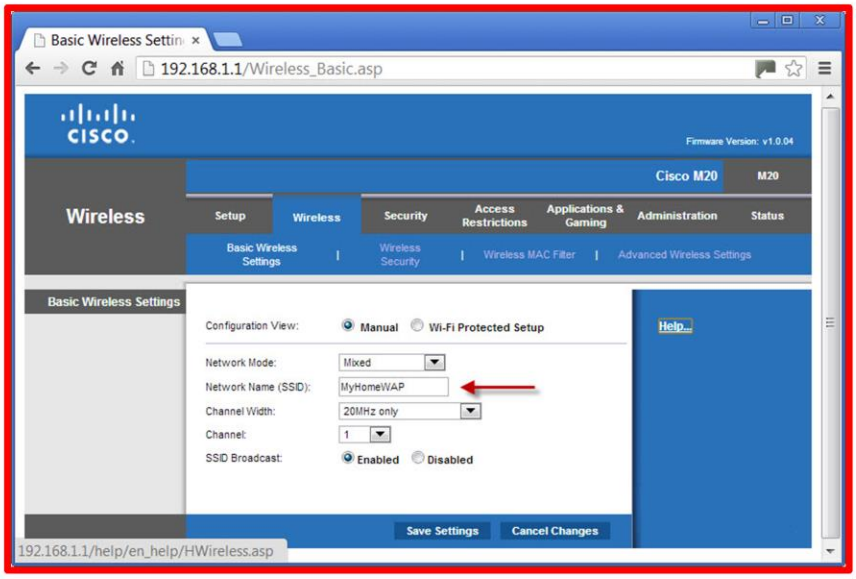
Media Access Control Filter



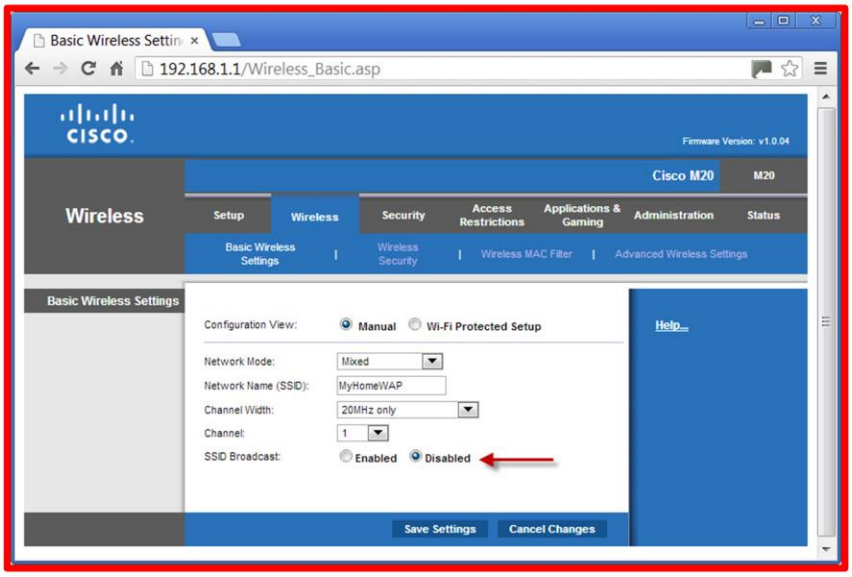
Service Set Identifier (SSID) Management

- SSID is used to identify wireless access points on a network
- Change the default name
- Don’t use a name that points to your organization
- Disable broadcast of SSID

Service Set Identifier (SSID) Management



Service Set Identifier (SSID) Disable



Temporal Key Integrity Protocol (TKIP)

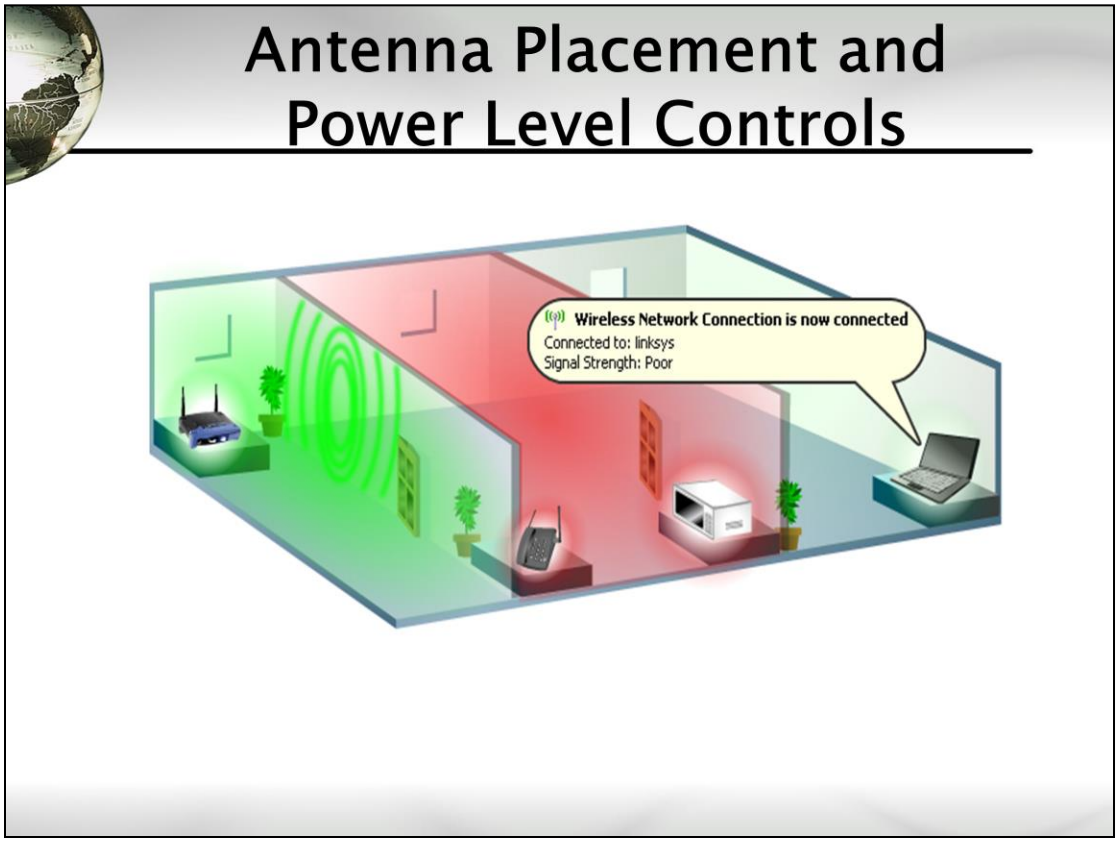
- Designed as the replacement for WEP without requiring replacement of legacy wireless hardware
- TKIP was implemented into 802.11 wireless networking under the name WPA
- TKIP improvements include a key-mixing function that combines the initialization vector with the secret root key before using that key with RC4 to perform encryption
- A sequence counter is used to prevent packet-replay attacks and a strong integrity check named Michael is used

CCMP

- CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality
  - Replaced TKIP in WPA
- Uses 128-bit keys with a 48-bit initialization vector (IV) that reduces vulnerability to replay attacks.
- Used with WPA2

Antenna Placement and Power Level Controls

- Set power level as low as possible
- Consider the channels
- Place antenna to avoid interference



Things that block 2.4 GHz signals

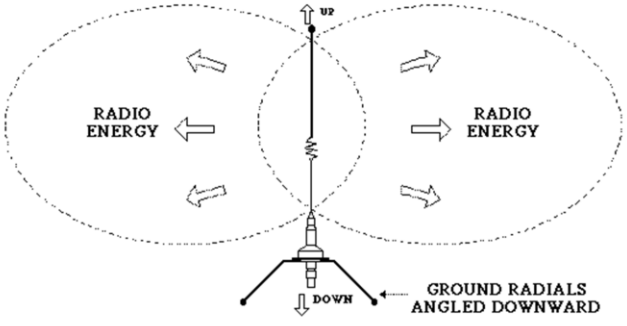
- Microwaves
- Cordless phones
- Baby monitors

Captive Portals

- A captive portal is an authentication technique that redirects a newly connected wireless web client to a portal access-control page
- The portal page may require the user to input payment information, provide logon credentials, or input an access code
- Think hotel wireless logon through web based portal access

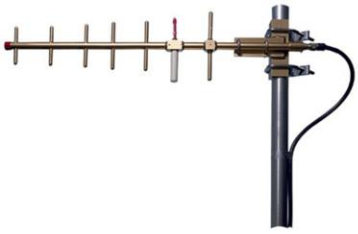
Antenna Types

- A wide variety of antenna types can be used for wireless clients and base stations
- The standard straight or pole antenna is an omnidirectional antenna that can send and receive signals in all directions perpendicular to the line of the antenna itself
- Sometimes also called a base antenna or a rubber duck antenna



Directional Antenna Types

- A Yagi antenna is similar in structure to a traditional roof TV antenna



- Cantennas are constructed from tubes with one sealed end

Directional Antenna Types

- Panel antennas are flat devices that focus from only one side of the panel

- Parabolic antennas are used to focus signals from very long distances or weak sources

Site Surveys

- A site survey is a formal assessment of wireless signal strength, quality, and interference using an RF signal detector

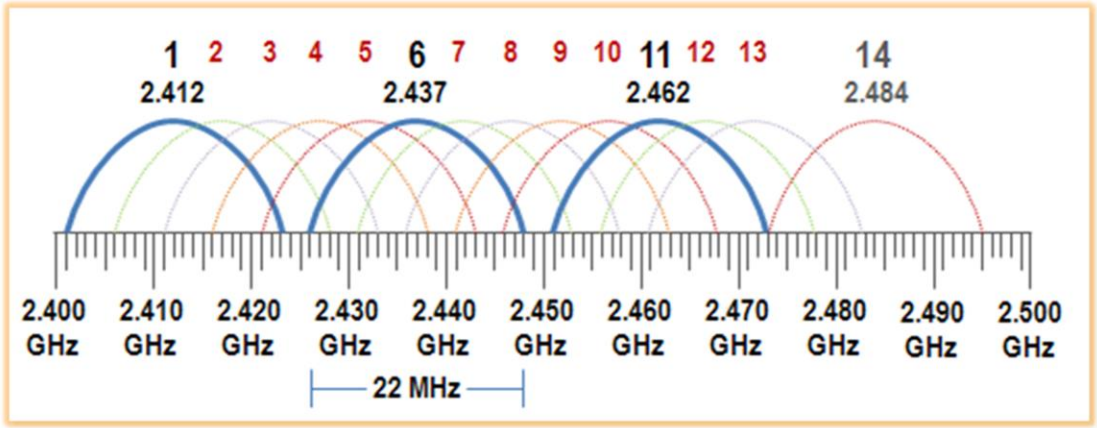
VPN over open wireless

- VPNs can be created over both wired and wireless connections and over both private and public networks (such as the Internet)
- Due to the security risks of wireless networks it's often recommended that you use a VPN to reduce those risks

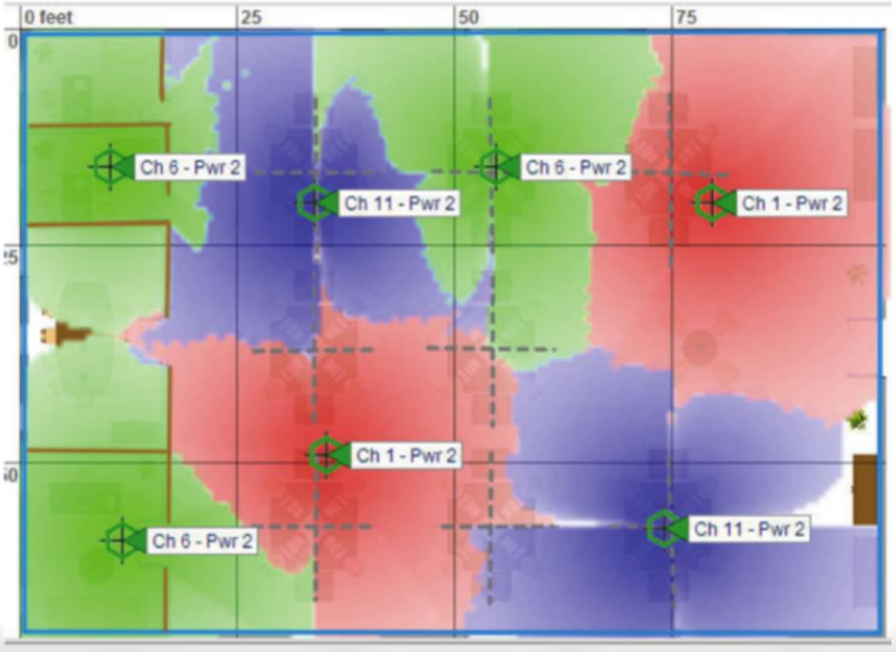
Overlapping WAP Channels

- Set the same SSID on all WAPs
- Overlap Between 10-25%
- Set on different Channels 1, 6, 11
- Alternate Channels so they are not touching each other.

Overlapping WAP Channels



Overlapping WAP Channels



177

A and B. The IEEE specifies 802.1X and EAP as the standard for secure wireless networking, and Protected EAP (PEAP) is standards based. PEAP provides mutual authentication and uses a certificate for server authentication by the client, while users have the convenience of entering password-based credentials.
Answer C is incorrect because LEAP is a Cisco-proprietary protocol.
Answer D is incorrect because WEP is the most basic form of encryption that can be used on 802.11-based wireless networks to provide privacy of data sent between a wireless client and its access point.

A and B. The IEEE specifies 802.1X and EAP as the standard for secure wireless networking, and Protected EAP (PEAP) is standards based. PEAP provides mutual authentication and uses a certificate for server authentication by the client, while users have the convenience of entering password-based credentials.
Answer C is incorrect because LEAP is a Cisco-proprietary protocol.
Answer D is incorrect because WEP is the most basic form of encryption that can be used on 802.11-based wireless networks to provide privacy of data sent between a wireless client and its access point.

D. The WPA2 standard implements the 802.11i protocols and is currently the highest standard for Wi-Fi communication security. Answer A is incorrect because a WAP refers to a wireless access point, which is the wireless network hardware that functions in the place of a wired switch. Answer B is incorrect because the WEP standard was proven to be unsecure and has been replaced by the newer WPA standards. Answer C is incorrect because the early WPA standard has been superseded by the WPA2 standard, implementing the full 802.11i.

D. The WPA2 standard implements the 802.11i protocols and is currently the highest standard for Wi-Fi communication security. Answer A is incorrect because a WAP refers to a wireless access point, which is the wireless network hardware that functions in the place of a wired switch. Answer B is incorrect because the WEP standard was proven to be unsecure and has been replaced by the newer WPA standards. Answer C is incorrect because the early WPA standard has been superseded by the WPA2 standard, implementing the full 802.11i.

C. A rubber duck antenna is an omnidirectional antenna.

C. A rubber duck antenna is an omnidirectional antenna.

B. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is based on the AES encryption scheme.

B. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is based on the AES encryption scheme.