Computer and Network Security

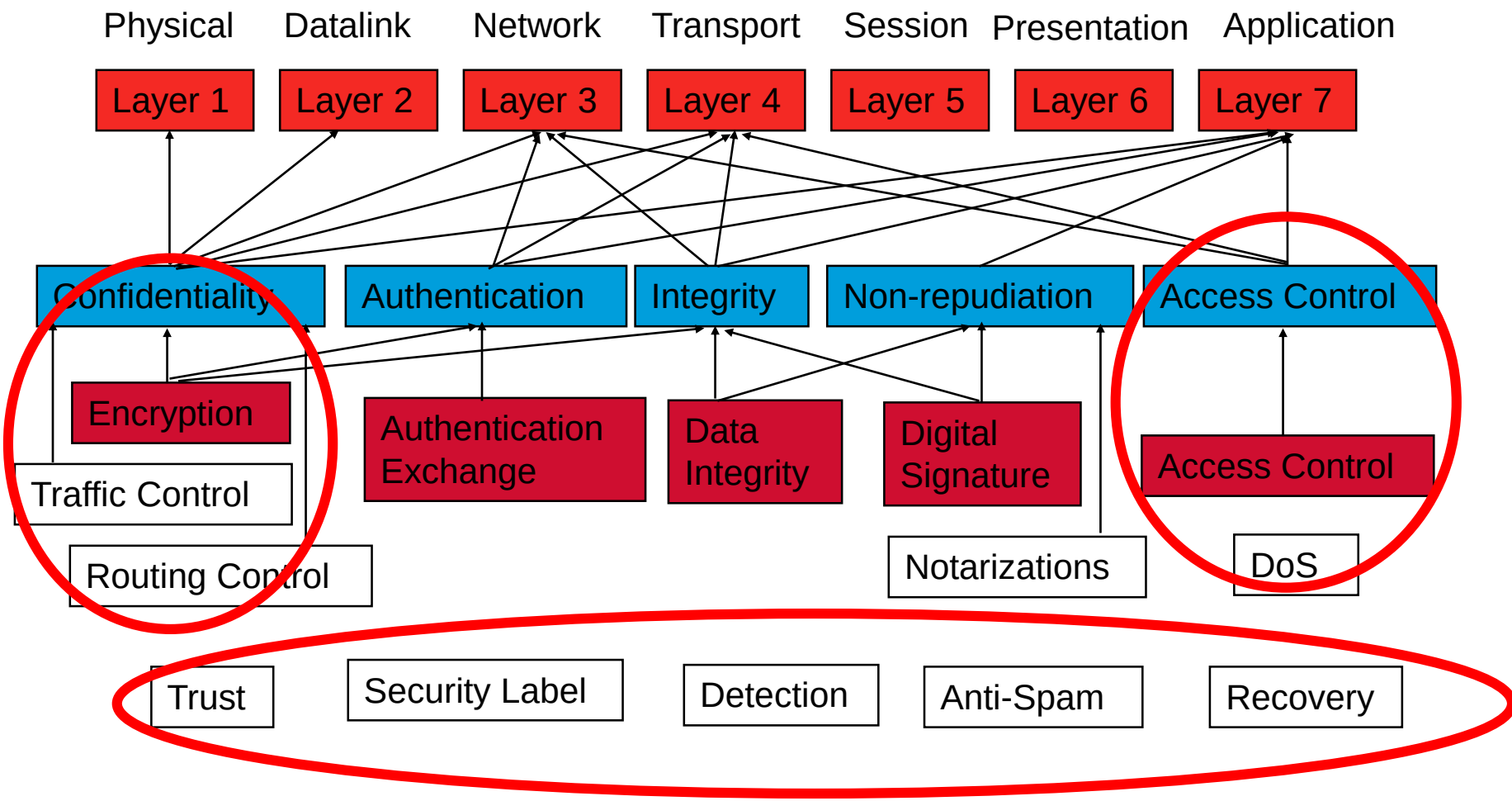
Dr. Chan Yeob Yeun

Week 12

Weekly Lecture Plan

Wk	Contents	Cmt	Wk	Contents	Cmt
1	Introduction		9	Foundations of Network Security II	
2	Foundations of Computer Security	Tutorial Assig Plan	10	Network-Based Threats and Attacks	
3	Identification and Authentication I		11	Network Security Protocols I	
4	Identification and Authentication II	Quiz 1	12	Network Security Protocols II	Quiz 3
5	Access Control		13	Firewalls	
6	Modern Computer Attacks		14	IDS / IPS	Assig Submit
7	Malicious Code	Assig Confirm	15	Revision and Presentation	
8	Foundations of Network Security I	Quiz 2	16	Exam	

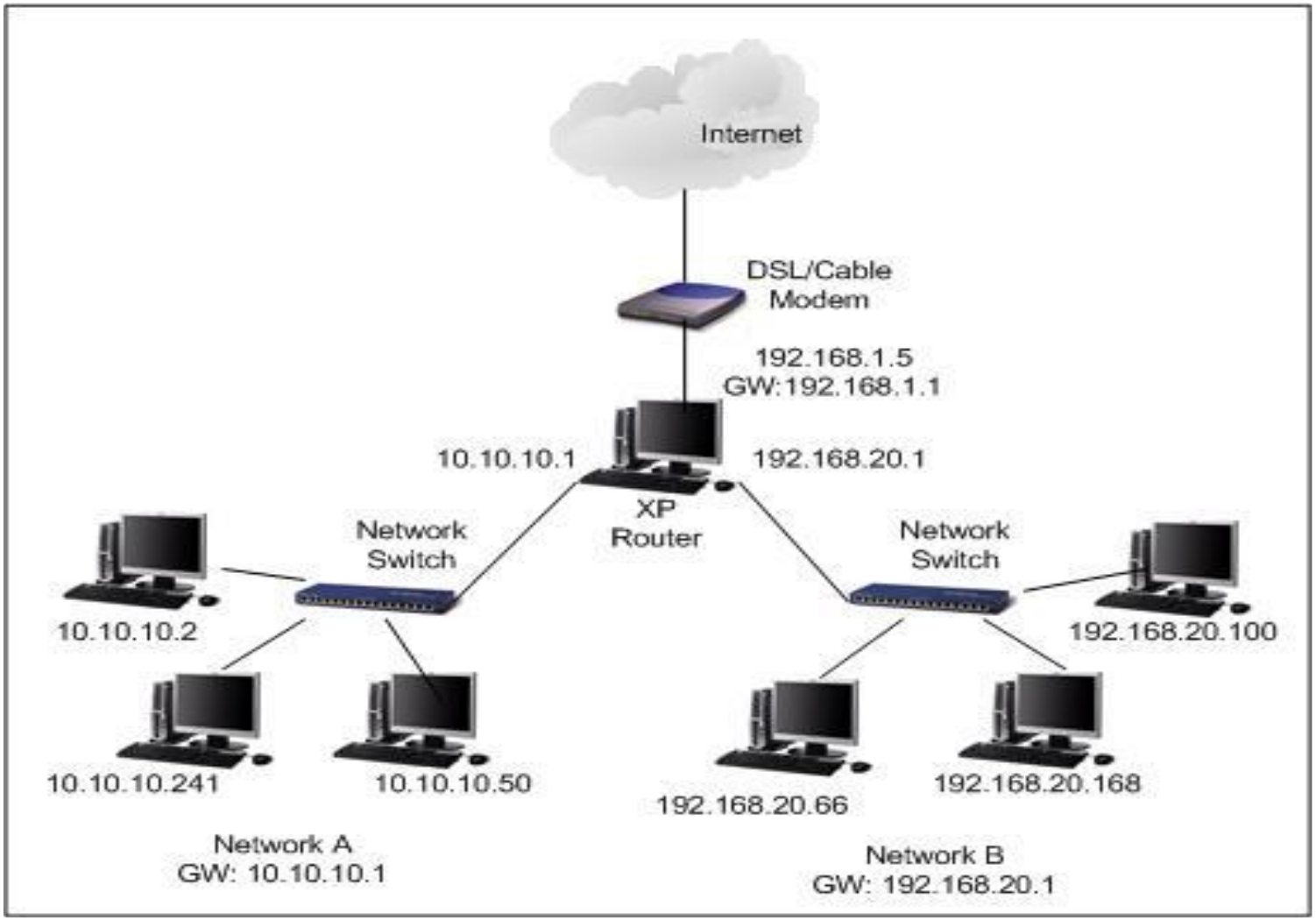
What is Network Security ?



Network Device Security

- Switch and Router Basics
  - Switches
  - Routers
  - Routing Protocols
- Network Hardening
  - Patches
  - Switch Security Practices
  - Access Control Lists
  - Services Not in Use
  - Administration Practices
  - Internet Control Message Protocol (ICMP)
  - Anti-Spoofing and Source Routing
  - Logging

Switch and Router Basics



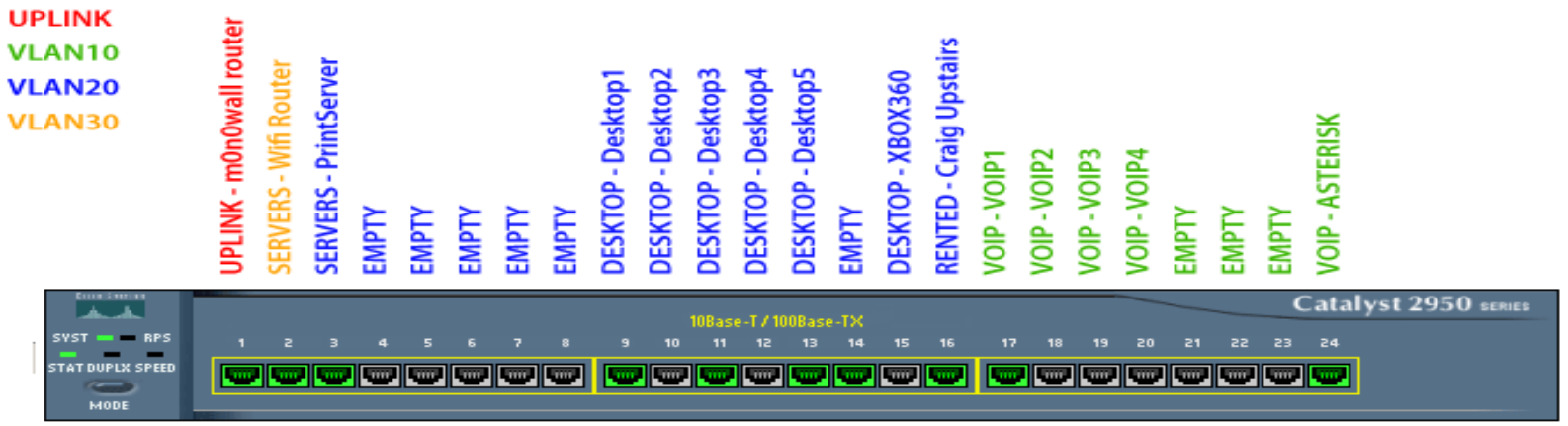
http://www.home-network-help.com/ip-forwarding.html

Switch and Router Basics

Switches and Routers can be thought of as the major interchanges

Switches are the evolving descendents of the network hub

- To overcome the performance shortcomings of hubs, switches were developed. These are intelligent devices that learn the various MAC address of connected devices and will only transmit packets to the devices they were specifically addressed to.
- They provide security benefit by reducing the ability to monitor or “sniff” another workstation’s traffic.
- Thus, with a switch, every workstation will only see its own traffic.



Switches

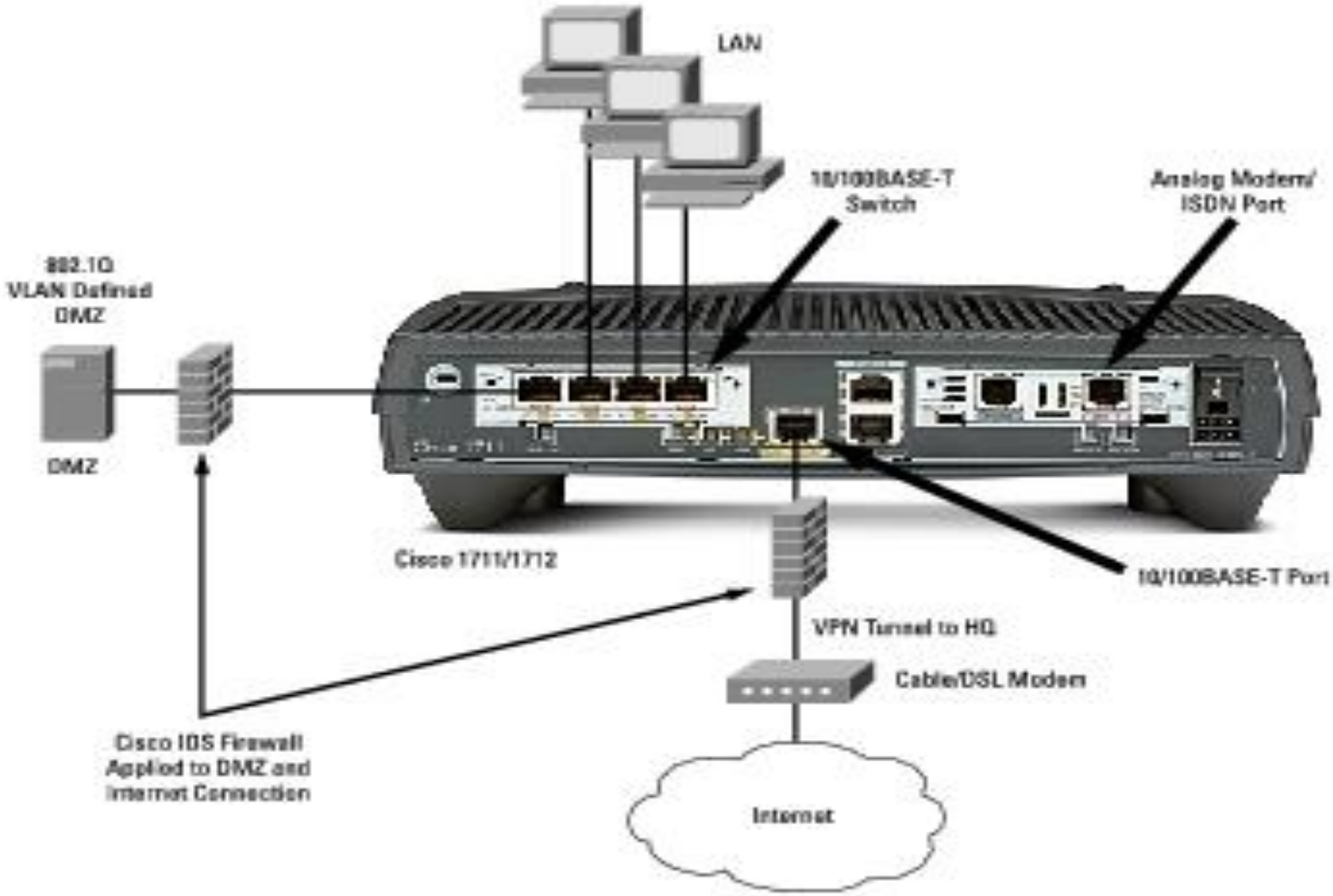
Shortcomings of Switches:

- A switched network cannot totally eliminate the ability to sniff traffic.
- A hacker can trick a local network segment into sending it another workstation's traffic with an attack known as Address Resolution Protocol (ARP) poisoning.
- ARP poisoning works by forging replies to ARP broadcast.
- E.g. Attacker would broadcast an ARP packet onto the network containing Victim's IP address but Attacker's MAC address.

Possible Solution

- In order to overcome ARP poisoning attacks, segregate sensitive hosts between two layer three devices or use virtual LAN (VLAN) functionality on switches. For high sensitive host may wish to statically define important MAC entries such as default gateway

Routers


LAN
10/100BASE-T
Switch
Analog Modem/
ISDN Port
802.1Q
VLAN Defined
DMZ
DMZ
Cisco 1711/1712
10/100BASE-T Port
VPN Tunnel to HQ
Cable/DSL Modem
Cisco IOS Firewall
Applied to DMZ and
Internet Connection
Internet

Routers

Routers operate at layer three, the network layer (IP) of the OSI model.

- Used to move traffic between different networks and between different section of the same network
- Have ability to perform IP packet filtering
- Learn the locations of various networks in two ways
  - Via routing protocol
  - Via manually via static routes
  - Networks use a combination of the two to get reliable connectivity between all necessary networks
- Static routes are needed
  - e.g. firewalls do not normally run routing protocols
  - If a firewall is not informing the network of any networks behind it, those routes must be statically added to a network router and propagated.

Routing Protocols

Two types of routing protocols:

- Distance-vector protocols: more simplistic and better suited for smaller networks and maintain tables of distances to other network.
- Link-state protocols: develop to address the specific needs of larger networks and use link-speed metrics to determine the best route to another network.

Choosing a routing protocol, one should check:

- Network size
- Firewall is not vulnerable to a routing protocol attack

Network Hardening

In order to securely configure the device, one needs

- Patches: updated released by the product vendor in timely manner
- Switch security practices: MAC addresses are unique for every network interface card, and switches can be configured to allow only specific MAC address to send traffic via a specific port on the switch, known as “port security”
- Access control lists (ACLs): Permit or deny TCP and UDP traffic on the source or destination address, or both, as well as on the TCP or UDP port numbers contained in a packet.
    - Router ACLs can increase network security by using border routers to drop unwanted traffic, removing the burden from the border firewalls.

Network Hardening

Administrative Practices

- Simple Network Management Protocol (SNMP): SNMP can be used to monitor such things as link operation and CPU load
- The Simple Network Management Protocol
    1. Protocol operations
    2. Transport mappings
    3. Security and administration
- First defined in RFC 1157 (SNMPv1)
- Separate documents beginning in SNMPv2
- Security and administration completed in SNMPv3
- SNMP can manage devices that can alert personnel to detect problems by sending *traps* to configured consoles

Network Hardening

Administrative Practices

- Simple Network Management Protocol (SNMPv3):
  - Security
    - authentication
    - Privacy
  - Administration
    - Authorization and view-based access control
    - Logical contexts
    - Naming of entities, identities, and information
    - People and policies
    - Usernames and key management
    - Notification destinations and proxy relationships
    - Remotely configurable via SNMP operations

Network Hardening

Administrative Practices

- Threats protected against by SNMPv3:
  - Masquerade/data origin authentication: interloper assumes the identity of a sender to gain its privileges
  - Modification of information/data integrity: alteration of in-transit messages
  - Message stream modification: messages are re-ordered, delayed, or replayed
  - Disclosure/data confidentiality: privileged information is obtained via eavesdropping on messages

Network Hardening

Administrative Practices

- SNMPv3 uses MD5 and DES as “symmetric,” i.e., secret key mechanisms:
  - (MD5 = Message Digest Algorithm 5, RFC 1321)
  - (DES = Data Encryption Standard)
- User Based Authentication Mechanims:MD5 message digest algorithm in HMAC
  - indirectly provides data origin authentication
  - directly defends against data modification attacks
  - uses private key known by both sender and receiver
  - 16 byte key
  - 128 bit digest (truncated to 96 bits)
- SHA an optional alternative algorithm
- Loosely synchronized monotonically increasing time indicator values
  - defends against certain message stream modification attacks

Network Hardening

Administrative Practices

– User Based Privacy Mechanism on:

1. Symmetric encryption used Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode
    - provides privacy / protection against disclosure
    - uses encryption
    - subject to export and use restrictions in many jurisdictions
2. 16 byte key (8 bytes DES key, 8 byte DES initialization vector)
3. Multiple levels of compliance with respect to DES due to problems associated with international use

Network Hardening

Internet Control Message Protocol

- ICMP provides a mechanism for reporting TCP/IP communication problems, as well as utilities for testing IP layer connectivity
- ICMP is defined by RFC792, which details many different types of ICMP communications, commonly know as messages.

Summary

- Routers and switches provide a number of mechanisms to enhance the overall security and performance of local network
- Switches reduce the risks of sniffing-based attacks against other local workstation, and they can further reduce risks via the strategic implementation of VLANs
- Routers provide the ability to implement ACLs to screen and drop unwanted traffic. Also, taking the time to harden the router against attacks will also increase the security of the network
- SNMPv3 provides security and administrations for protecting against masquerading, modifications, data confidentiality and entity authentication
- Proactive control of ICMP can prevent an attacker form learning significant information about network topologies

Introduction to Secure Network Design

All information systems create risks to an organization.

The goal of secure network design is to enable authorized communications while mitigating information risk to acceptable levels:

1. Acceptable Risk
2. Designing Security into a Network
    - **Network Design Models**
3. Designing an Appropriate Network
4. The Cost of Security

Introduction to Secure Network Design

Acceptable Risk

- Security Policy
  - This makes an Information Security Officer job easier and your network more secure
  - Definition: A formal statement of the rules by which people who are given access to an organization's technology and information assets must abide
  - Acts as a road map to guide in the design and operation of the security within your network
  - The design and configuration of the infrastructure becomes the enforcement of those documents.
  - Can measure the security of the network against conformance to the policy
- Guidelines – an organization's best practices
- Standards – the minimum set of operations criteria for a certain technology or asset

Introduction to Secure Network Design

Designing Security into a Network

- Security is easily overlooked aspects of network design, and try to fit existing network can be expensive and difficult to implement properly
- For example, firewalls, IDS, to secure and monitor multiple application systems.

Designing Security into a Network

- Network design Models:
  - Networks built with many connections to other networks will be harder to secure due to the number of access control mechanisms
  - Not all screening is explicit such as shopping mall, airport, federal prisons
  - Different security requirements for low and high risk groups
  - All the above mentioned elements can be translated into network design such as firewall, access control systems, monitoring and controlling traffic movements and detect unauthorized activities.

Introduction to Secure Network Design

Designing an Appropriate Network

- Number of requirements and expectations for a network
- Organization availability, performance requirements
- Protecting sensitive network assets
- Setting up efficient and secure links to other networks
- Ability to provide levels of security with any risks associated with the assets on that network

Introduction to Secure Network Design

Designing an Appropriate Network

- Design and maintain a network
- Understanding of what are required by network architects, engineers and users
- It is vital to understand your network needs with regards to performance, security and controls.

The Cost of Security

- Determine the organization's costs for each security breach.
- This helps management to determine the value to the organization of the various security control mechanisms.
- Consider an expected loss so determine appropriate spending levels

Performance

The network will play a huge rule in meeting the performance requirements:

- Determine the appropriate network technology to meet the bandwidth requirements projected for two or three years in the future.
- Also consider implementing QoS for providing appropriate bandwidth and giving priority applications.
- Filtering, compressing, encrypting and address-translating operations should be performed at the access and distribution layers.
- The network is highly segmented, a single network failure at the access or distribution layers does not affect the entire network.

Availability

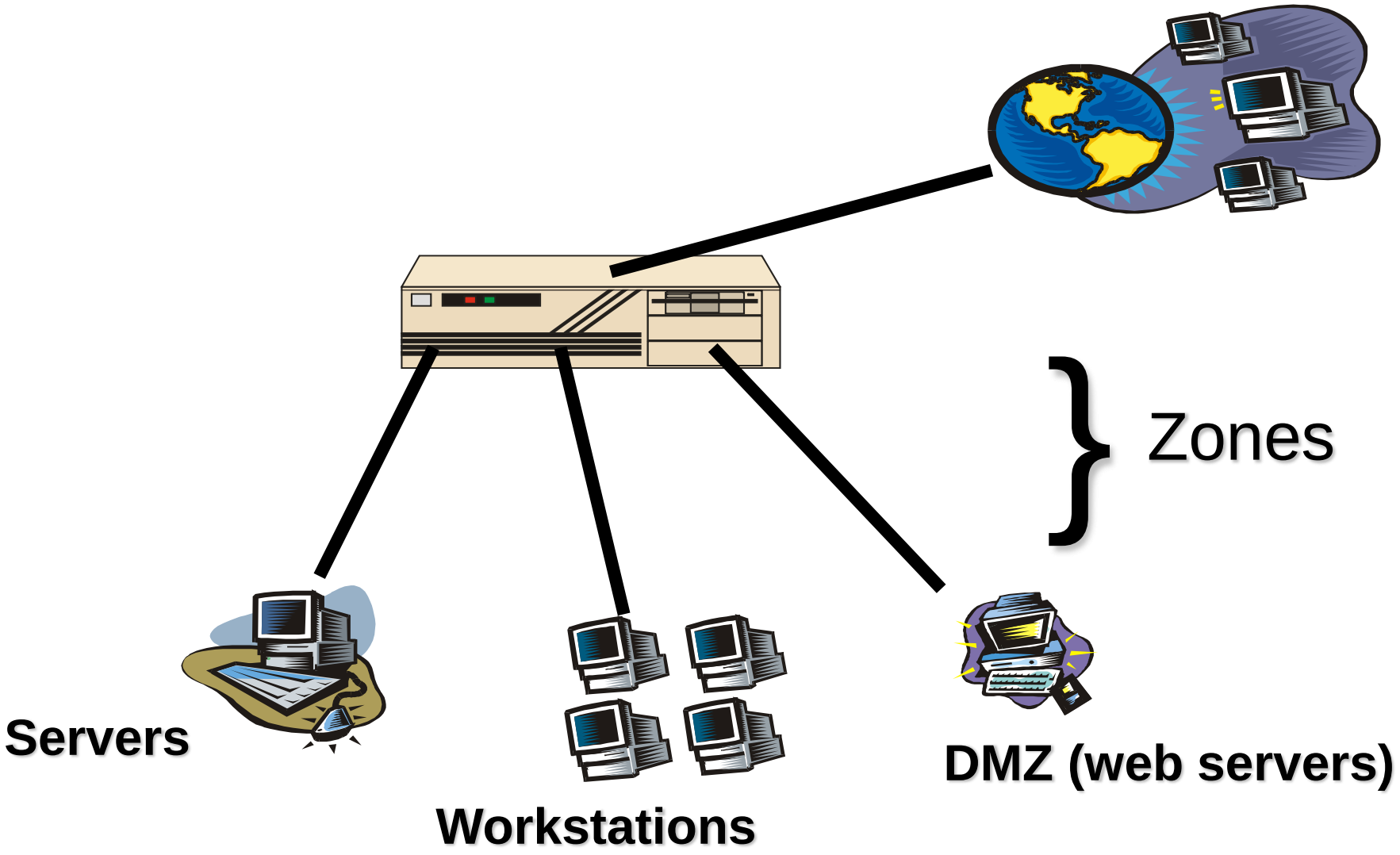
Network availability requires that systems are resilient and available to users on a timely basis.

- DoS: Unavailable systems cost organizations real dollars in lost revenue
- Avoid single points of failure within the architecture

Solutions: Implementing a redundant firewall or router solution is to achieving a full high-availability network architecture.

- Good availability design will incorporate redundant hardware components at the switch, network, firewall, and application levels
- Also consider maintaining multiple internet links to different service providers to insulate an organization from problems at any one provider

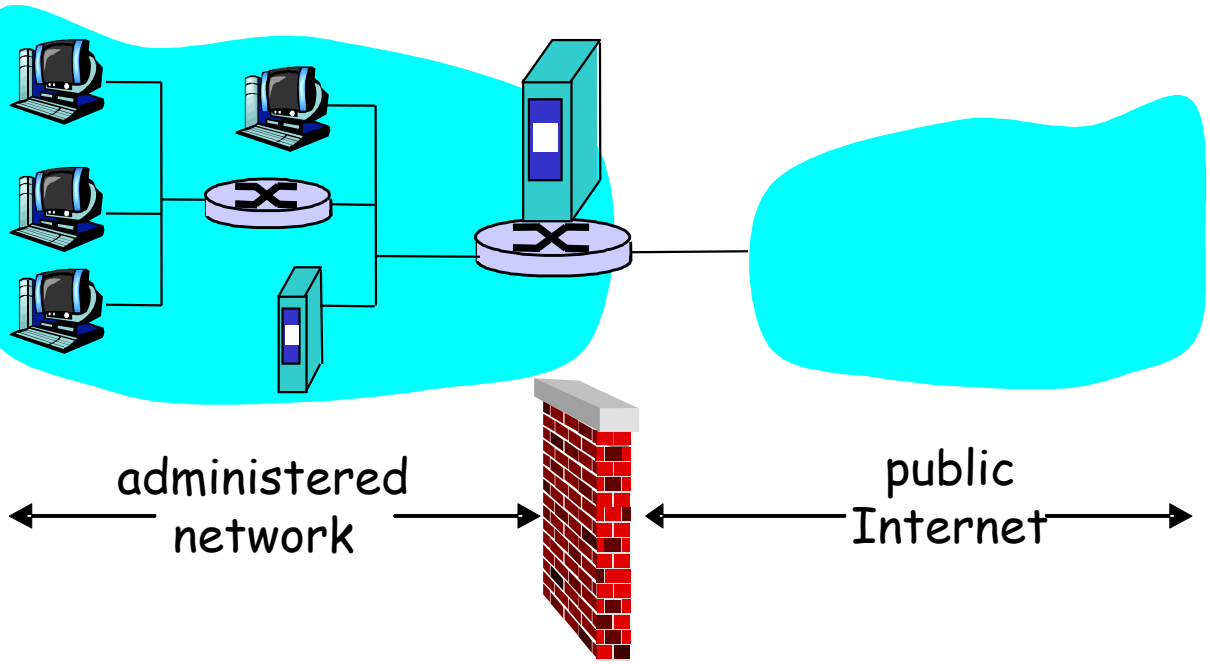
Security



Security

A firewall is a machine that monitors all traffic to and from a site

This allows for monitoring, filtering, logging, and proper access to the network



Security

Designing and implementing security in network and system architectures, it is helpful to identify critical security control and understand the consequences of a failure in those controls.

Securing individual nodes on the network, it is important to secure the network as a whole.

Perimeter security is only as strong as its weakest link.

Good practices for reducing risks include periodic auditing of the external networks and implement firewalls to permit only those communications required to conduct business.

Security

Wireless Impact on the Perimeter

Remote Access Considerations

Internal Security Practices

Intranets, Extranets and DMZs

Host Hardening

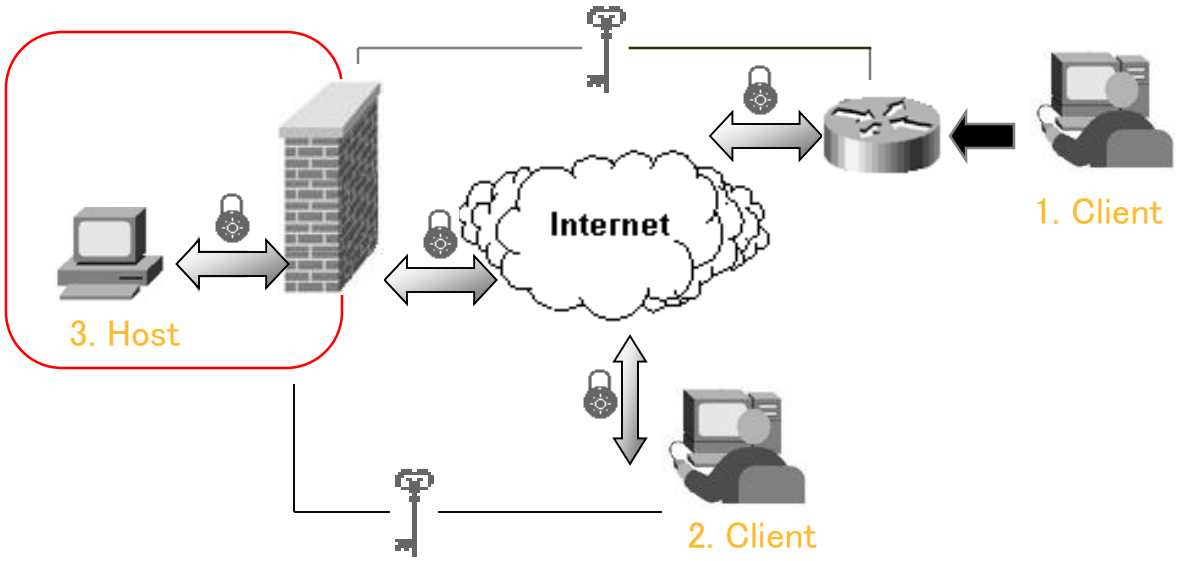
Outbound Filtering

Remote Access Considerations

- Most organization networks allow user access to internal resource from remote locations.
- Remote access is now generally provided via a Virtual Private Network (VPN)
- Risk: Attackers may gain access to an unprotected PC, the VPN could be used to tunnel traffic past the organization firewalls and the protection they provided.
- Solution: Security administrators should ensure that adequate protection is implemented over the endpoints.
    - E.g. a host can only communicate inside the VPN, thus preventing a remote user from using it as a conduit.

Security

VPN via Firewall



1. *Firewalls and Routers* share an encryption key.
2. *Client and Firewall* share an encryption key.
3. *Firewall and Host* share an encryption key.

Security

Internal Security Practices

- Organizations deploy firewalls strictly around the perimeter of their network leave themselves vulnerable to internally initiated attacks such as logic bombs, Trojan horse and virus.

Intranets, Extranet and DMZs

- Intranets: To provide internal users with access to applications and information securely.
- Extranets: These are company-controlled application networks that are made available to trusted external parties.
- DMZs: An organization may want to provide public Internet access to certain systems.
    - E.g. a company to receive Internet e-mail, the e-mail server must be made available to the Internet.

Security

Host Hardening

- The practice of disabling unnecessary services and reconfiguring other services for greater security is often referred to as host hardening.

Outbound Filtering

- Failure to restrict outbound access creates a number of risks. E.g. failure to filter traffic leaving the organization network may allow an attacker to use the network to launch attacks on other networks
- Web Access Considerations: organizations could configure their infrastructure to permit access to specific categories of web sites while denying access to others such as pornography, games and music sites.

Security

Outbound Filtering

- Outbound Port Filtering: It will prevent users from using applications that are dangerous or are not business related in the corporate environment.
- Instant Messaging: IM allows users to “chat” with other users connected to the IM system
  - Pros: Valuable business tool for audio and video conferencing and usage reporting. Thus, save money and travel costs.
  - Cons: IM clients do not provide any sort of transport encryption, leaving such communications open to passive monitoring and eavesdropping.
  - Solutions: encrypting IM for audio and video conferencing

Summary

The goal of network security is to enable authorized communications while mitigating information risk to acceptable level.

The network will play a huge rule in meeting the performance requirements such as implementing QoS, filtering and encrypting.

Network availability requires that systems are resilient and available to users on a timely basis.

Designing and implementing security in network and system architectures, it is helpful to identify critical security control and understand the consequences of a failure in those controls.