

# DATA COMM

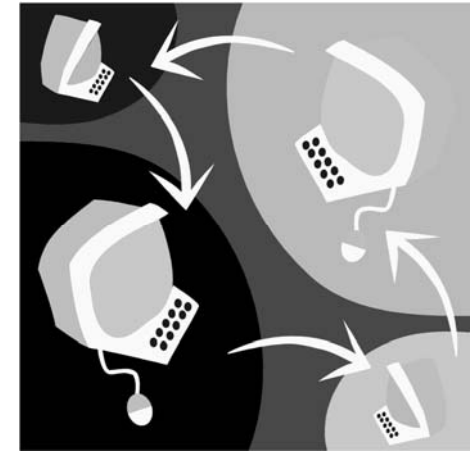
## CSH5 Chapter 5 “Data Communications & Information Security” Raymond Panko

1

Copyright © 2011 M. E. Kabay. All rights reserved.

## Topics

- Sampling of Networks
- Network Protocols & Vulnerabilities
- Standards
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- TCP/IP Supervisory Standards
- Application Standards

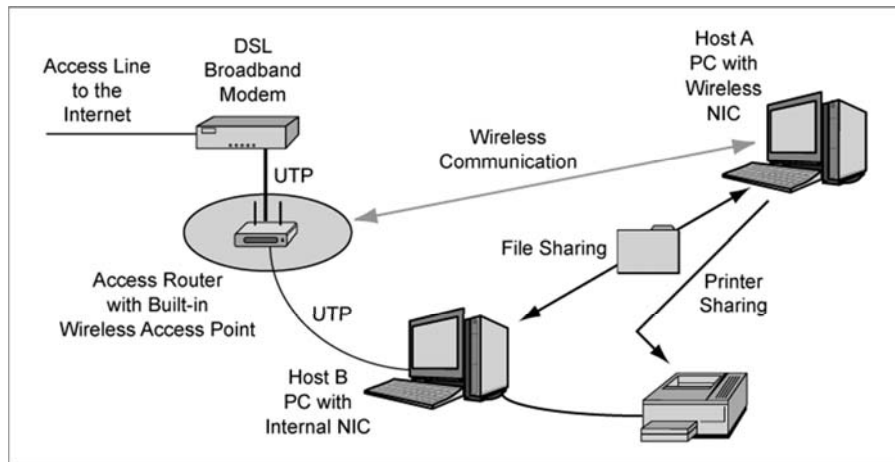


2

Copyright © 2011 M. E. Kabay. All rights reserved.

## Sampling of Networks

### ➤ Simple Home Network

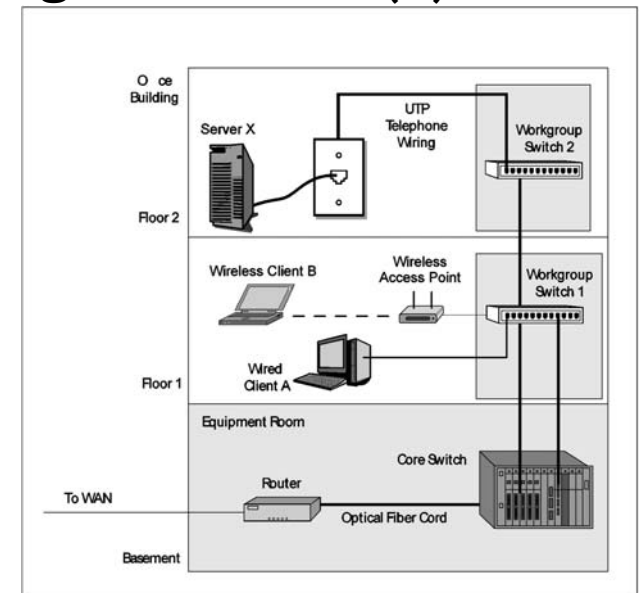


3

Copyright © 2011 M. E. Kabay. All rights reserved.

## Sampling of Networks (2)

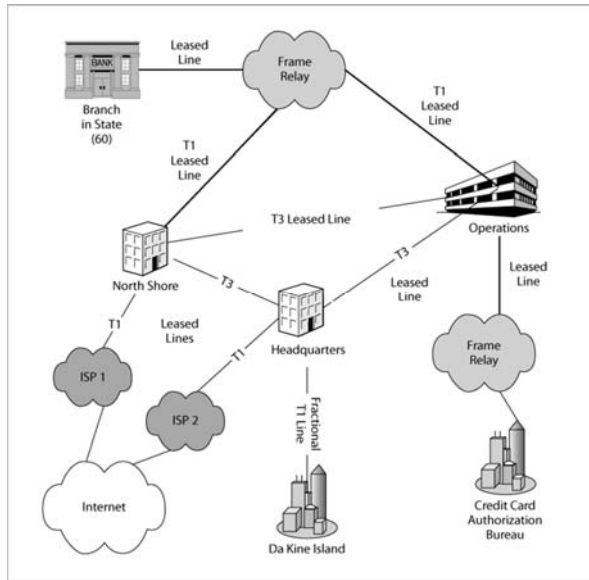
### ➤ Building LAN



4

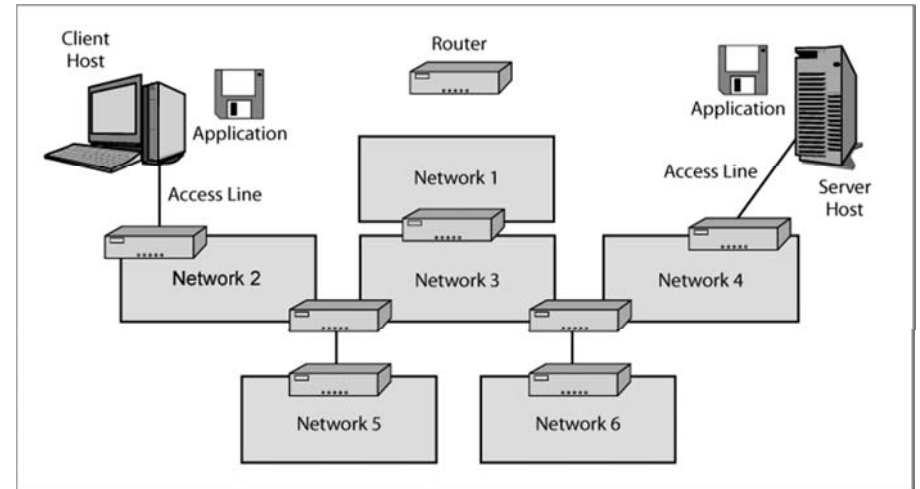
# Sampling of Networks (3)

## ➤ WANS



# Sampling of Networks (4)

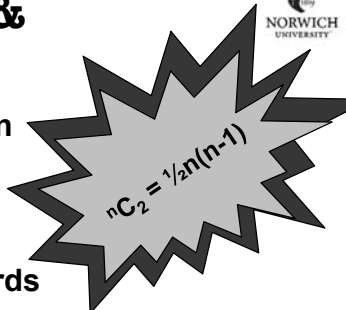
## ➤ Internet



# Network Protocols & Vulnerabilities

## ➤ Standards allow interconnection

- Otherwise we would suffer combinatorial explosion



## ➤ Security implications of standards

1. Inherent design of the standard itself
2. Degree to which security considerations are built into the standard (or not)
3. Effectiveness of implementation of standards in vendor products

# Standards

- Core Layers
- Layered Standards Architectures
- Single-Network Standards
- Internetworking Standards



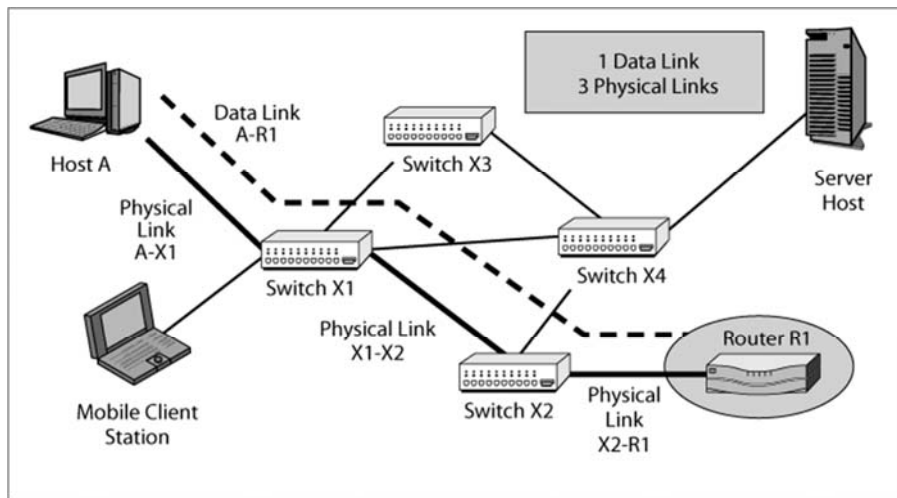
# Core Layers

Super Layer	Description
Application	Communication between application programs on different hosts attached to different networks on an internet.
Internetworking	Transmission of packets across a routed internet. Packets contain application layer messages.
Single Network	Transmission of frames across a single switched network. Frames contain packets.

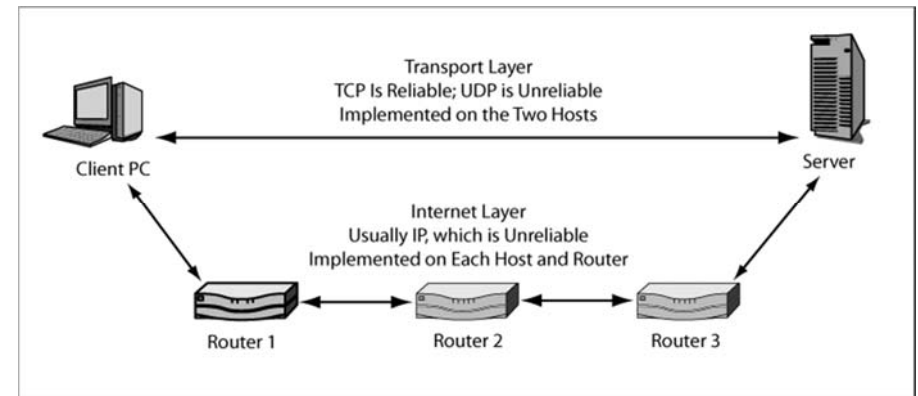
# Layered Standards Architectures

Super Layer	TCP/IP	OSI	Hybrid TCP/IP-OSI
Application	Application	Application	Application
		Presentation	
		Session	
Internet	Transport	Transport	Transport
	Internet	Network	Internet
Network	Subnet Access	Data Link	Data Link
		Physical	Physical

# Single-Network Standards



# Internetworking Standards



# Internet Protocol (IP)

- Basic functions of IP
  - ❑ Organizes packets
  - ❑ Determines how routers move packets
- IPv4 main protocol of today's Internet
  - ❑ Descriptive portion = *header*
    - ✓ Consists of *fields*
  - ❑ Packets can be split into smaller *fragments*
    - ✓ All have same *identification field*
    - ✓ Assigned *fragment offset* value (sequence #)
    - ✓ Reassembled on receiving side
    - ✓ Source & destination addresses
  - ❑ Running out of IPv4 address space!

# IPv4 Packet Structure

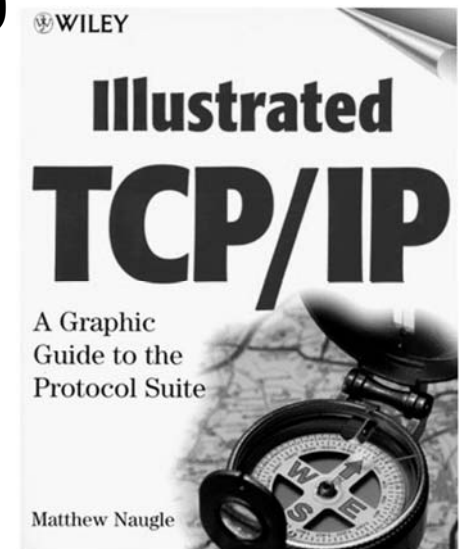
Bit 0				Bit 31			
Version (4 bits) Value is 4 (0100)	Header Length (4 bits)	Diff-Serv (8 bits)	Total Length (16 bits) length in octets				
Identification (16 bits) Unique value in each original IP packet			Flags (3 bits)	Fragment Offset (13 bits) Octets from start of original IP fragment's data field			
Time to Live (8 bits)	Protocol (8 bits) 1 = ICMP, 6 = TCP, 17 = UDP		Header Checksum (16 bits)				
Source IP Address (32 bits)							
Destination IP Address (32 bits)							
Options (if any)					Padding		
Data Field							

# IPv6 Packet Structure

Bit 0				Bit 31			
Version (4 bits) Value is 6 (0110)	Diff-Serv (8 bits) Can be used for Priority, etc.	Flow Label (20 bits) Marks a packet as part of a specific flow of packets; Can be used instead of the destination IP address in routing					
Payload Length (16 bits)		Next Header (8 bits) Name of next header		Hop Limit (8 bits)			
Source IP Address (128 bits)							
IPsec uses a security header to implement security w/ IPv6							
Destination IP Address (128 bits)							
Next Header or Payload (Data Field)							

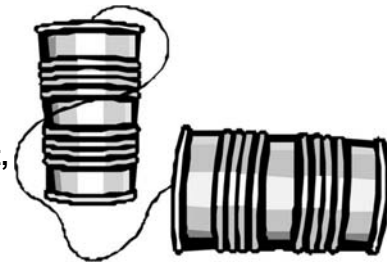
# Transmission Control Protocol (TCP)

- Connection-Oriented & Reliable Protocol
- Reliability
- Flag Fields
- Octets & Sequence Number
- Acknowledgement Numbers
- Window Field
- Options
- Port Numbers
- TCP Security



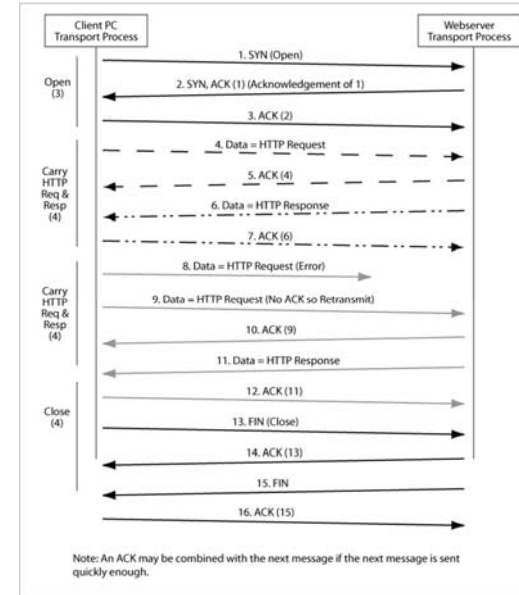
# Connection-Oriented & Reliable Protocol

- Connection-oriented protocols
  - ❑ Initiate *session* of continued interaction
  - ❑ E.g., telephone call between two people using POTS (plain old telephone system)
  - ❑ Protocols for initiating and terminating session (e.g., ringing, “Hello,” “Bye,” hanging up)
- Connectionless protocols
  - ❑ No session initiated
  - ❑ Message sent without necessarily having indication of receipt
  - ❑ E.g., radio, TV broadcast, Web, & e-mail



Copyright © 2011 M. E. Kabay. All rights reserved.

# TCP Session Elements



# Reliability

- *Unreliable* protocol
  - ❑ Does not detect or correct errors
- TCP is *reliable* protocol
  - ❑ TCP checksum field
  - ❑ Recipient uses same algorithm to recompute checksum value
  - ❑ Discrepancy results in dropping packet
- Sender waits for ACK
  - ❑ After specified wait time, resends same packet

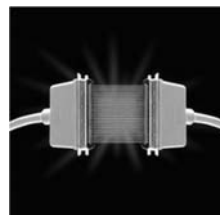
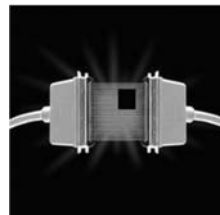


Image Copyright © eHow. All rights reserved. URL: <http://tinyurl.com/3k86vki>  
 Permission requested 2011-09-12 for use of copyrighted material.

Copyright © 2011 M. E. Kabay. All rights reserved.

# TCP Segment

Bit 0		Bit 31	
Source Port Number (16 bits)		Destination Port Number (16 bits)	
Sequence Number (32 bits)			
Acknowledgement Number (32 bits)			
Header Length (4 bits)	Reserved (6 bits)	Flag Fields (6 bits)	Window (16 bits)
TCP Checksum (16 bits)		Urgent Pointer (16 bits)	
Options (if any)			Padding
Data Field			

Flag fields are 1-bit fields. They include SYN, ACK, FIN, RST, PSH, and URG

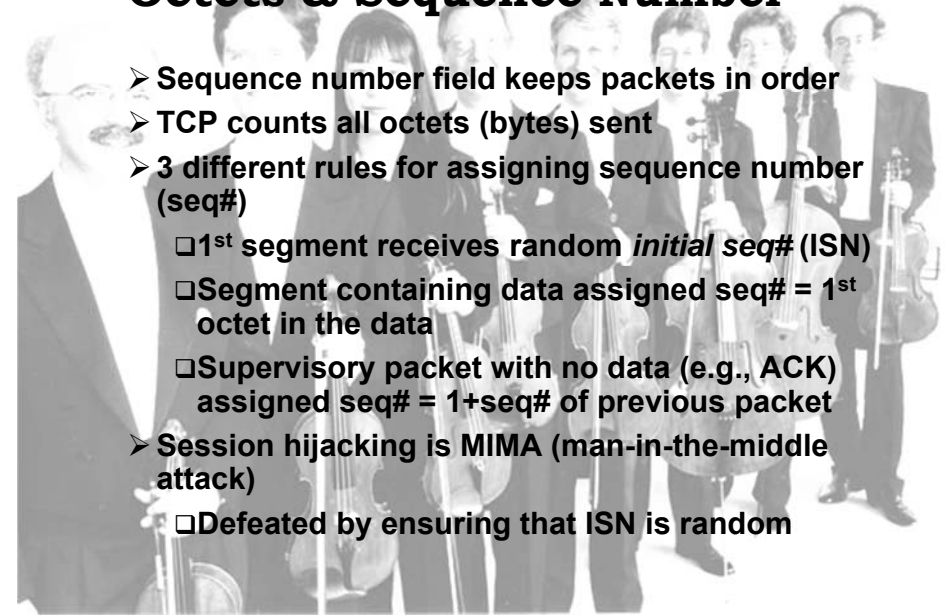
Copyright © 2011 M. E. Kabay. All rights reserved.

## Flag Fields

See "TCP Analysis - Section 4: TCP Flag Options"  
<http://www.firewall.cx/tcp-analysis-section-4.php>

- General term for any single bit variable
  - ❑ Bit = 0 → flag is *not set*
  - ❑ Bit = 1 → flag is *set*
- 6 flags used by TCP header
  - ❑ URG – urgent (e.g., to abort data transfer)
  - ❑ ACK – acknowledgement of receipt
  - ❑ PSH – push (establish priorities)
  - ❑ RST – reset (reject packet / reset connection)
  - ❑ SYN – synchronization (request)
  - ❑ FIN – finished (last packets – terminate)

## Octets & Sequence Number



- Sequence number field keeps packets in order
- TCP counts all octets (bytes) sent
- 3 different rules for assigning sequence number (seq#)
  - ❑ 1<sup>st</sup> segment receives random *initial seq#* (ISN)
  - ❑ Segment containing data assigned seq# = 1<sup>st</sup> octet in the data
  - ❑ Supervisory packet with no data (e.g., ACK) assigned seq# = 1+seq# of previous packet
- Session hijacking is MIMA (man-in-the-middle attack)
  - ❑ Defeated by ensuring that ISN is random

## Port Numbers

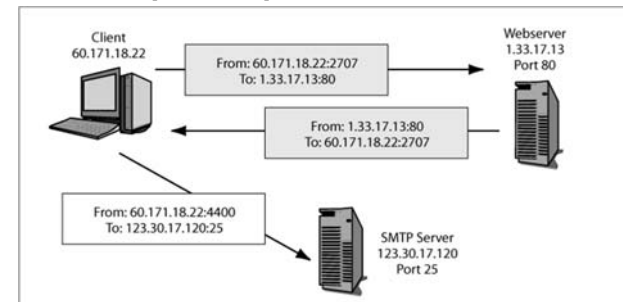
- 1<sup>st</sup> two fields use *TCP port numbers (P#)*
- Servers
  - ❑ P# specifies *service* (application)
  - ❑ E.g., TCP 80 → HTTP; TCP 25 → SMTP; TCP 20 & 21 → FTP



- Clients
  - ❑ Random ephemeral P# generated when connecting to server
  - ❑ Windows uses TCP P# ∈ {1024,4999}
  - ❑ IETF standard range is TCP P# ∈ {5000,65534}
  - ❑ Difference causes problems for firewalls

## Sockets

- Socket = IP address & TCP Port #
  - ❑ Written nnn.nnn.nn.nn:nn
- Socket spoofing
  - ❑ Generate packets with socket data matching existing connection
  - ❑ Insert spoofed packets into data stream



## TCP Security

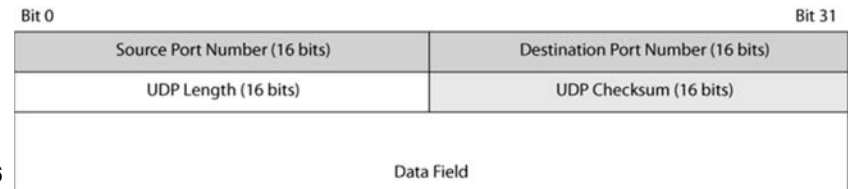
- TCP originally designed without security
  - ❑ And continues without it
- IPsec center of IETF efforts for Internet security
  - ❑ But few users have moved to IPsec
  - ❑ Therefore some pairs of users apply electronic signature
- RFC 2385, “Protection of BGP Sessions via the TCP MD5 Signature Option”
  - ❑ Border Gateway Protocol used for exchange among administrative systems
  - ❑ Long-term relationships (like leased lines in old days)
  - ❑ Viewed as relatively weak security

25

<http://tools.ietf.org/html/rfc2385>

## User Datagram Protocol (UDP)

- Some services do not require reliability
  - ❑ VoIP (Voice over IP)
  - ❑ SNMP (Simple Network Management Protocol)
- UDP: connectionless & unreliable – & simple
- UDP & TCP both use port #s – but are different types of ports
  - ❑ So always specify which kind of port #
  - ❑ E.g., “TCP port 80” for HTTP
- UDP even weaker than TCP



26

## TCP/IP Supervisory Standards

- ICMP
- DNS
- DHCP
- DRP
- SNMP



27

## ICMP

- Internet Control Message Protocol
  - ❑ E.g., *echo* & *echo reply*
  - ❑ Check for activity/existence of host
  - ❑ *Ping* is program that “pings” using *echo/echo reply* sequence
  - ❑ Attackers often ping hosts to map network
- *Traceroute (tracert)*
  - ❑ Also lists routers on path between sender and responder
  - ❑ Firewalls often drop *echo reply* messages
- ICMP also used for error messages
  - ❑ E.g., response to malformed packet
  - ❑ Reveals IP address of router – useful for attacker



28

# DNS

- Domain Name System
  - ❑ Resolve alphanumeric domain name (e.g., norwich.edu) into numeric address (e.g., 192.149.109.19)
  - ❑ Network of DNS root servers exchange info
- DNS cache poisoning
  - ❑ Attacker inserts incorrect data about host name – IP address relation
  - ❑ Subsequent users are misdirected to a wrong site
- DNS security complex & unresolved issue

# IPv4 Address Space Exhaustion: DISCUSS!

- IPv4 uses 32 bits  $\cong$  4.29e9 addresses
  - ❑ Being eaten up fast by mobile devices
  - ❑ IPv6 uses 128 bits  $\cong$  1.70e38
- van Beijnum, I. (2010) “>90% of IPv4 address space used; IPv6 move looking messy.” Ars Technica (Jan 21, 2010) < <http://tinyurl.com/yaqu3f9> > (retrieved 12 Sep 2011)



BT IPv6 > IPv4 Exhaustion Countdown <http://penrose.uk6x.com/>

**RIPE Regional registry IPv4 address exhaustion in... 141 Days, 05 Hours, 21 Minutes, 53 Seconds.**

**APNIC IPv4 RIR: All Gone! 15th April 2011**

**IANA Central IPv4 Registry: All Gone! 1st February 2011**

- BT has been providing IPv6 network services since 2000.
- For information about new BT IPv6 services please contact BT Global Services.
- For IPv6 peering requests please visit the BT Public IPv6 Peering Request page.

You are using IPv4.

Copyright © 2011 M. E. Kabay. All rights reserved.

# DHCP

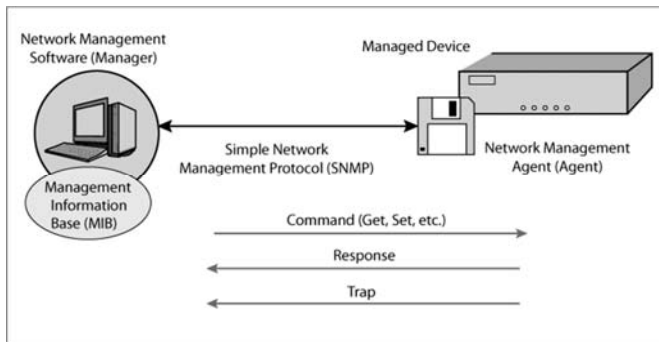
- Dynamic Host Configuration Protocol
  - ❑ Servers have fixed IP addresses
  - ❑ Client PCs on internal networks have dynamic (temporary) addresses on Internet
  - ❑ Problems arise because DHCP may assign different IP addresses on subsequent uses
- P2P (peer-to-peer) applications less secure
  - ❑ Need to locate peer despite change of IP address
  - ❑ Exploited by P2P software used for illegal file sharing

# Dynamic Routing Protocols

- Routers exchange information about available routes
  - ❑ Traffic data
  - ❑ Broken links
- Many dynamic routing protocols available
  - ❑ RIP – Routing Information Protocol
  - ❑ OSPF – Open Shortest Path First
  - ❑ BGP – Border Gateway Protocol
  - ❑ EIGRP® – Cisco Systems’ Enhanced Interior Gateway Routing Protocol
- Attacker may be able to insert false packets into protocols to misdirect packets
  - ❑ Could lead to MIMA

## SNMP

- Simple Network Management Protocol
  - ❑ Control devices such as routers, switches, gateways, hosts...
  - ❑ IETF SNMP allows control of devices
  - ❑ May reconfigure devices
- Attackers can use remote reconfiguration
  - ❑ Many system managers disable remote configuration capabilities



33

Copyright © 2011 M. E. Kabay. All rights reserved.

## Application Standards

- Application layer standards have their own security issues – *discussed in other chapters*
- HTTP (HyperText Transfer Protocol) & HTML (HyperText Markup Language)
- E-mail: SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol), IMAP (Internet Message Access Protocol), MIME (Multipurpose Internet Mail Extensions), S/MIME (Secure MIME)
- Telnet, FTP (File Transfer Protocol), SSH (Secure Shell)
- VoIP (Voice over IP), P2P, SOA (Service-Oriented Architecture), Web services

34

Copyright © 2011 M. E. Kabay. All rights reserved.

# DISCUSSION

35

Copyright © 2011 M. E. Kabay. All rights reserved.