

Computer System Security and Management

SMD139

Lecture 4: Networks and Security
Peter A. Jonsson



History

60's

- A series of memos by Licklider at MIT, describing a "Galactic network"
- Soon thereafter - Licklider head of computer research program at DARPA

60's #2

- Kleinrock, also at MIT, wrote article on packet switching instead of circuit switching
- Kleinrock convinced Roberts of the feasibility of packet switching. Roberts connected two computers over a phoneline

60's #3

- 1968 - Roberts went to DARPA with a funding request for "ARPANET"
- Late 68 - four computers connected, using Network Control Protocol (NCP) for Host to Host communication

70's

- NCP depended on the network being reliable
- Kahn and Cerf started working on what became TCP/IP
- Initial design had no separation of TCP and IP, at a later stage they realized that UDP was needed

80's

- Transition from NCP to TCP/IP for entire network on January 1, 1983
- Resulted in buttons distributed with the text "I survived the TCP/IP transition"

Types of Networks

Wide Area Networks

- ◉ Span large areas (countries, continents, ..)

Local Area Networks

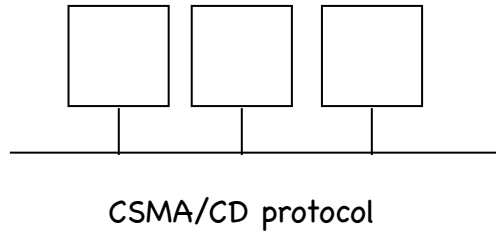
- ◉ Spans the office, or building
- ◉ Very few hops
- ◉ Generally some form of Ethernet
- ◉ Typically 10 Mbit/s to 1 Gbit/s

Layers

- ◉ Layer 5: Application (HTTP, SMTP, FTP)
- ◉ Layer 4: Transport (TCP, UDP, UDP Lite)
- ◉ Layer 3: Network (IP)
- ◉ Layer 2: Link (Ethernet, PPP)
- ◉ Layer 1: Physical (Individual bits on transmission medium, fiber or twisted copper wire)

Ethernet

Traditional Ethernet



CSMA

- ⦿ Don't interrupt others when they talk!
- ⦿ Listen before sending
- ⦿ Does not guarantee collision free communication - transmission delays are troublesome
- ⦿ Entire packet transmission time wasted

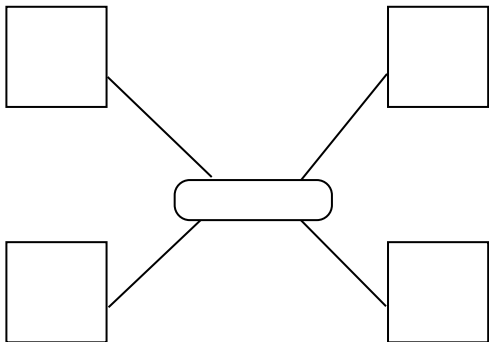
Collision Detection

- ⦿ Colliding transmissions aborted to reduce wasted time

MAC addresses

- ⦿ Unique 48 bit address for every adapter
- ⦿ Used to get each frame from one node to another within the same network
- ⦿ Allocation of addresses administered by IEEE
- ⦿ Manufacturer buys a portion of the available addresses to ensure uniqueness

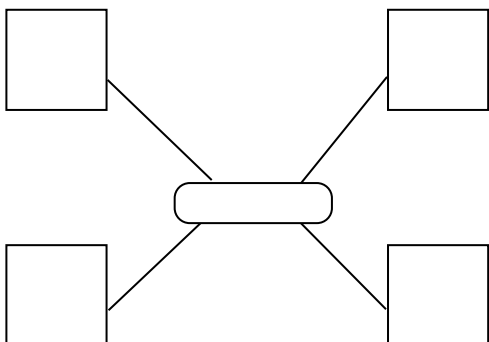
Hubs #1



Hubs #2

- Hub acts as a broadcast repeater, so shortened cable length
- Still CSMA/CD protocol
- One faulty link does not bring down the entire network
- Cheap cables

Switches #1



Switches

- The switch queues packets and transmit to destination, not everybody else
- Nodes can transmit at their full capacity
- Today switches has replaced hubs
- Typical capacity 20-40 ports

TCP/IP

Internet Protocol (IP)

- ◉ Designed to work well on a number of different link technologies, not only Ethernet
- ◉ Current version (v4) gives 32 bit of addresses
- ◉ 127.0.0.1 is the ordinary loopback interface

Private Networks

- ◉ Some addresses are reserved for private use, namely
 - ◉ 10.0.0.0 to 10.255.255.255
 - ◉ 172.16.0.0 to 172.31.255.255
 - ◉ 192.168.0.0 to 192.168.255.255

ARP

- ◉ IP Address -> MAC Address mapping
- ◉ RARP: MAC Address -> IP Address mapping
- ◉ Each node keeps a table (ARP table), this table can be modified with the "arp" command

DHCP

- Automatic assigning of network information
- Server assigns IP address

Netmask

- Defines the split of the IP address into network and host part
- /24 and 255.255.255.0 are the same
- All IP's with equal network part are in the same subnet

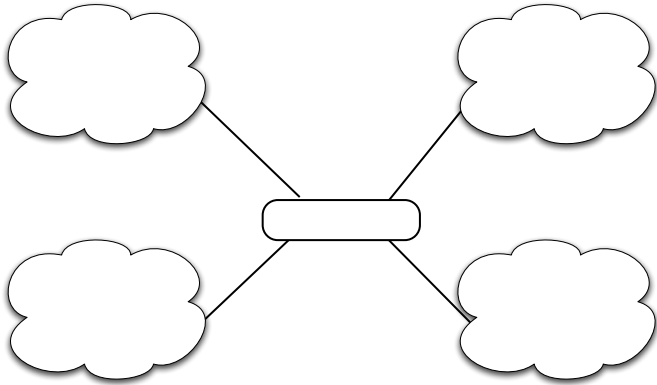
Network Settings

- IP Address: The address of the interface/machine
- Netmask: How big is the network that is directly connected to your computer
- Default Gateway: Packets which end up outside your network are sent here

How to debug

- ping
- traceroute
- snoop/tcpdump
- ifconfig, route
- ipconfig /all on Windows

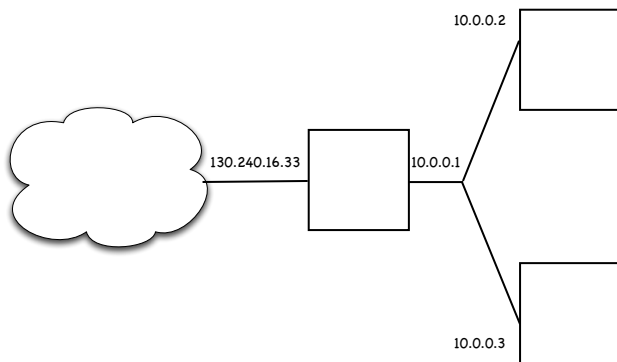
Routers #1



Routers #2

- Uses IP Addresses
- The routing table decides where traffic is sent

NAT



To NAT or not?

- No need for extra addresses from ISP
- Can change local addresses without telling the world
- Can change ISP without renumbering on the inside

To NAT or not? #2

- ⦿ There is no global address shortage
- ⦿ IPv6 has more than enough addresses
- ⦿ All applications do not work through NAT
- ⦿ Abuse tracking is harder through NAT

Security

Threats

- ⦿ Ordinary break ins, by
 - ⦿ Social Engineering
 - ⦿ Finding holes
- ⦿ Viruses/Worms
- ⦿ Trojan Horses
- ⦿ Denial of Service attacks

Consequences #1

- ⦿ Classified/Sensitive Information might leak
 - ⦿ Passwords
 - ⦿ Customer records
 - ⦿ Intellectual Property

Consequences #2

- Computers might stop working - probably equals financial losses
 - Common from Viruses/Worms/Trojan horses
 - The entire point of DOS attacks

Consequences #3

- Regardless of what happened - it needs to be cleaned up, both preventing people from working and incurring a cost for "the cleaner"

Partial Solutions

- Install antivirus software and make sure it is updated at all times
- Education of users
 - Do not blindly click on everything sent to you by strangers
 - Never give away passwords, to anyone

ARP poisoning

- Switches are not as secure as people think they are - it is easy to see others traffic

Chroot - change root directory for a command

- Contains a process to a certain directory (say /chroot), if it tries to access /etc it will really access /chroot/etc
- Not an excuse for running insecure software!
- Better than nothing, but absolutely not foolproof - there are ways to get out of both chroot and jail

Firewalls

- Filters packets, idea is to avoid forwarding unauthorized/unwanted packets
- Implementation 101: Block everything, open up for things that should be let through
- Do NOT block all ICMP, Path MTU Discovery is needed

Rule of Thumb

- If a computer is not secure enough to be without a firewall - it is not secure enough to be on the network at all

Getting past FW's

- Trick the user/admin (Social engineering)
- Find a vulnerability in the FW
- Throw "random" packets at it, with luck someone will disable the firewall

Securing Machines

- Same as firewall - close down everything that is not necessary
- Make sure the user running the service has the least amount of privileges possible
- Restrict who can connect to the service
- Make sure your machine is patched with the latest security updates

Virtual Private Network

- A tunnel into your network from the outside
- Useful for people who work from home but still need to access critical systems

IPsec

- Provides security at the IP Layer, below TCP/UDP
- Possible to tunnel over IP (IP over IP, duh)

Components

- Authentication Header (AH) - responsible for authentication
- Encapsulated Security Payload (ESP) - responsible for encryption
- Internet Key Exchange (IKE) - responsible for handshake to establish encrypted communication

Routing

Intra-Domain Routing

- ◉ Routing within an autonomous system
- ◉ Interior Gateway Protocols (IGP)
- ◉ Common Protocols:
 - ◉ RIP - Distance Vector Protocol
 - ◉ OSPF - Link State Protocol

RIP

- ◉ Uses hop count as routing metric
- ◉ Infinity = 16
- ◉ Exchanges information with neighbors by response messages (advertisements) consisting of subnet addresses and distances to each subnet

OSPF

- ◉ Open: Publicly available
- ◉ Each router has a complete topology map
- ◉ Paths computed with Dijkstra's shortest path algorithm (Router uses itself as source node)
- ◉ Advertisements by flooding

Extra features in OSPF

- Authentication on all messages
- Multiple same cost paths allowed
- Hierarchical OSPF in large domains

Inter-Domain Routing

- Border Gateway Protocol (BGP) common
- Does not care what routing is used within the AS

Lab instructions

Stuff to do

- Configure inetd.conf
- Check daemons started in the runlevel you normally use
- Run nmap from another machine to check for open ports
- Configure your firewall

Quagga

- Labs will use OSPF
- Software: <http://www.quagga.net>