CWSP Guide to Wireless Security

Designing a Secure Wireless Network

Objectives

- Describe the basic principles of security design
- Define network segmentation and tell how it can be used for WLANs
- List ways in which wireless hardware can be located securely
- Describe the steps that can be taken to protect wireless devices

Basic Principles of Security Design

- Five key security principles
  - Layering
  - Limiting
  - Diversity
  - Obscurity
  - Simplicity

Layering

- Wireless security should be created in layers
  - Making it unlikely that an attacker possesses the tools and skills to break through all the layers of defenses
- Layers include:
  - Strong door locks
  - Antivirus software
  - Strong passwords
- Problem with layered approach
  - All the layers must be properly coordinated to provide a cohesive security perimeter

Limiting

- Limiting access to information reduces the threat against it
- Only those who must use data should have access
- The amount of access granted to someone should be limited to what that person needs to know
- Limiting is more than placing a password on a system
- Users should have the least amount of information necessary to do their jobs, and no more

Diversity

- Layers must be different (diverse)
  - If a thief penetrates one layer, he cannot use the same techniques to break through all other layers
- Using diverse layers of defense means:
  - Breaching one wireless security layer does not compromise the entire system
- Diversity in the transitional security model involves:
  - Implementing both MAC address filtering and DHCP restrictions

Obscurity

- Security by obscurity
  - Obscuring what goes on inside a system or organization and avoiding clear patterns of behavior
  - Makes attacks from the outside much more difficult
- Wireless information security
  - Important not to advertise what security is in place
  - Do not use predictable passwords
- Security by obscurity is sometimes criticized as being too weak if used as the only technique

Simplicity

- Information security is, by its very nature, complex
- Complex security systems
  - Can be hard to understand, hard to troubleshoot, and hard to feel secure about
- Secure system should be simple enough for those on the inside to understand and use
- Challenge is to make the system simple from the inside but complex from the outside
  - Will reap a large benefit in information security

Simplicity (continued)

Table 7-1 Basic security principles

Principle	Description	Example
Layering	Multiple layers of defenses that surround the information	Using antivirus software, strong passwords, and strong door locks
Limiting	Restrict access to information	Limit access to management features of access points
Diversity	Different types of defenses	Use MAC address filtering and DHCP restrictions in the transitional security model
Obscurity	Hide anything that could be useful to attacker	Use a cryptic SSID
Simplicity	Security system must not be confusing to inside security personnel but only to attackers	Use multiple firewalls

Network Segmentation

- Segmentation divides the network into smaller units
- Network segment is a subset of a larger network
- Reduces the amount of traffic on a network
- Non-deterministic networking: Devices share same media and send packet any time
- Segmentation reduces Collision Errors: two packets are sent at the same time
- Collision domain is
  - Area that encompasses all of the network devices that can cause collisions

Network Segmentation (continued)

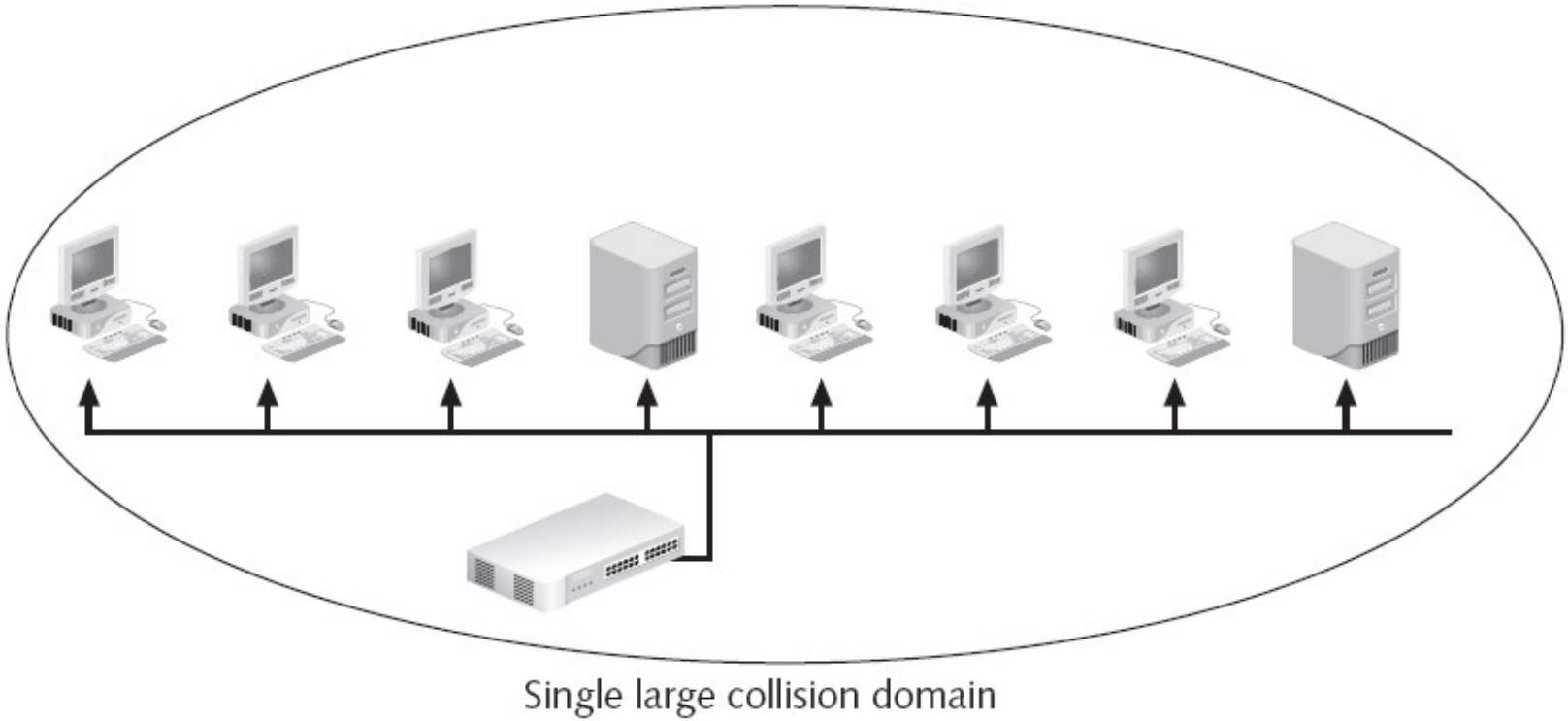


Figure 7-1 Collision domain

Network Segmentation (continued)

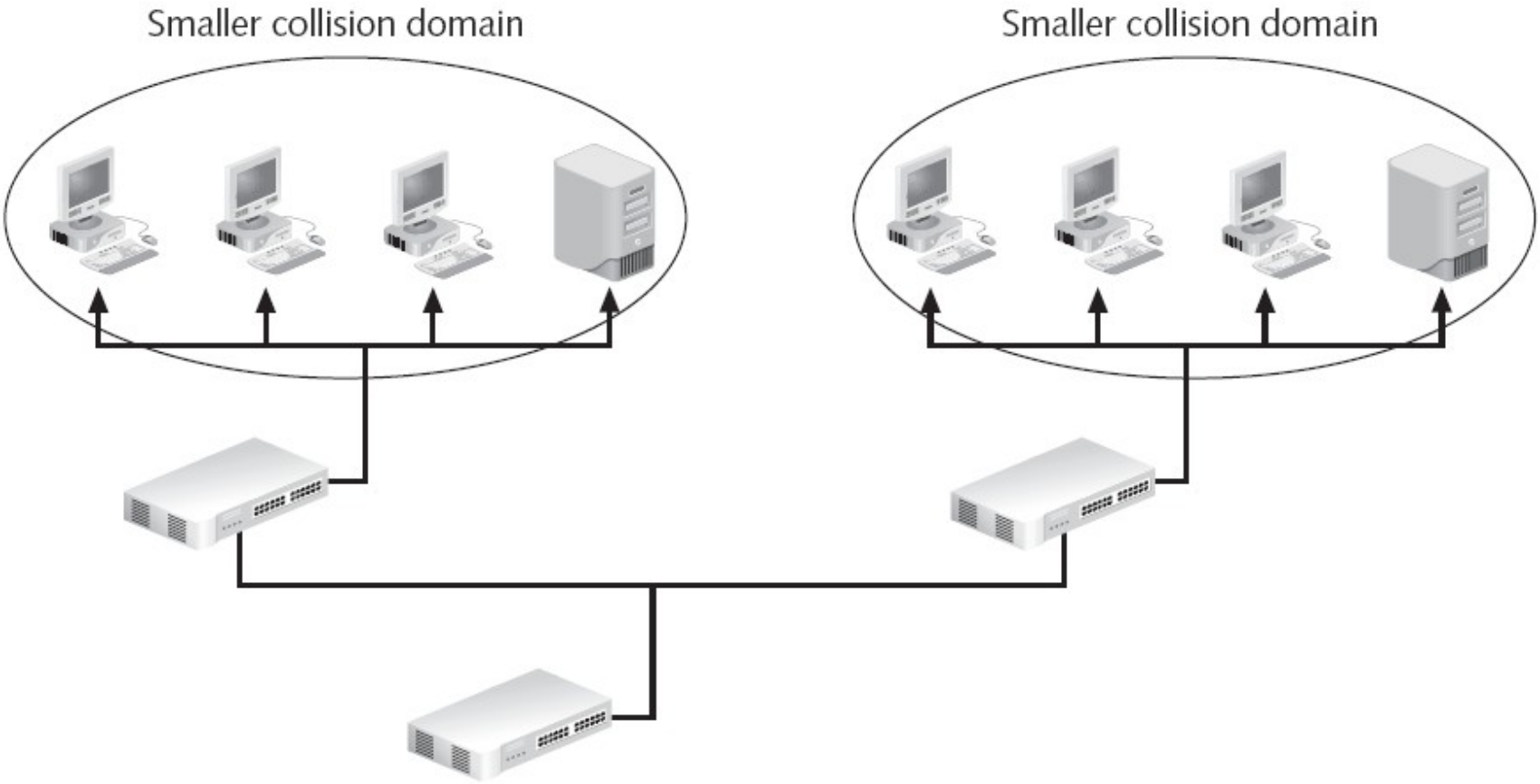


Figure 7-2 Segmentation limits collision domains

Network Segmentation (continued)

- Network segment and a subnet are different
  - Segment is created by connecting equipment to a physical device
  - Subnets are usually created by grouping together computers by Internet protocol (IP) addresses
- Wireless segmentation can be accomplished through adding access points
  - Devices serviced by separate APs are not strictly sharing the same media
- Segmentation creates smaller segments for security

Network Segmentation (continued)

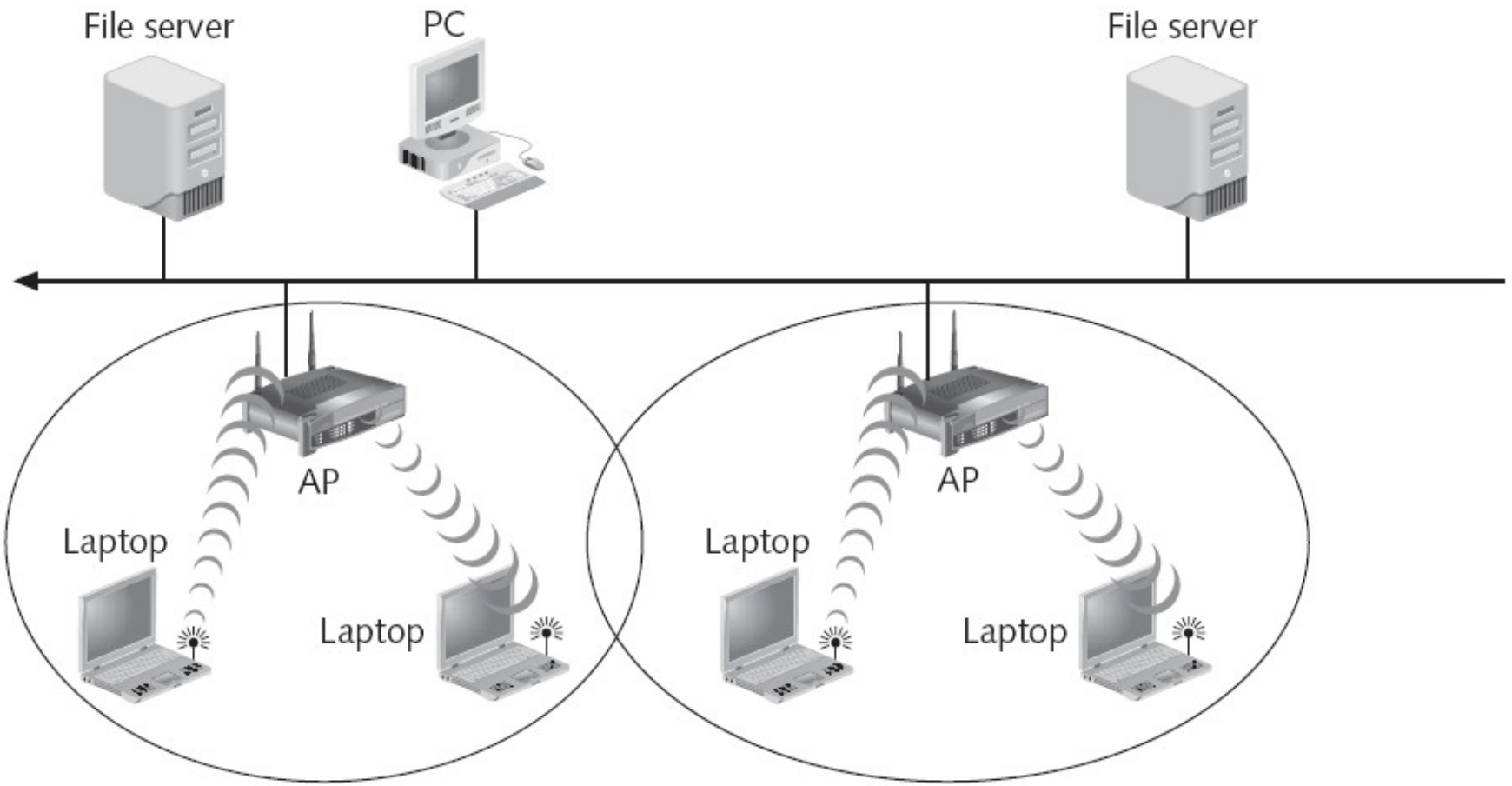


Figure 7-3 Segmentation by adding access points

Segmenting with Devices and Technologies

- Segments can be created using bridges, switches, and routers
- In wireless network, segments are created using:
  - Wireless gateways
  - Wireless routers
  - Wireless switches
  - Firewalls
  - Demilitarized zones
  - Network address translation

Segmenting with Devices and Technologies (continued)

- Firewall
  - Sometimes called a packet filter
  - Designed to prevent malicious packets from entering the network or computer
  - Can be software based or hardware based
  - The foundation of a firewall is a rule base
    - Establishes what action the firewall should take when it receives a packet: allow, block, or prompt
  - Stateless packet filtering
    - Looks at the incoming packet and permits or denies it based strictly on the rule base

Segmenting with Devices and Technologies (continued)

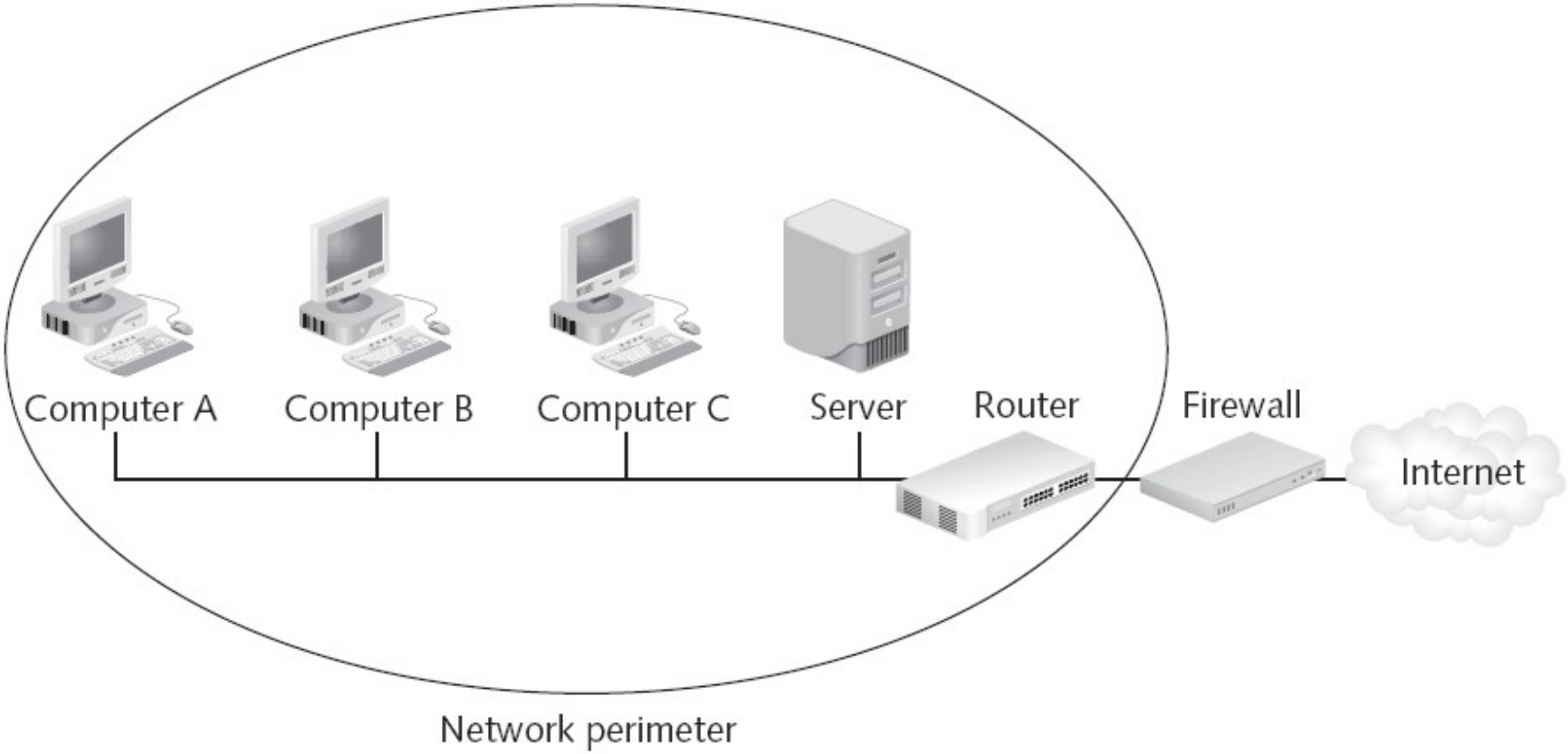


Figure 7-4 Hardware firewall position in network

Segmenting with Devices and Technologies (continued)

Table 7-2 Stateless packet filtering rule

Rule Description	Explanation	Filtering
Source address = any	The source IP address is that of the Web server on the Internet.	Because you cannot know in advance what the IP address of a Web server is, this rule allows a packet coming from anywhere to enter the network.
Destination address = internal IP address	The destination address is the IP address of the computer on the internal network where the packet is being sent.	This rule allows packets directed to this internal computer to pass through but it blocks packets that do not have the correct destination address.
Port = 80	The port indicates what this packet contains, namely an HTML document.	No other types of content besides HTML documents are allowed.

Segmenting with Devices and Technologies (continued)

- Firewall (continued)
  - Stateful packet filtering
    - Keeps a record of the state of a connection between an internal computer and an external server
  - Firewalls are a critical tool for protecting a wireless network from attacks
  - Many security experts maintain that wireless APs should be treated as “unsecure”
    - And placed outside of the firewall

Segmenting with Devices and Technologies (continued)

Table 7-3 Stateful packet filtering rule

Rule or State Description	Explanation	Filtering
Source address = any	The source IP address is that of the Web server on the Internet	Because you cannot know in advance what the IP address of a Web server is, this rule allows a packet coming from anywhere to enter the network.
Destination address = internal IP address	The destination address is the IP address of the computer on the internal network where the packet is being sent.	This rule allows packets directed to this internal computer to pass through but it blocks packets that do not have the correct destination address
Destination address = internal IP address	Did this computer on the internal network request this information from the Web server?	This state observation prevents those packets from entering that were not first requested by an internal computer.
Port = 80	The port indicates what this packet contains, namely an HTML document.	No other types of content besides HTML documents are allowed.

Segmenting with Devices and Technologies (continued)

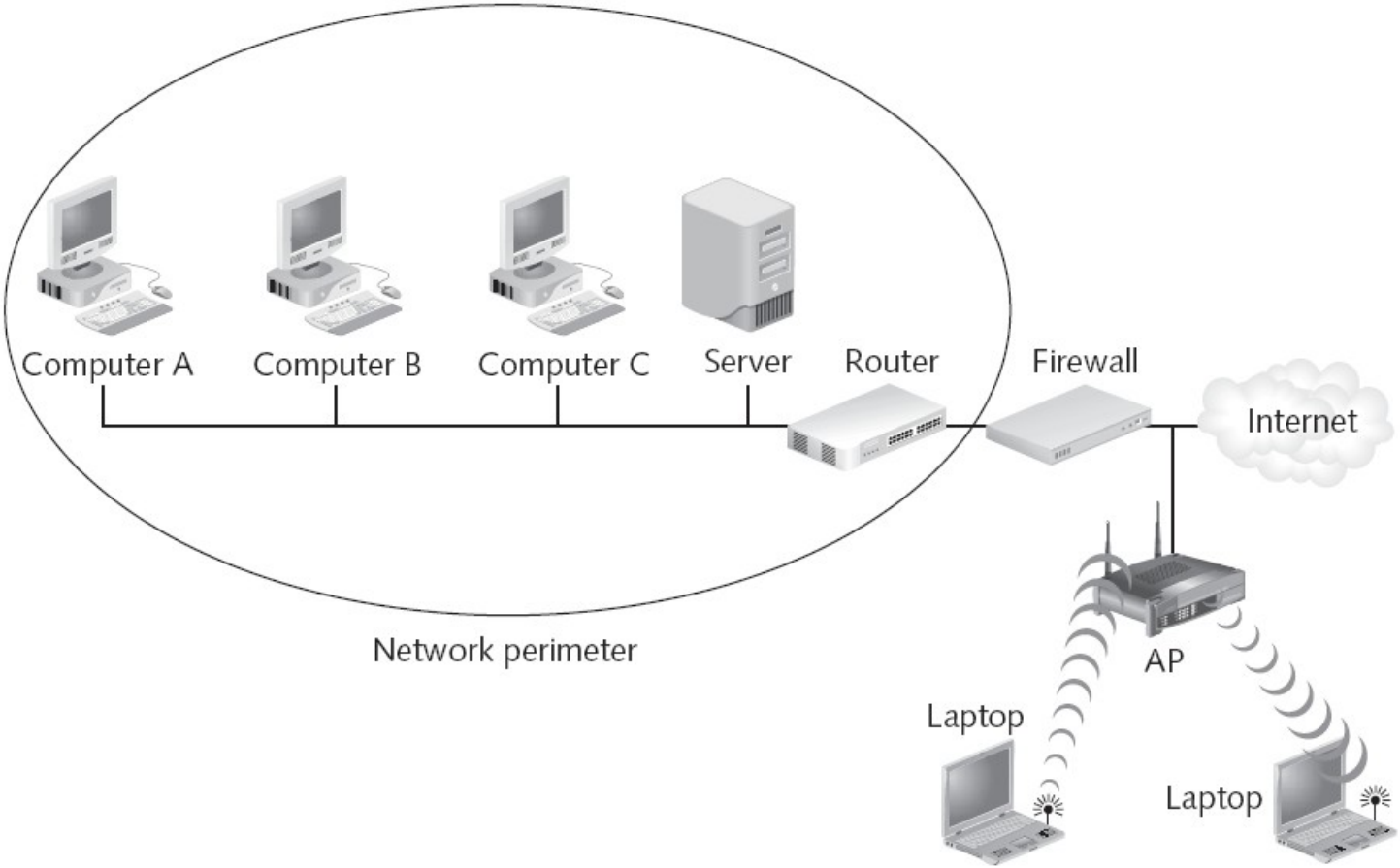


Figure 7-5 Access point outside firewall

Segmenting with Devices and Technologies (continued)

- Demilitarized zone (DMZ)
  - Separate network that sits outside the secure network perimeter and is protected by a firewall
  - Outside users can access the DMZ but cannot enter the secure network
  - May not be practical for a SOHO network

Segmenting with Devices and Technologies (continued)

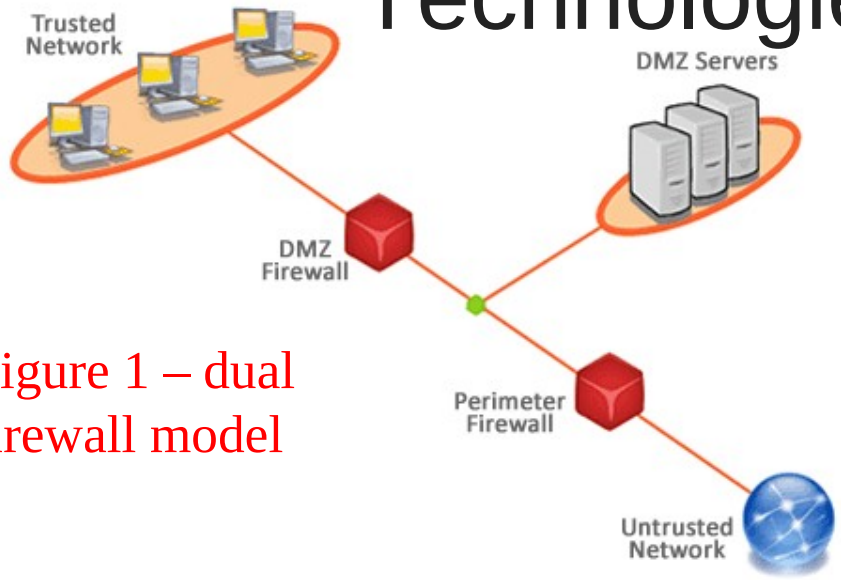


Figure 1 – dual firewall model

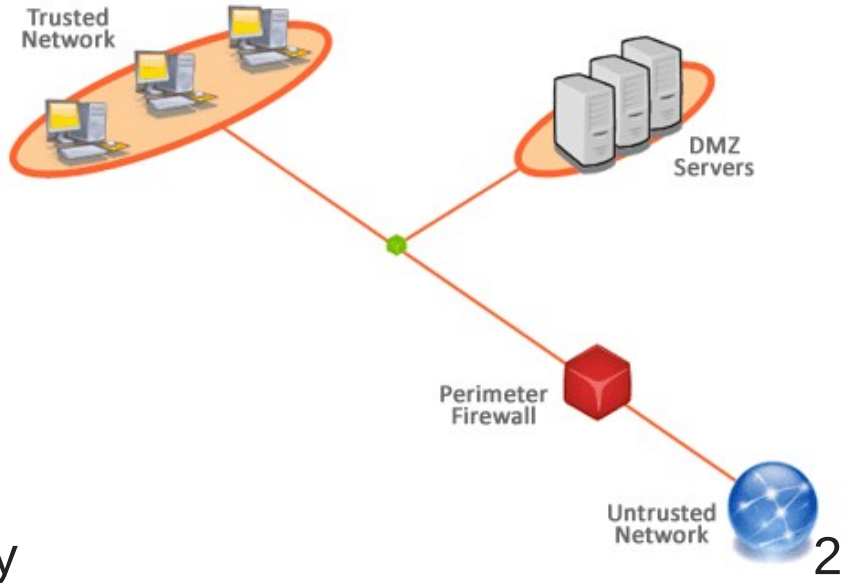


Figure 2 – single firewall model

Segmenting with Devices and Technologies (continued)



Figure 7-7 Setting up a DMZ

Segmenting with Devices and Technologies (continued)

- NAT Replaces the sender's actual IP address with another IP address ; - Private addresses used only on private internal network
  - When using NAT, a private address is assigned to a network device
    - And replaced with a real address when a packet leaves the network
  - Port address translation (PAT)
    - Each packet is given the same IP address but a different port number
    - A single IP address is to be shared by several users

Segmenting with Devices and Technologies (continued)

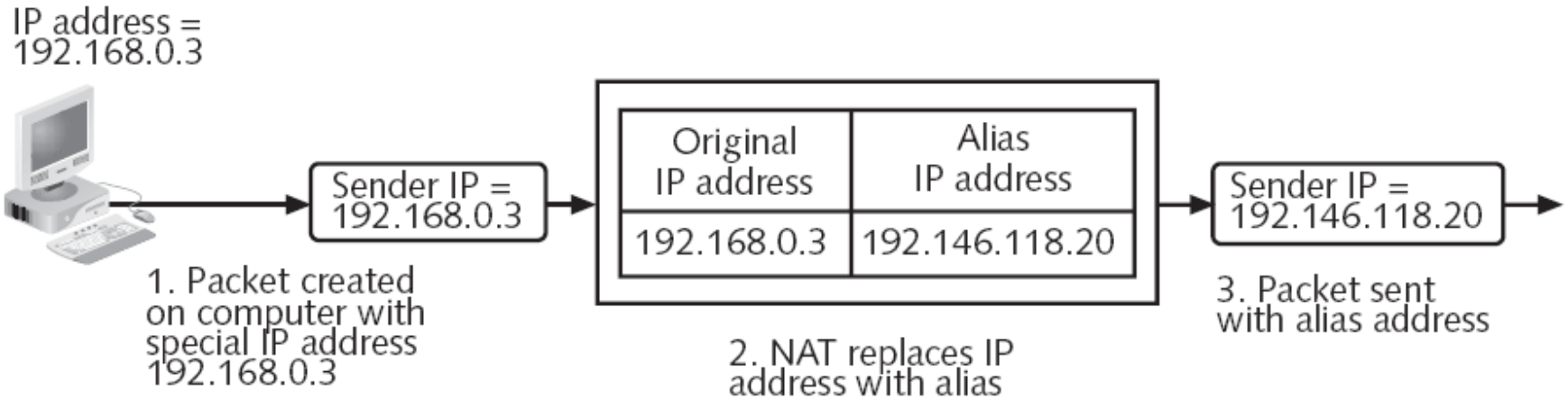


Figure 7-8 Network address translation (NAT)

Segmenting with Devices and Technologies (continued)

Table 7-4 Private IP addresses

IP Address Class	Private IP Addresses
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

Segmenting with Devices and Technologies (continued)

- Network address translation (NAT) (continued)
  - Advantages
    - Security
    - Conserves IP addresses
    - Segmentation
  - Disadvantages
    - Problems with applications/complication (NAT represents one more complexity in setting up and managing the network. It also makes troubleshooting more confusing due to address substitutions

Segmenting by Virtual LANs (VLANs)

- Virtual local area network (VLAN)
  - Logical grouping of network devices within a larger network
  - Devices can be dispersed throughout the network
- How a VLAN works
  - Unicast transmission
    - Packet is sent to a single device
  - Broadcast transmission
    - Packet is sent to all network devices

Segmenting by Virtual LANs (VLANs) (continued)

- How a VLAN works (continued)
  - Broadcast domain (continued)
    - Area in which a broadcast occurs
  - Broadcasts can have an impact on network throughput as more devices send more broadcast transmissions
    - Can be solved creating a VLAN
  - The key to VLANs is the ability of the switch to correctly direct packets
  - IEEE 802.1q
    - Standard for marking VLAN packets
    - Supports trunking

Segmenting by Virtual LANs (VLANs) (continued)

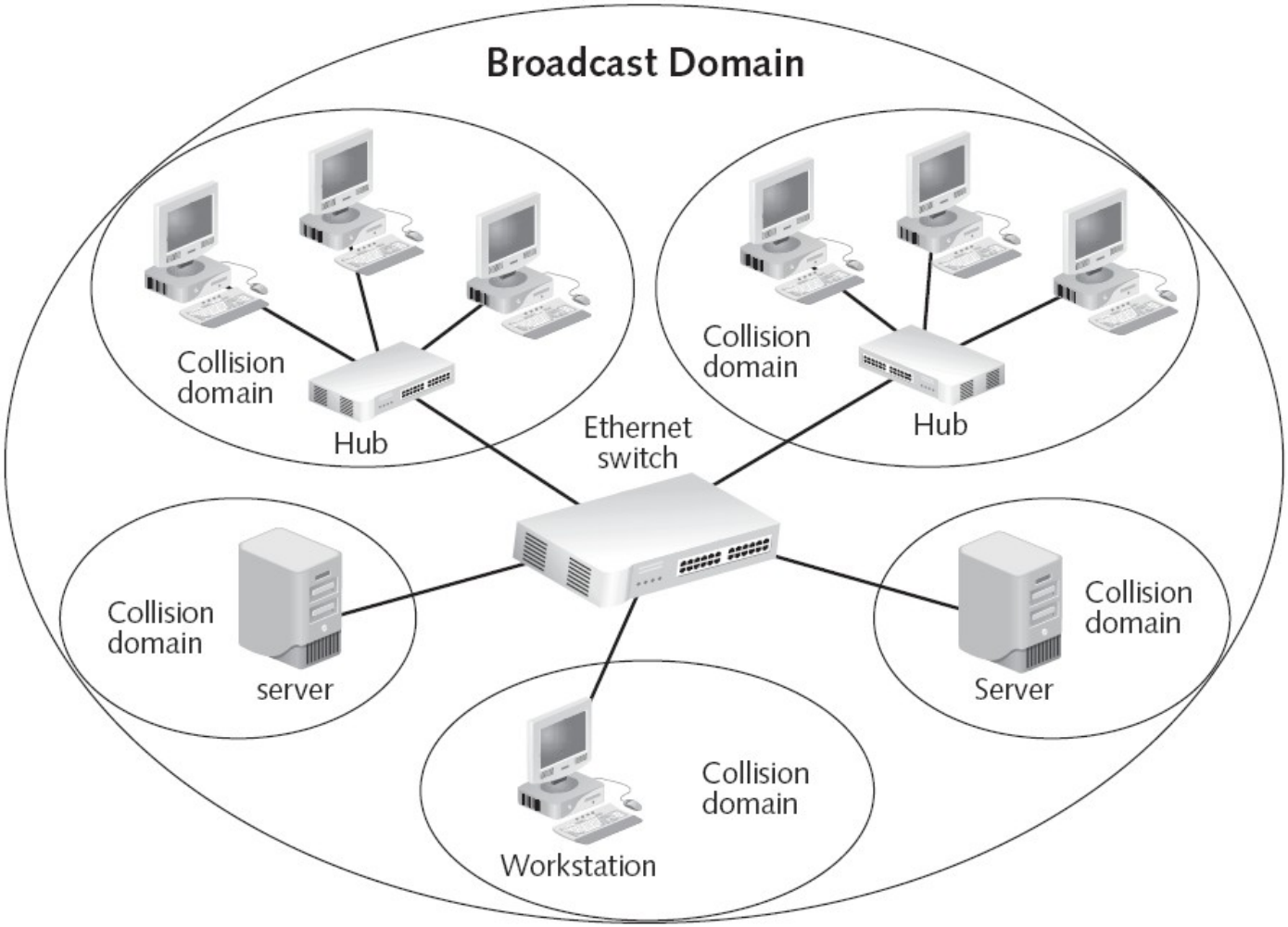
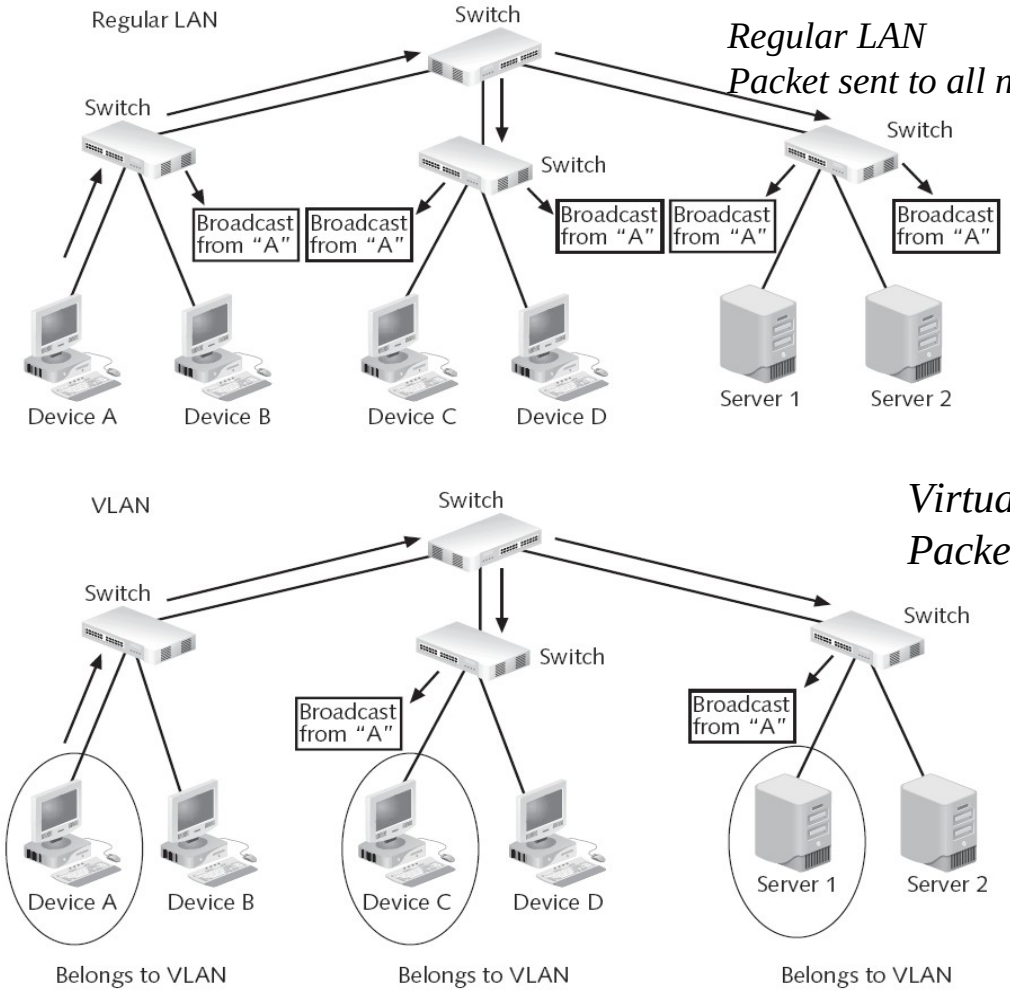


Figure 7-9 Collision domain versus broadcast domain

Segmenting by Virtual LANs (VLANs) (continued)



Regular LAN
Packet sent to all network devices

Virtual LAN
Packets are correctly directed

Figure 7-10 Regular LAN versus VLAN

Segmenting by Virtual LANs (VLANs) (continued)

- How a VLAN works (continued)
  - IEEE 802.1q (continued)
    - Inserts a 4-byte “tag” header within the existing Ethernet packet
  - Cisco Systems’ Inter-Switch Link (ISL)
    - “Wraps” the original Ethernet packet with 30 bytes of additional information

Segmenting by Virtual LANs (VLANs) (continued)

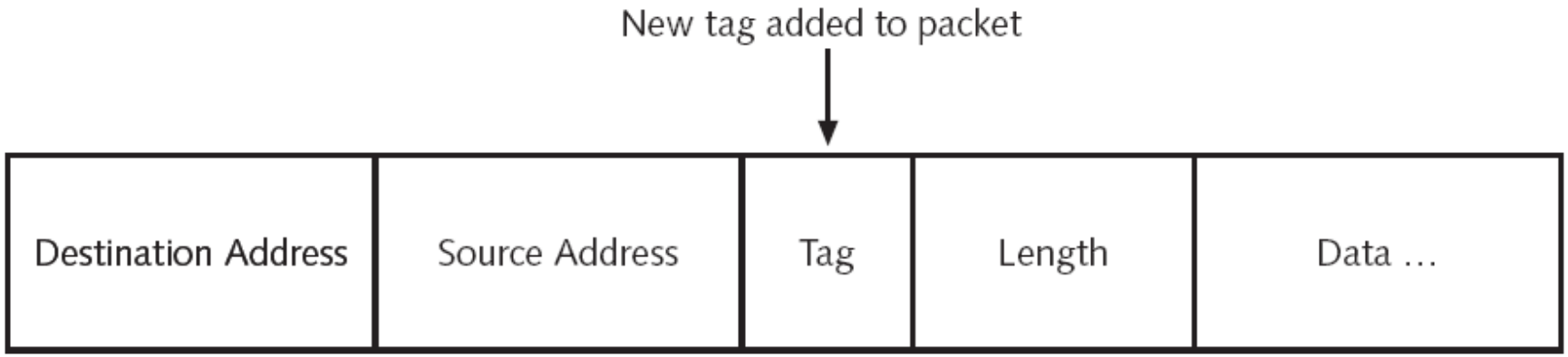


Figure 7-11 Packet with VLAN tag

Segmenting by Virtual LANs (VLANs) (continued)

Table 7-5 Tag header fields

Field Name	Value	Length	Description
Protocol identifier (TPID)	Fixed value of 0x8100	2 bytes	Indicates that the packet is carrying IEEE 802.1q information
Tag control information (TCI)	VLAN ID	2 bytes	Contains the unique ID of the VLAN

Segmenting by Virtual LANs (VLANs) (continued)

Table 7-6 ISL fields

Field Name	Length	Description
Header field	26 bytes	Embedded within header is a 10-bit VLAN ID
Cyclic redundancy check (CRC) trailer field	4 bytes	An error check in addition to the standard packet checking performed by Ethernet

Segmenting by Virtual LANs (VLANs) (continued)

- Wireless VLANs
  - Can be used to segment traffic
  - Flexibility depends on which device separates the packets and directs them to different networks
    - Switch-based configuration does not handle roaming users well since packets are separated at switch level
    - AP-based configuration
      - AP is responsible for separating the packets
      - Different VLANs are transmitted by the AP on different SSIDs

Segmenting by Virtual LANs (VLANs) (continued)

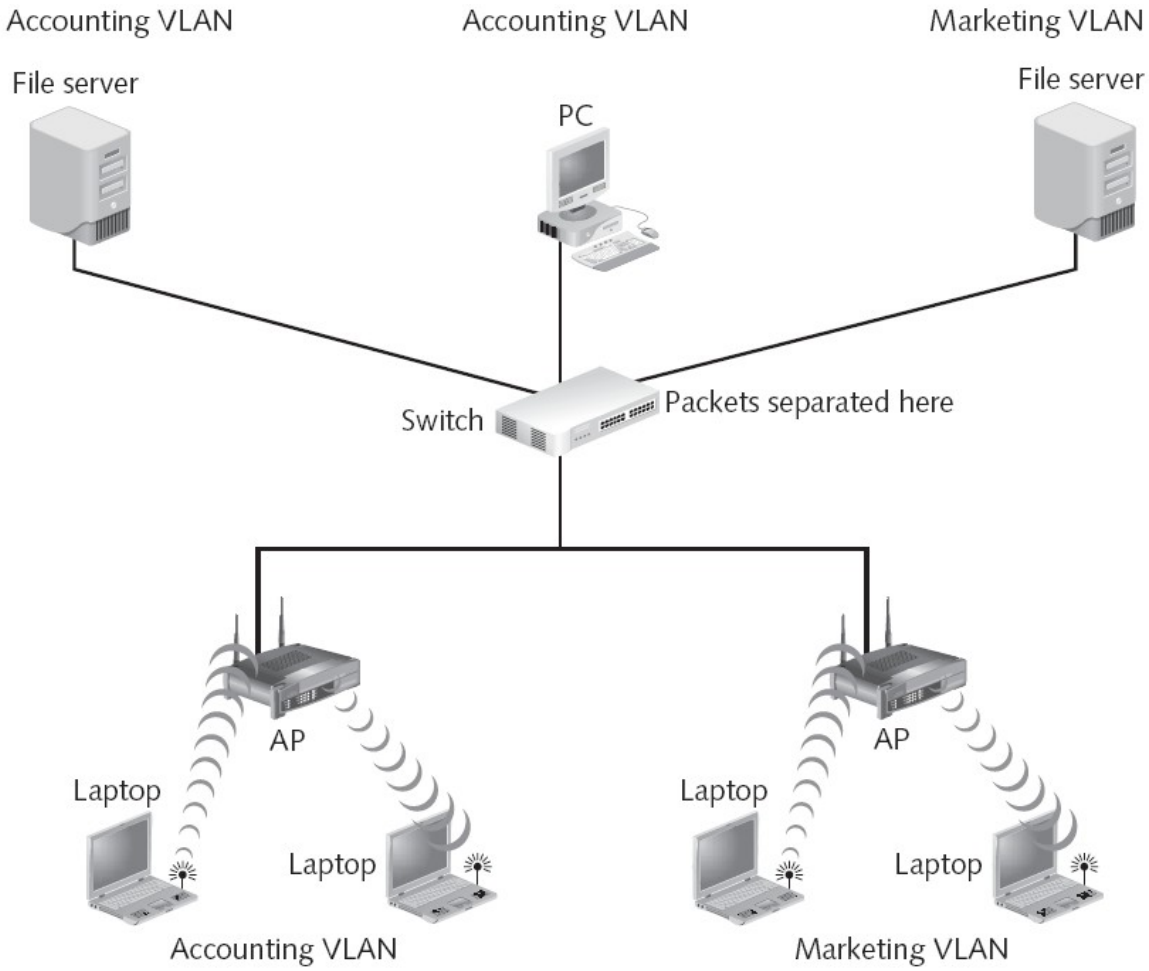


Figure 7-12 Packets separated at switch

Segmenting by Virtual LANs (VLANs) (continued)

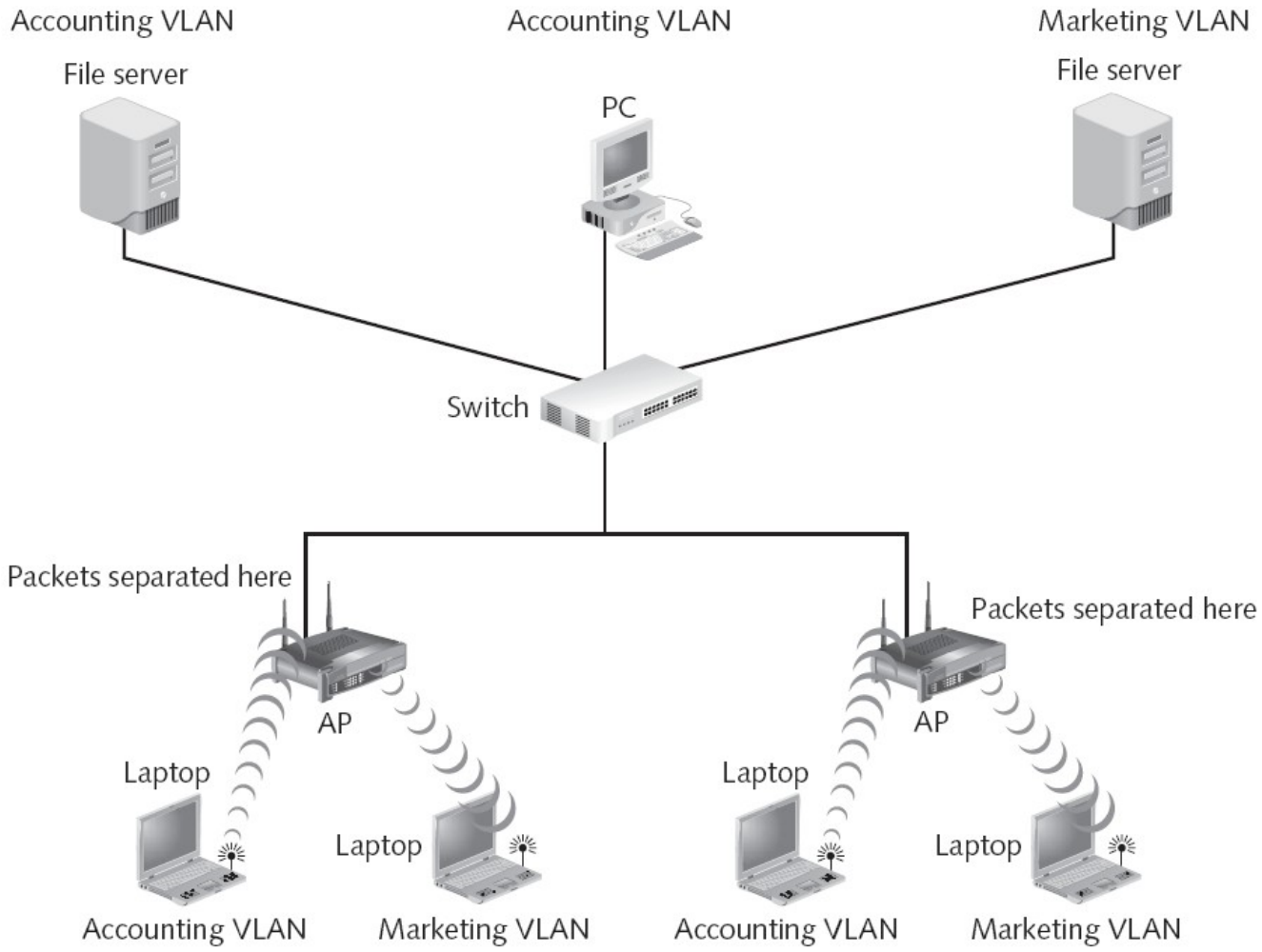


Figure 7-13 Packets separated at access point

Segmenting by Virtual LANs (VLANs) (continued)

- Wireless VLANs (continued)
  - Many organizations set up two wireless VLANs: employees and guests
  - Wireless VLANs allow a single access point to service both VLANs

Segmenting by Virtual LANs (VLANs) (continued)

Table 7-7 Wireless VLAN

Access Level	SSID	VLAN ID	Encryption
Employees only	Employee	1	WPA2 Enterprise
Outside guests	Guest	2	None

Hardware Placement

- Placing the hardware in a physically secure location is also important for security
- APs should be securely fastened to a wall, pole, or similar object to deter thieves
- Plenums
  - Air-handling space above drop ceilings used to circulate and otherwise handle air in a building
  - Placing an AP in a plenum can be a hazard
    - Enclose AP within a plenum-rated enclosure to meet fire safety code requirements

Hardware Placement (continued)



Figure 7-14 Access point secured with lock

Wireless Device Security

- Security of the wireless devices themselves should not be overlooked
- Includes:
  - Personal firewall
  - Antivirus
  - Antispyware
  - Patch software
  - Tools to identify new classes of attacks

Personal Firewall Software

- Each wireless device should have its own software firewall installed
- Hide all unused ports
  - Attackers cannot even see which ports to attack
- Use of ports is governed by a set of rules
- Personal firewalls also support outbound monitoring

  http://www.addictivetips.com/windows-tips/windows-7-firewall-outbound-protection/

  (windows 7 and up revision outbound monitoring rule setup)

Personal Firewall Software (continued)

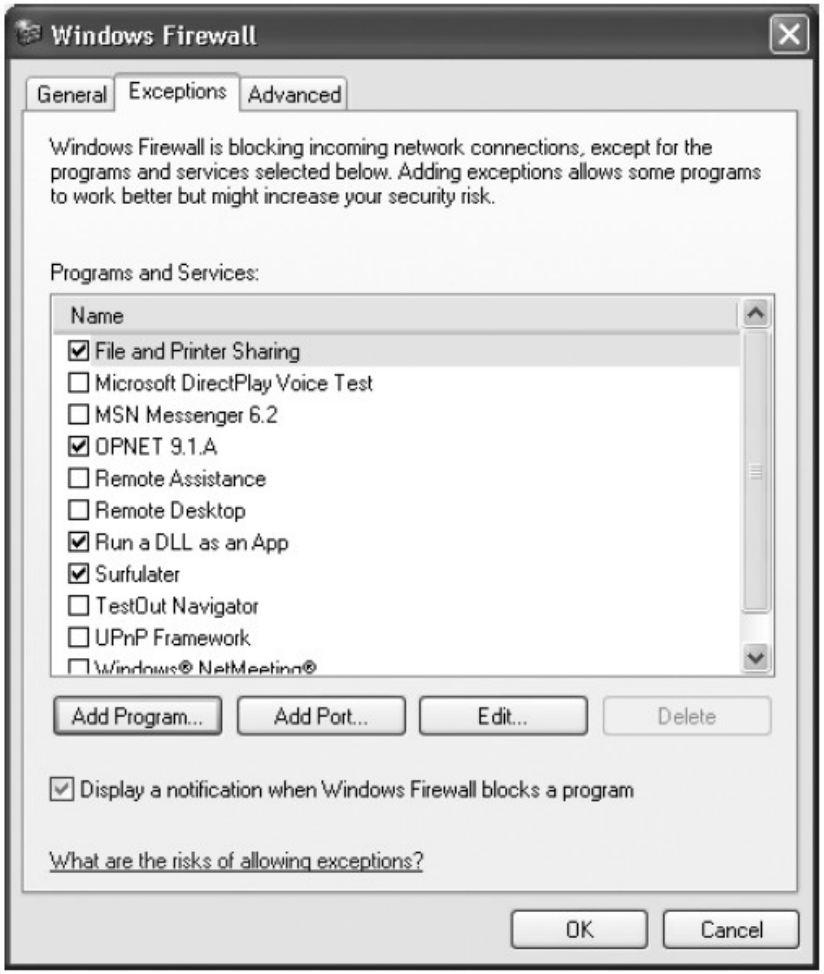


Figure 7-15 Microsoft personal firewall

Antivirus Software

- Best defense against viruses
- Can scan a computer for infections and isolate any file that contains a virus
- Drawback
  - Definition files or signature files must be continuously updated to recognize new viruses
- Most antivirus software packages work with the Windows Security Center
  - Central location to manage some security tools

Antivirus Software (continued)

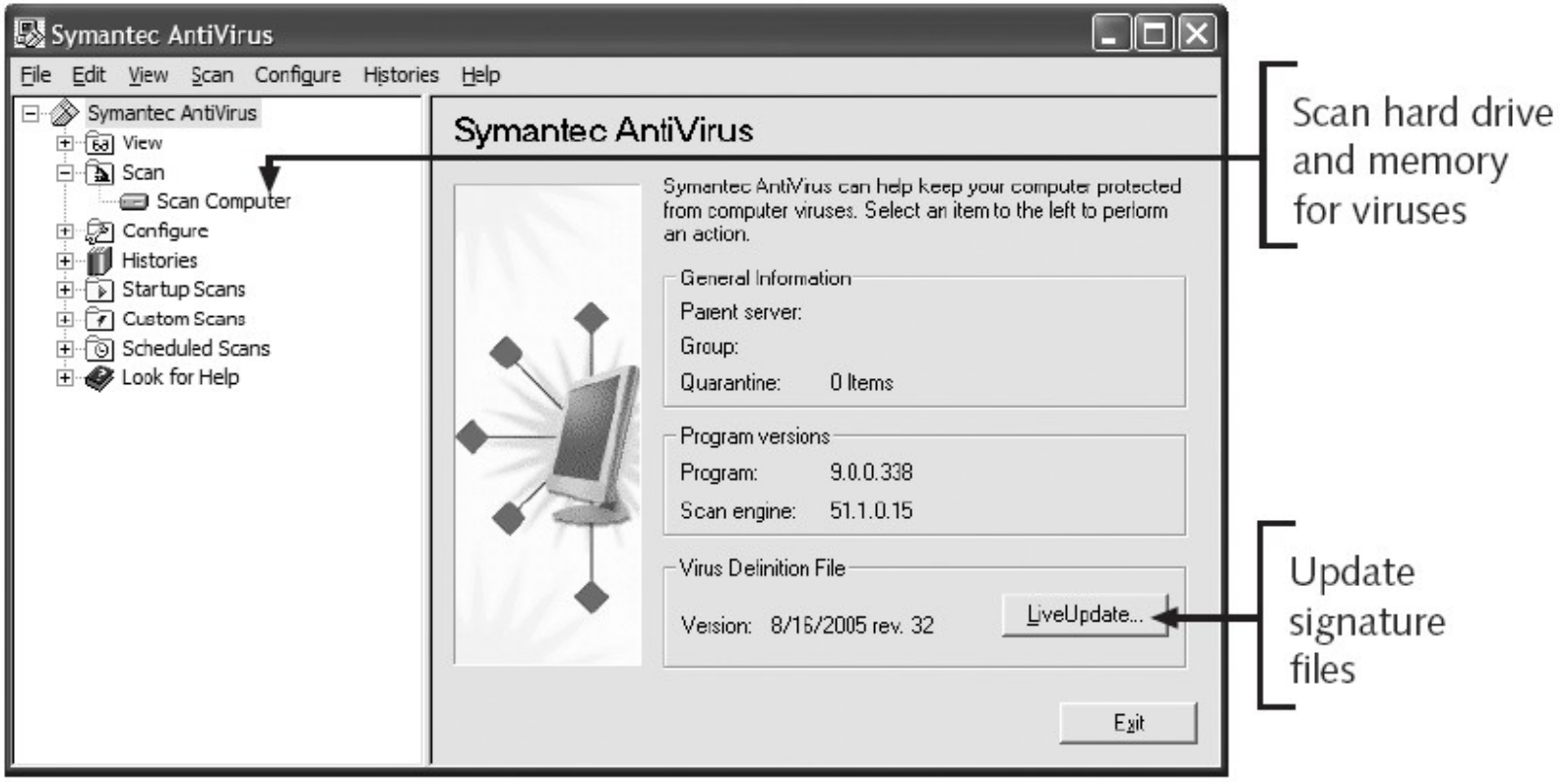


Figure 7-16 Antivirus software features

Antivirus Software (continued)



Figure 7-17 Windows monitoring AV software

Antispyware

- Helps prevent computers from becoming infected by different types of spyware
- Similar to AV software
  - Must be regularly updated
  - Provides continuous real-time monitoring and performs a complete scan

Patch Software

- Describes software security updates
  - Provided by vendors for their application programs and operating systems
- Generally designed to fix security vulnerabilities
- Microsoft patch classifications
  - Critical
  - Important
  - Moderate
  - Low
- Desktop computers can automatically receive Windows patches

Patch Software (continued)



Figure 7-18 Microsoft patch information

Patch Software (continued)



Figure 7-19 Windows automatic update options

Rootkit Detectors

- Rootkit
  - Software tools that attacker uses to break into a computer
    - And obtain special operating system privileges
      - To perform unauthorized functions and hide all traces of its existence
  - Includes several programs designed to:
    - Monitor traffic, create a back door into the computer, change log files, and attack other network devices
- Rootkit itself causes no direct damage to computer

Rootkit Detectors (continued)

- Fundamental problem in detecting rootkits
  - User can no longer trust the operating system
- Programs are available to help detect rootkit
- Disinfecting a computer that has a rootkit is difficult
  - Most security experts recommend to reformat the hard drive and reinstall the OS

Summary

- Five security key principles
  - Layering
  - Limiting
  - Diversity
  - Obscurity
  - Simplicity
- Segmenting a network has several advantages
  - One of which is security
- A VLAN is a logical grouping of network devices within a larger network

Summary (continued)

- Security on wireless devices, such as laptops or PDAs, is also important
  - Personal firewall software
  - Antivirus software
  - Antispyware software
  - Patch software
  - Rootkit detectors