"I can't explain it – it's just a funny feeling that I'm being Googled."

ECPE/COMP 178

Computer Network Security

Introduction

Slide 1 of 842

Recommended General Reading

The Cuckoo's Egg *(easy read)*
The Art of Intrusion
Spies Among Us *(easy read)*
Secrets of Computer Espionage

Conceptual vs Technical

Recommended Technical Reading

Counter Hack Reloaded
Hacking: The Art of Exploitation
Intrusion Signatures & Analysis
Rootkits

★★★★★

Recommended Tool Reading

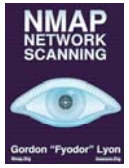
Secrets of Network Cartography
www.networkuptime.com/nmap/index.shtml

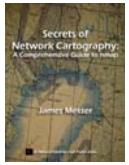
Nmap Network Scanning

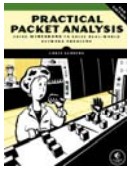
Practical Packet Analysis

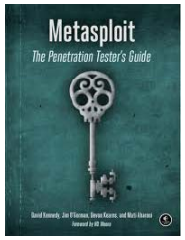
Metasploit – Guide

And then there is the web....









ECPE/COMP 178

Tools and material used in this class may carry import/export restrictions, may not be legal to possess or use in some countries, may violate ISP/UOP acceptable use policies.

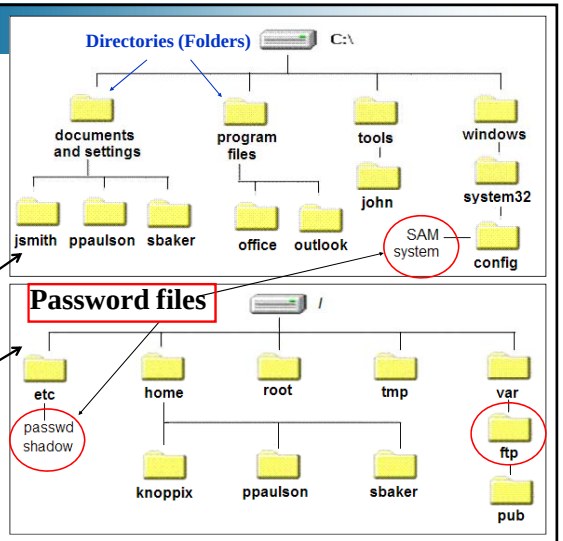
Installing and using the software tools on your computers will likely require excluding the tools from AntiVirus software and changing software firewall settings.

Visiting <u>any</u> ~~'hacking'~~ website carries a risk.

You must understand this!

<u>Windows</u> directory structure

<u>Linux</u> directory structure



Class Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
  Human access
  Physical access
  LAN (insider) access
  Remote (Internet) access
  Wireless access
E. Anatomy of an Attack
  Step 1: Target survey
  Step 2: Vulnerability assessment
  Step 3: Vulnerability exploitation
  Step 4: Maintaining access/persistence
  Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

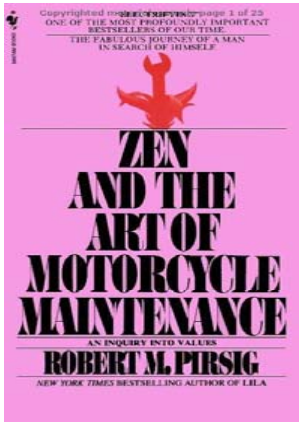
Introduction

Hacking is a state of mind…

Like crossing the nation on a motorcycle,

(or sanity)

not everyone is cut out for it….



2600Hz

- Back in 1971 Cap'n Crunch cereal gave away a plastic whistle called the Captain Crunch whistle. If you blew it it made a 2600 Hz tone.
- Back then, A 2600Hz tone told the AT&T long lines that a trunk line was ready and available to route a new call. People quickly learned that the Cap'n Crunch whistle sidestepped the phone system's billing system.
- www.2600.com – The Hacker Quarterly

2600hz

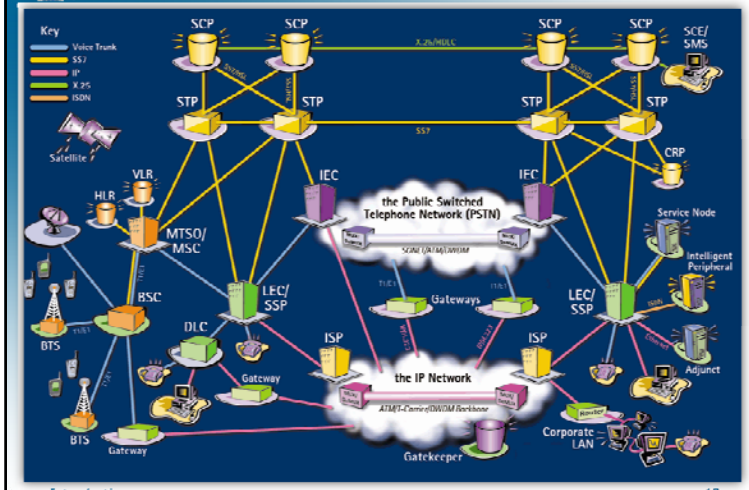
Telephone Network

- aka Phreaking
- Switch-hooking rotary dialers
- MultiFrequency signaling between switch centers
  - 2600 Hz in-band signaling tone
  - John Draper – Cap'n Crunch whistle
  - Blue box – Draper teaches Woz

eBay $21++

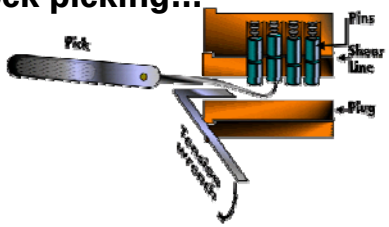
Bell converts to out-of-band signaling

The Network Has Grown



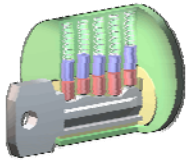
Introduction

Hacking is like lock picking…



- **attitudinally**
- **historically**
- **conceptually**
- **technically**

- **MIT computer access**
  - **early timeshare systems**



MIT's *The Art of Lock Picking (Chapter 7)*

The attacker (already an expert) …

- Knows each lock's special characteristics
- Can recognize and exploit the "personality traits" of each lock, so picking will go much faster
- Never underestimates analytic skills involved in lock picking
- Never thinks that the picking tool opens the lock
- Knows that the pick is just running over the pins to gain information about the lock
- Knows it's the human who opens the lock
- Remembers what works with each lock
- Erases his fingerprints
- Lives a life of research, trial & error, and practice.

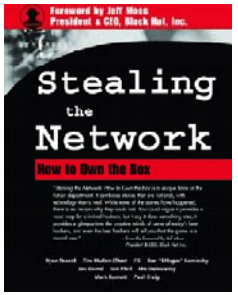
Anatomy of a Computer Attack

The attacker (already an expert) …

- Knows each OS's special characteristics
- Can recognize and exploit the "personality traits" of each OS, so exploitation will go much faster
- Gathers general information about the target
- Scans the target, determining the number of computers, their OSs, their open ports
- Scans deeper, looks for specific vulnerabilities
- Attempts to exploit each vulnerability found, eventually finding a way in and accomplishing goal
- Stores programs and/or creates accounts that will allow easier access next time
- Erases any evidence that he was ever there
- Lives a life of research, trial & error, and practice.

Introduction

From *Stealing the Network: How to Own the Box…*



- "Even the best hackers will tell you that the game is a mental one."
- **"While you may have the skills, if you lack the mental fortitude, you will never reach the top."**
- "Hackers have the big picture in mind while working on the smallest detail."
- **"And they don't expect the first thing they try to work."**

Introduction

"And they don't expect the first thing they try to work!"

"And they don't expect the first thing they try to work."

"And they don't expect the first thing they try to work."

...wait till you see what Blind SQL Injection is like!

Class Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   Human access
   Physical access
   LAN (insider) access
   Remote (Internet) access
   Wireless access
E. Anatomy of an Attack
   Step 1: Target survey
   Step 2: Vulnerability assessment
   Step 3: Vulnerability exploitation
   Step 4: Maintaining access/persistence
   Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

Scale

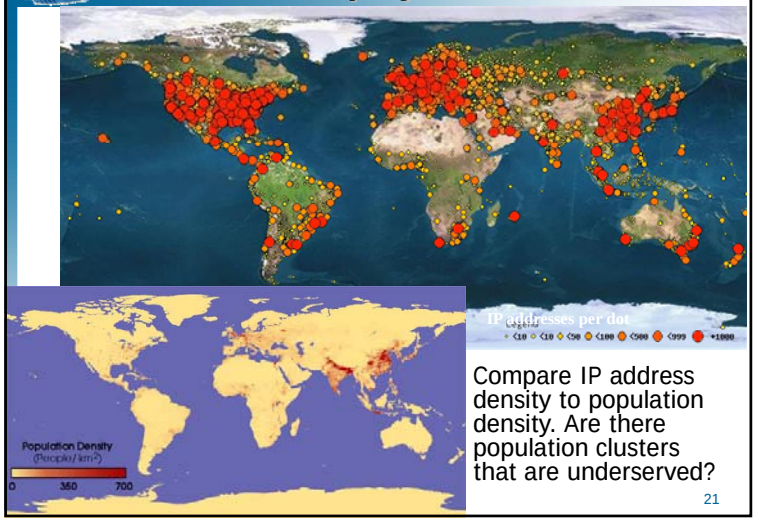
- BAN - Body Area Network (sensors)
- PAN - Personal Area Network (smartphones)
- HAN - Home Area Network
- LAN - Local Area Network
- CAN - Campus Area Network (multi-building)
- MAN - Metropolitan Area Network (city)
- WAN - Wide Area Network (regional)

Internet Traffic Flows

Maps are made difficult as Internet circuits/traffic are a moving target w/many multi-national circuit providers.

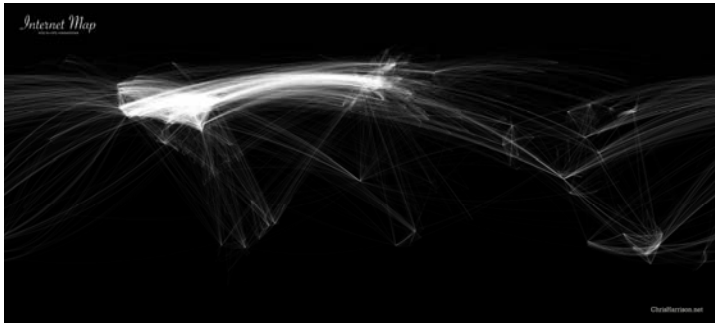
- **Traffic flow map – EU traffic to Asia goes via....**
- **What other inferences could be made?**

Internet Map by IP Addresses



Compare IP address density to population density. Are there population clusters that are underserved?

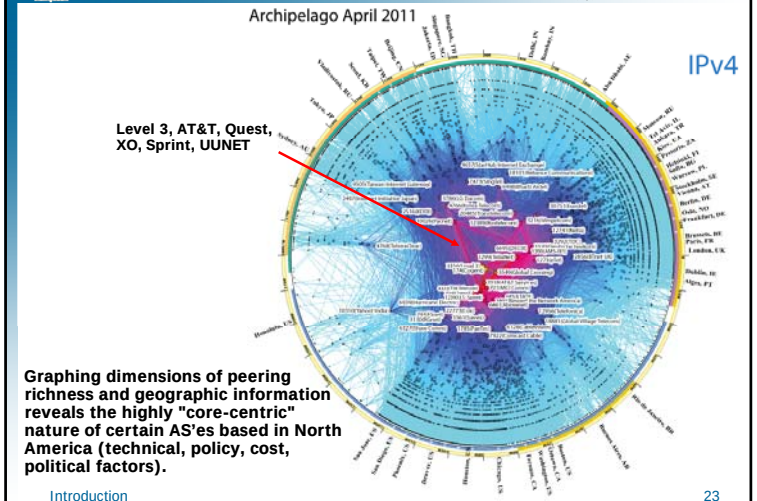
City by City Connections



Logical paths

illuminate interconnection patterns (2007)

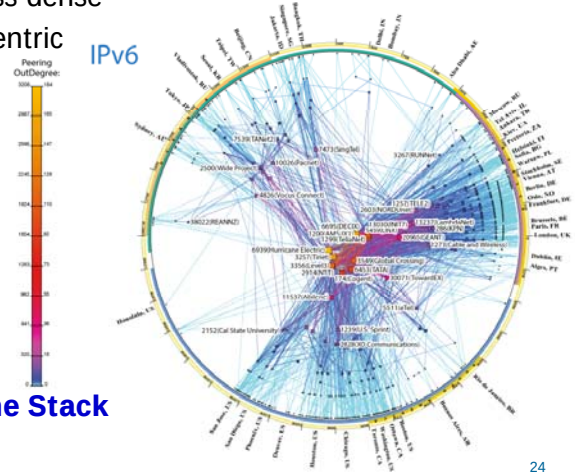
'Skitter Map' By Peering



Graphing dimensions of peering richness and geographic information reveals the highly "core-centric" nature of certain AS'es based in North America (technical, policy, cost, political factors).

'Skitter Map' By Peering

- IPv6 – less dense
- Europe centric



- IPv6?

Push the Stack

IPv4 Address Exhaustion

ByeBye v4 – We hardly got to know you

4.3B IPv4 addresses /8 = 16,777,216 addresses

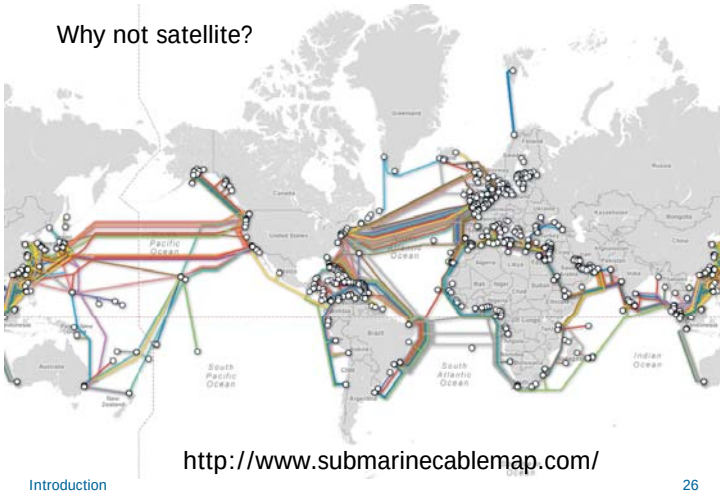
As of Jan 02, 2013

IANA Unallocated Address Pool Exhaustion: 03-Feb-2011

RIR	Proj. Exhaustion Date	Remaining /8 Pool (/8s)
APNIC:	19-Apr-2011 (actual)	0.8943
RIPE:	14-Sep-2012 (actual)	0.9467
ARIN:	03-Jun-2014	3.0083
LACNIC:	23-Sep-2014	2.8944
AFRINIC:	23-Mar-2021	3.8045

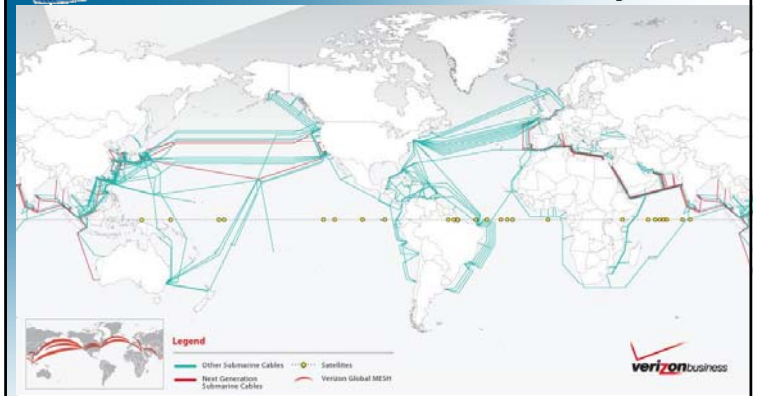
Global Connectivity

Why not satellite?



http://www.submarinecablemap.com/

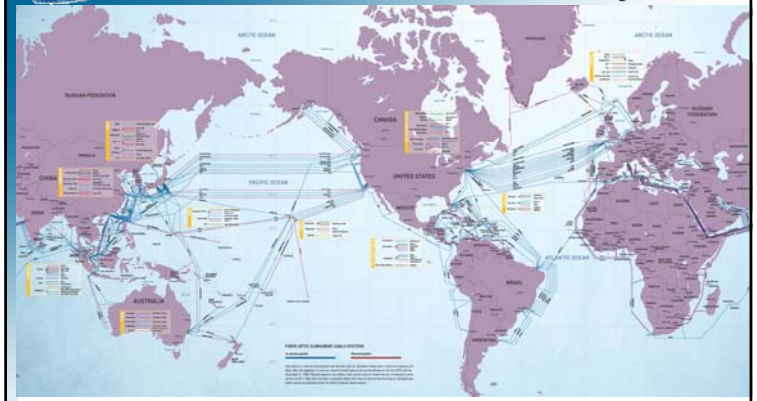
Verizon Undersea Cable Map



Note: Other = non-Verizon

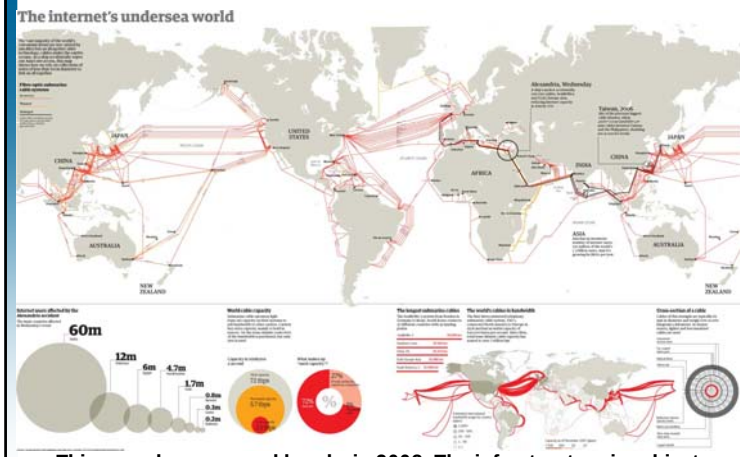
Verizon implies they have lots of undersea cables – but only the red are really theirs.

2009 Submarine Cable Map



Map shows who really owns the various undersea cables

By Undersea Cable Cuts



This map shows several breaks in 2008. The infrastructure is subject to accident – and attack.

Recent Cable Outages

August 27, 2012

- Cable between UK – Netherland breaks (anchor)

November 11, 2012

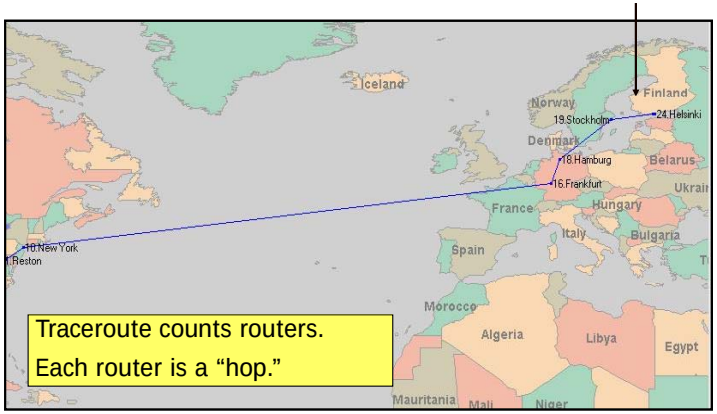
- Cable failure takes out 10% of Aus-N.Z. capacity

February 28, 2012

- 4 cables severed – Africa & Middle East impacted

Traceroute to Finland

24 Hops (Routers)



tracert in DOS

```
C:\Documents and Settings\Groo.MONARCH>tracert www.thepiratebay.org

Tracing route to www.thepiratebay.org [83.140.176.146]
over a maximum of 30 hops:

  1   655 ms   457 ms   573 ms  10.38.160.1
  2   366 ms   576 ms   859 ms  RDC-24-26-162-193.mn.rr.com [24.26.162.193]
  3   467 ms   634 ms   610 ms  srp0-1.mplsmn01-rtr2.mn.rr.com [24.26.162.2]
  4     *      487 ms   471 ms  so0-1-2.chcgil3-rtr1.kc.rr.com [24.94.160.13]
  5   463 ms   280 ms   301 ms  pop1-chi-P7-2.atdn.net [66.185.141.93]
  6   497 ms   421 ms   496 ms  Sprint.atdn.net [66.185.150.218]
  7   426 ms   284 ms   473 ms  sl-bb22-chi-2-0.sprintlink.net [144.232.20.20]
  8   379 ms   435 ms   361 ms  sl-bb24-chi-8-0.sprintlink.net [144.232.26.109]

  9   525 ms   442 ms   447 ms  sl-bb25-nyc-5-0.sprintlink.net [144.232.9.157]
 10   476 ms   565 ms   492 ms  sl-bb20-msq-2-0.sprintlink.net [144.232.20.74]
 11   586 ms   537 ms   616 ms  sl-bb21-msq-15-0.sprintlink.net [144.232.9.110]

 12   646 ms   585 ms   449 ms  sl-bb20-cop-14-0.sprintlink.net [144.232.19.30]

 13   526 ms   468 ms   365 ms  sl-bb21-cop-15-0.sprintlink.net [80.77.64.34]
 14   584 ms   420 ms   622 ms  sl-bb21-sto-14-0.sprintlink.net [213.206.129.34]

 15   557 ms   529 ms   594 ms  sl-gw10-sto-15-0.sprintlink.net [80.77.96.42]
 16   559 ms   575 ms   627 ms  80.77.101.2
 17   596 ms   500 ms   515 ms  hey.mpaa.and.apb.bite.my.shiny.metal.ass.thepira
tebay.org [83.140.176.146]

Trace complete.

C:\Documents and Settings\Groo.MONARCH>
```

Note: Deprecated

PAN, LAN, CAN, MAN, WAN

- **PAN** – Personal Area Network (piconet)
  - covers a few meters, telephones, PDA's
- **LAN** – Local Area Network
  - covers a small physical area, no leased circuits
- **CAN** – Campus Area Network
  - covers a limited geographical area, single entity
- **MAN** – Metropolitan Area Network
  - spans a city (~50km), optical backbone
- **WAN** –Wide Area Network
  - spans metropolitan, regional, or national boundaries, uses leased circuits

TCP/IP

Everything you absolutely positively must know about TCP/IP

TCP = Transport Control Protocol
UDP = User Datagram Protocol
IP = Internet Protocol

TCP and IP control the vast majority of traffic that moves over the Internet!

A Brief Review

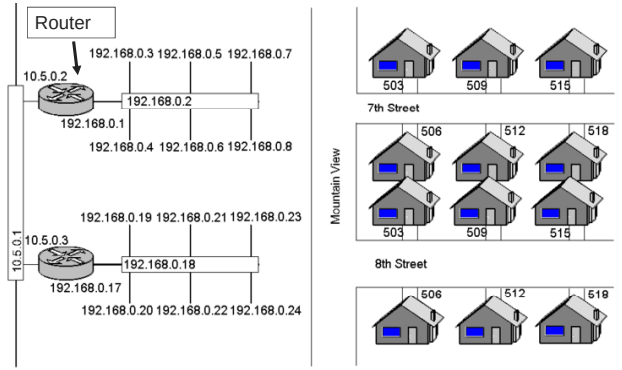
TCP/IP

Internet Addressing - it's all about: **IP = Internet Protocol**

IP Addresses and Port Numbers

- **IP Address**: Identifies your network and your computer. Every computer that uses the Internet must have a unique IP address.
- **Port Number**: Identifies your application (or "service"). Every application (e.g. browser, email) that uses the Internet must have a port number.
- **COMPARE**: It's like a Post Office that delivers only post cards. All messages are broken up into numbered post cards (packets), each sent to an address (IP address) and a person at that address (port number). **Every packet is labeled with a TO & FROM IP address and TO & FROM port number.**

IP Addresses



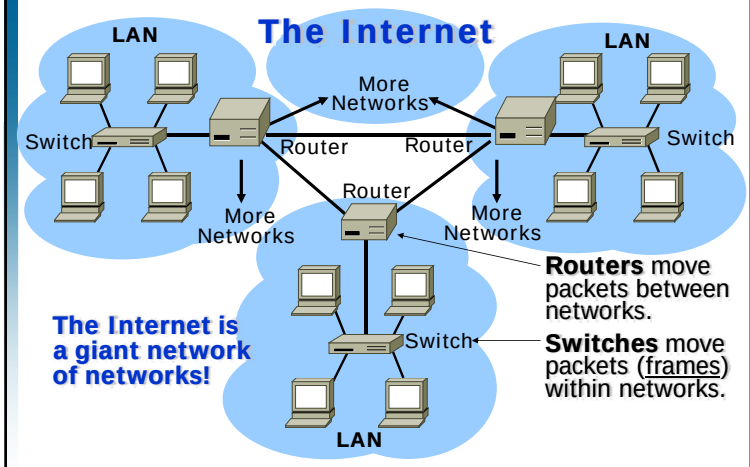
IP Addresses are similar to neighborhood addresses

IP Addresses

IP Addresses- Identify networks and computers

- IPv4 (version 4) is current (IPv6 is next)
- IPv4 addresses are 32 bits long (four 8-bit bytes)
- IPv4 max. 2^{31} (4,294,967,296) addresses
- Displayed in 4-byte "dotted decimal" form (quad)
- Addresses range from 0.0.0.0 to 255.255.255.255.
- A decimal byte ranges from 0 to 255 (11111111)
- Therefore, the IP address 192.200.5.130 is really:
  11000000 11001000 00000101 10000010
  (spaces added for clarity)
- Are part network address, part computer address
- Routers move packets based on their IP addresses
- aka Dotted Quad

Internet Collective



Non-Routable Addresses

- Non-routable IPv4 addresses
  - 10.0.0.0 – 10.255.255.255 10/8
  - 172.16.0.0 – 172.31.255.255 172.16/12
  - 192.168.0.0 – 192.168.255.255 192.168/16
  - Internet routers ***should*** drop packets addressed to these address spaces; can be used in labs and LANs without fear of packets "escaping" into the Internet
- Routable IPv4 addresses - plus
  - Every address that is **not non**-routable

```
martians = "{ 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, \
             10.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, \
             0.0.0.0/8, 240.0.0.0/4 }"
```


Port Numbers

Identify applications (services)

- Port numbers are 16 bits long.
- Device can have up to 2^{16} (65,536) port numbers
- They are always displayed in decimal form.
- Addresses range from 0 to 65,535.
- 0 to 1023 = server application port numbers.

- 1024 to 65,535 = client application port numbers.
- Client apps are browsers, email programs, etc.
- Therefore, the port number 80 (web site) is really:
  0000 0000 0101 0000
  (spaces added for clarity)

Server Port Numbers

Server application port numbers (0 to 1023)

- 21 – ftp (file transfer protocol)
- 22 – ssh (secure shell)
- 23 – telnet (remote login)
- 25 – smtp (simple mail transport protocol)
- 53 – dns (domain name service)
- 69 – tftp (trivial file transfer protocol)
- 80 – http (hypertext transfer protocol - web pages)
- 110 – pop3 (post office protocol)
- 135, 139, 445 – netbios (network basic input output system - printer/file sharing)
- 443 – https (encrypted web pages; s = secure)

Server apps are web servers, email servers, etc.
Servers listen, clients connect, then the two talk

Server Port Numbers

7	tcp/udp	echo	
17	tcp/udp	qotd	quote of the day
19	tcp/udp	chargen	character generator
79	tcp/udp	finger	
194	tcp/udp	irc	internet relay chat

And many obscure/deprecated/??? port numbers

398	kryptolan
416	silverplatter
460	skronk

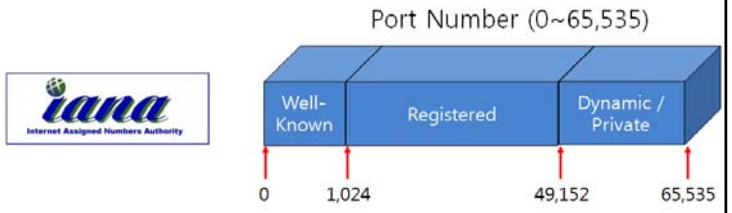
We will revisit these soon

Port Numbers

Assigned by IANA: Internet Assigned Numbers Authority

0–1023	the Well Known Ports
1024–49151	the Registered Ports
49152–65535	Dynamic and/or Private Ports

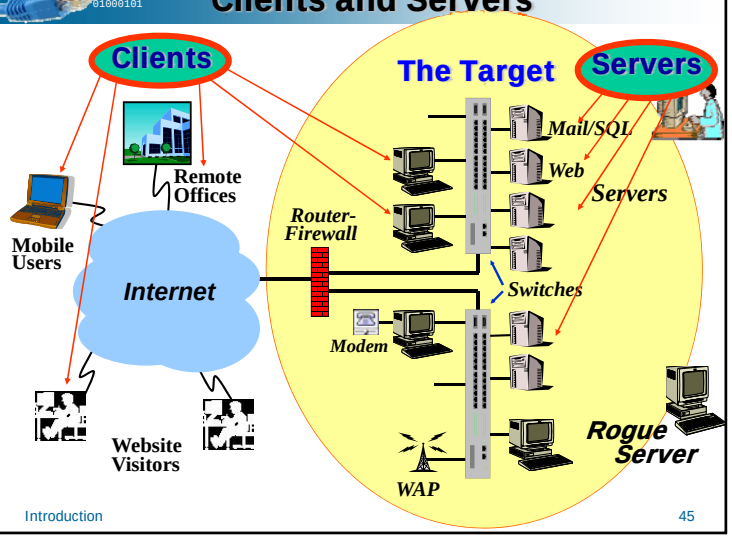
Well Known ports SHOULD NOT be used without IANA registration
Registered ports SHOULD NOT be used without IANA registration



Risky Protocols

- **Most Microsoft LAN exploits take advantage of the following protocols in some way:**
- NetBIOS (TCP Ports 137, 138, 139) – used by Windows networking to connect clients to file and print servers. Should never be allowed through the Firewall except through an encrypted tunnel (as in a VPN)
- RPC Locator (TCP Port 135) – used by Windows networking to locate network services that use the RPC protocol. Should never be allowed through the Firewall

Clients and Servers



LAN (MAC) Addresses

- Every NIC (Network Interface Card) has a **unique** address called the **MAC** (Media Access Control) address.
- MAC vs. IP: It's like a housing community that delivers mail based on lot number vs. the world-based postal address.
- MAC addresses (48 bits) are given in **hexadecimal**. Hexadecimal represents binary numbers in 4-bit groups:

0000 = 0	0100 = 4	1000 = 8	1100 = C
0001 = 1	0101 = 5	1001 = 9	1101 = D
0010 = 2	0110 = 6	1010 = A	1110 = E
0011 = 3	0111 = 7	1011 = B	1111 = F

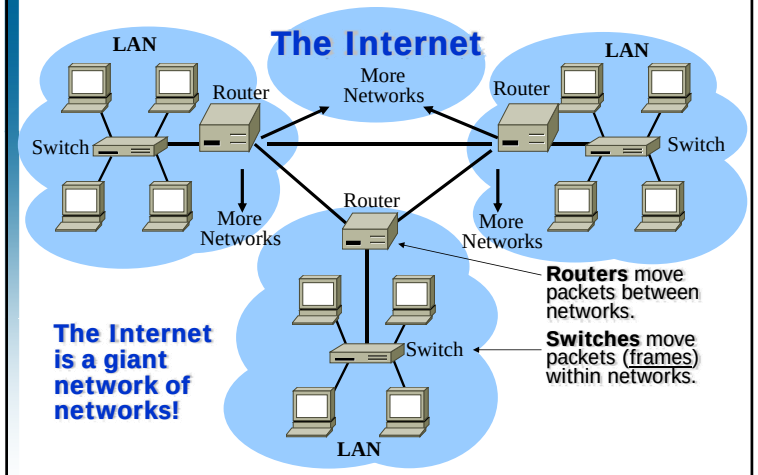
- An example MAC address is: **00-0E-35-56-60-FA**

  0000 0000 0000 1110 0011 0101 0101 0110 0110 0000 1111 1010
- The first 24 bits (00-0E-35) identifies the manufacturer. The second 24 bits (56-60-FA) represents the NIC card. **Q: What help is that?**
- ***Switches move packets based on their MAC addresses***

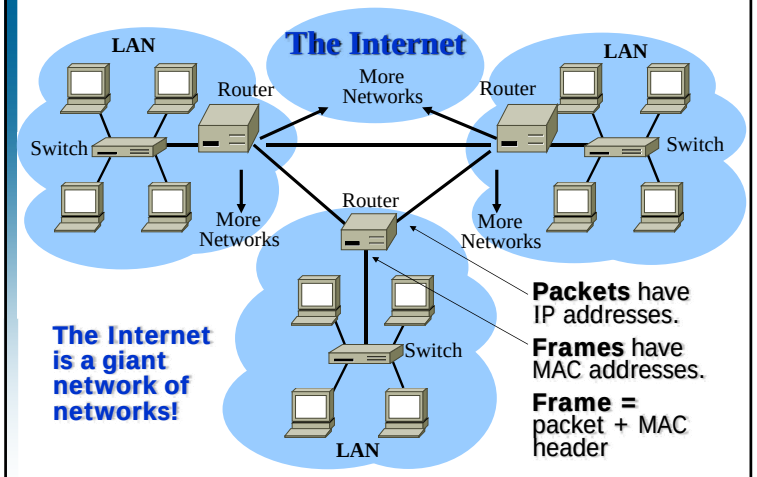
Address Summary

- ***Every computer*** connected to the Internet must have a unique **IP address (Routing, NAT)**
  - Devices get address from an ISP or DHCP
- ***Every program*** that communicates over the Internet must have a unique (to the computer) **port number**.
  - Most services (web, email, etc.) have an assigned port number (web servers use port 80).
- ***Every computer*** on a LAN (whether the LAN is connected to the Internet or not) must have a unique **MAC address**.

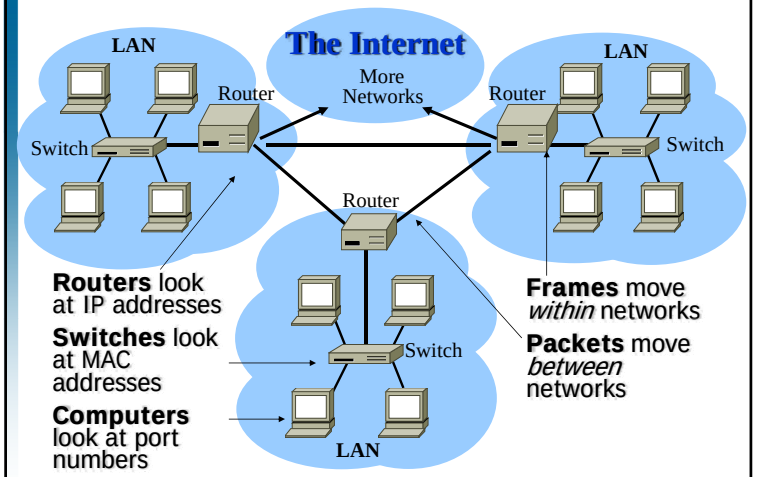
Internetwork aka The Net



The Internet

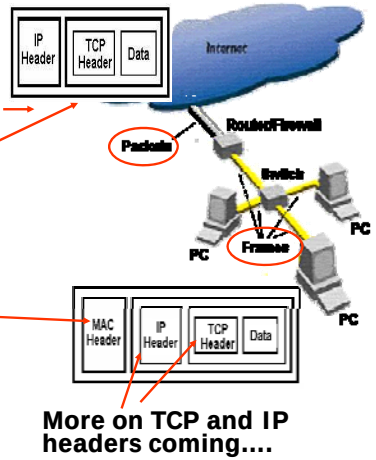


The Internet



Packets & Frames

- **Packets travel the Internet**
  - Every packet has 32-bit TO/FROM **IP** addresses
  - And 16-bit TO/FROM port numbers
- **Frames travel LANs**
  - Every frame has 48-bit TO/FROM **MAC** addresses



More on TCP and IP headers coming....

Internet Sockets

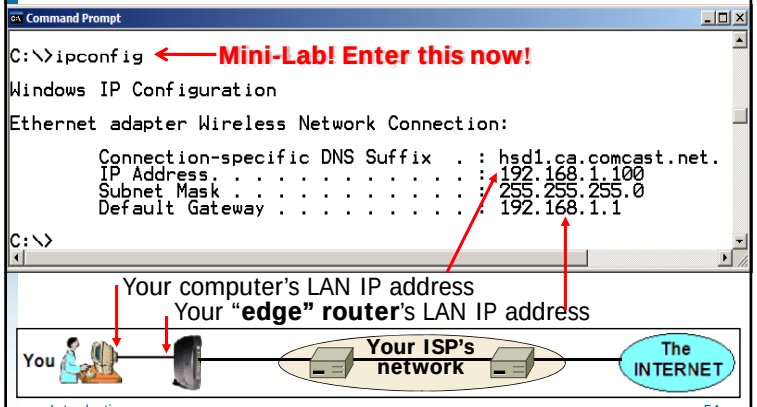
- Socket – coding term for a TCP/IP stack API
  - A socket is an IP address/Port number pair
  - A connection between an application and the TCP/IP stack
  - An endpoint of a bi-directional inter-process communication flow across the Internet
- An attacker who "owns" a remote box, will have his attack code open a socket on the victim box. This socket connects to a socket on attacker's box – or vice versa

Servers

- Nothing moves over the Internet unless there is a connection through which it flows.
- All connections start with a server listening
  - We call this an open port
- Therefore, if a box has no open ports, it is invulnerable to a (direct) remote attack! Well, sort of…
- An attacker's only options are (1) human access (e.g. send the human a Trojan email attachment or trick him into visiting your website) or (2) physical access.
- If you are running a Peer-to-Peer service (AIM, ICQ, ~~Napster~~, ~~Kazaa~~, ~~Morpheus~~, ~~Limewire~~, eMule, BitTorrent, etc.), your computer is a server!
- If you are running Windows, your computer is a server, but this generally only makes you vulnerable to insider attacks.

What's My IP Address?

Use **ifconfig** (Linux) **ipconfig** (in a DOS window) to determine computer's IP address, and the "inside" IP address of your "edge" router

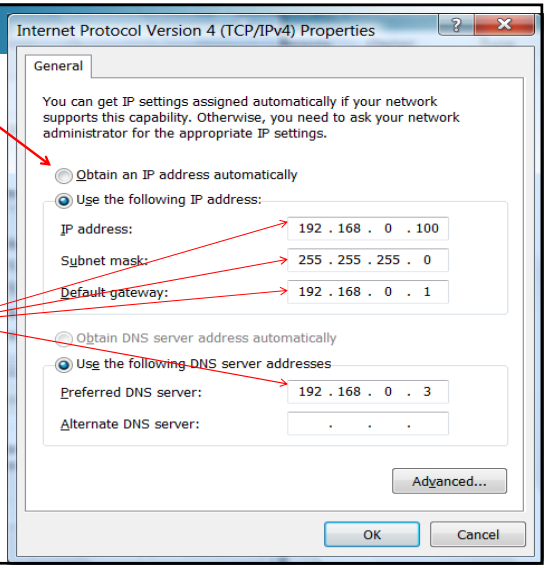


DHCP = Dynamic Host Configuration Protocol

When the client boots, it asks a DHCP server for these values

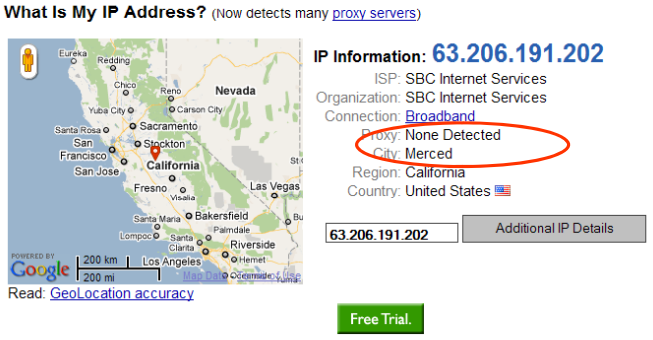
Otherwise, **you** set them yourselves

A **static** IP



Gateway IP Address

Use **whatismyipaddress.com/** to find out what the world sees as your "outside" IP address. This could be a cable modem, a DSL modem, etc.



What Ports Are Open?

Use **netstat –an** to find out what ports are open on your machine (a= all, n= numbers only, do not determine the services associated with port numbers).

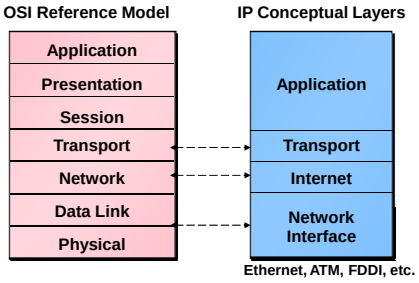
```
Command Prompt
C:\>netstat -an        <-- Mini-Lab! Enter this NOW!

Active Connections     You're listening, so you're a server

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1241         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:62514        0.0.0.0:0              LISTENING
  TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.100:2869     192.168.1.1:1186       CLOSE_WAIT
  TCP    192.168.1.100:4972     66.102.7.99:80         ESTABLISHED
  TCP    192.168.1.100:12226    0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*

                                IP address
                                Port number
```

Introduction **IP addresses** 57

```
Command Prompt
C:\Documents and Settings\Name>ipconfig /all

Windows IP Configuration        <-- Mini-Lab! Enter this NOW!

        Host Name . . . . . . . . . . . . : K1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : dc.dc.cox.net

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 220
Connection
        Physical Address. . . . . . . . . : 00-0E-35-05-60-6E

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dc.dc.cox.net
        Description . . . . . . . . . . . : Realtek RTL8139/810x Fami
ernet NIC
        Physical Address. . . . . . . . . : 00-00-F0-7E-F1-42
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 68.100.160.199
        Subnet Mask . . . . . . . . . . . : 255.255.248.0
        Default Gateway . . . . . . . . . : 68.100.160.1
        DHCP Server . . . . . . . . . . . : 172.19.105.16
        DNS Servers . . . . . . . . . . . : 68.100.16.25
```

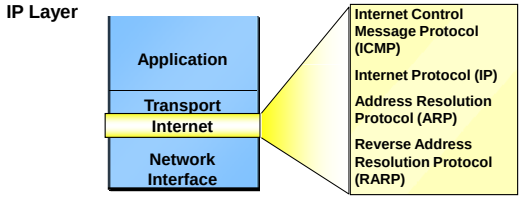
ISO OSI Model

The TCP/IP Protocol Stack



Introduction 59

The Internet Layer



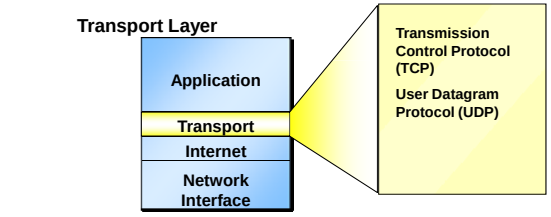
IP Datagram

VERS	HLEN	Type of Service	Total Length	ID	Flags	Frag Offset	TTL

Protocol	Header Checksum	Src IP Address	Dst IP Address	IP Options	Data

Introduction 60

The Transport Layer



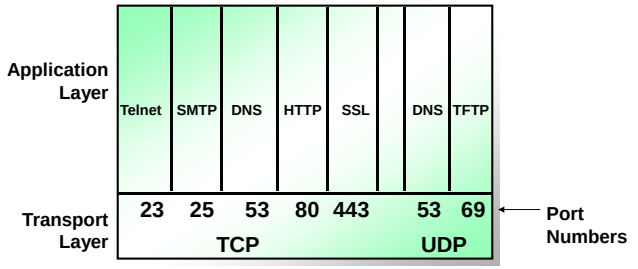
TCP Segment Format

Src Port	Dst Port	Seq #	Ack #	HLEN	Reserved	Code Bits	Window	Check Sum	Urgent Ptr	Option	Data

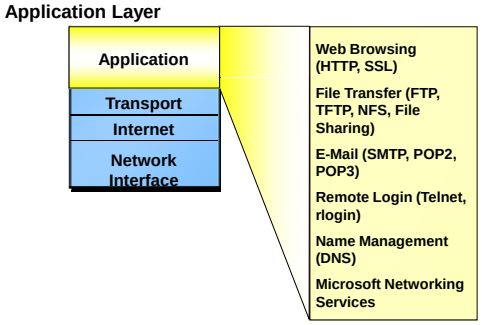
UDP Segment Format

Src Port	Dst Port	Length	Check Sum	Data

Port Numbers



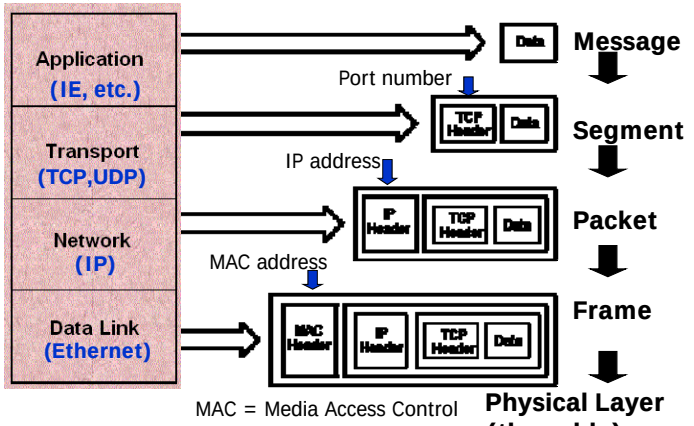
Application Layer



"It's a layer 8 problem" = clueless User/Management

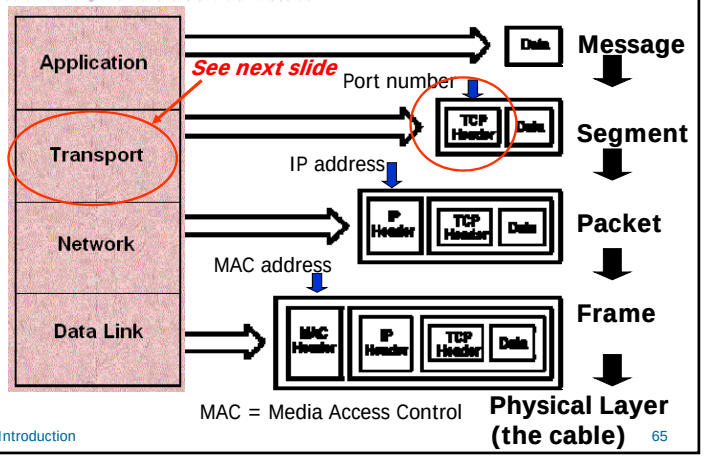
Data Flow

The TCP/IP Protocol Stack



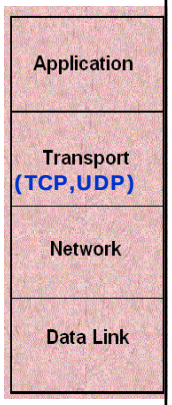
Data Flow

The TCP/IP Protocol Stack



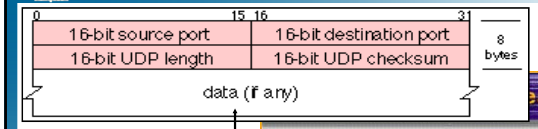
Transport Layer

- The Transport Layer is responsible for program-to-program communication (therefore, it uses port numbers)
- In TCP/IP there are two Transport Layer protocols:
- The Transport Control Protocol (TCP) guarantees that information is received as it was sent – it's connection-oriented
- The User Datagram Protocol (UDP) performs no end-to-end reliability checks – it's connectionless



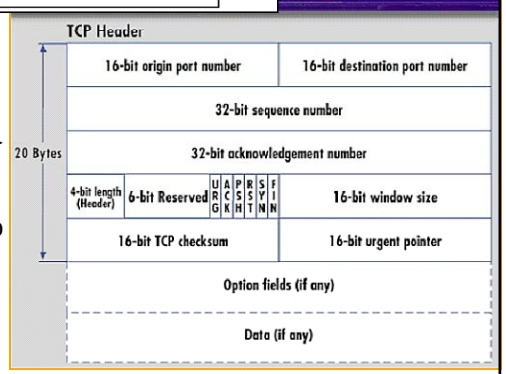
Let's look at the TCP and UDP headers….

Headers

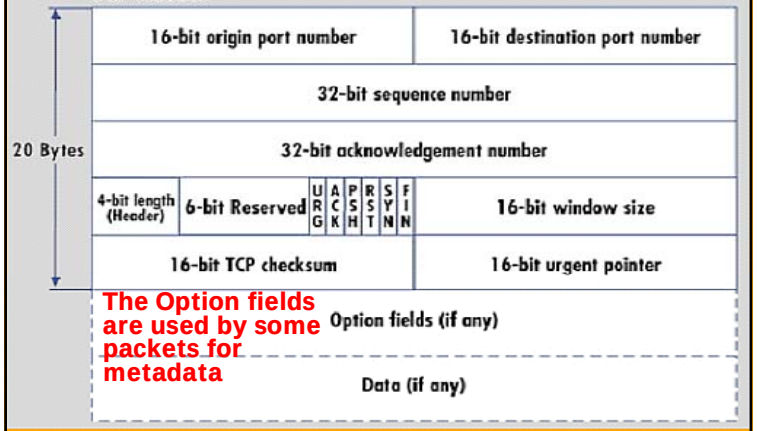


The UDP Header

- Compare this header with the **TCP header**
- What's added?
- What can TCP do that UDP *cannot* do?
  - **Be reliable!**
- What can UDP do?



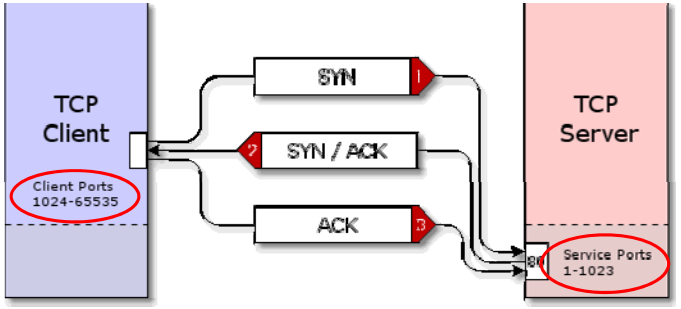
TCP Header



The Option fields are used by some packets for metadata

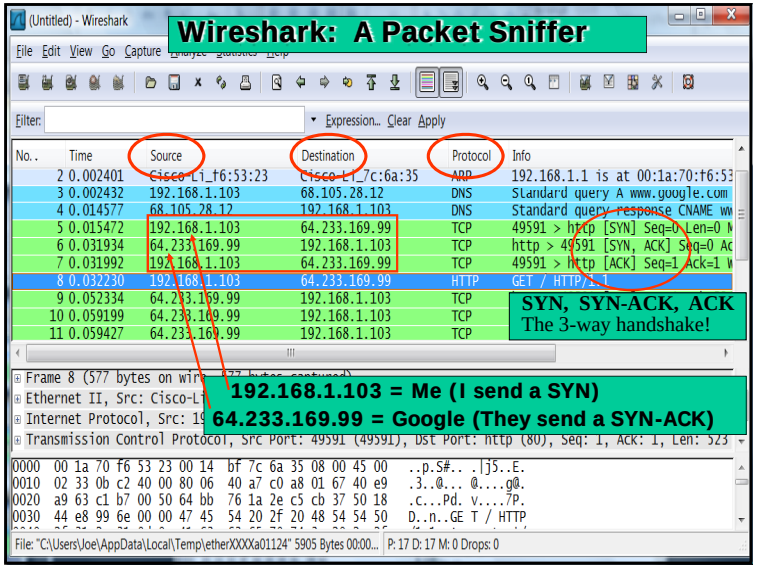
3-Way Handshake

Since TCP is connection-oriented, it requires a 3-way handshake to get started (notice the reserved port numbers)



Introduction 69

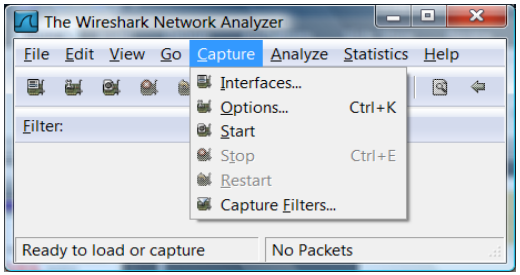
Wireshark: A Packet Sniffer



Wireshark

Using Wireshark to see the 3-way handshake

- Run Wireshark.
  - Click on the desktop icon or…
  - Click on Start/All Programs/Wireshark/Wireshark.
- Select Capture/Interfaces (*see next slide*).

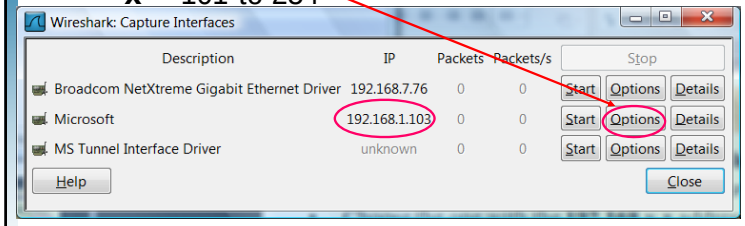


Introduction 71

Wireshark

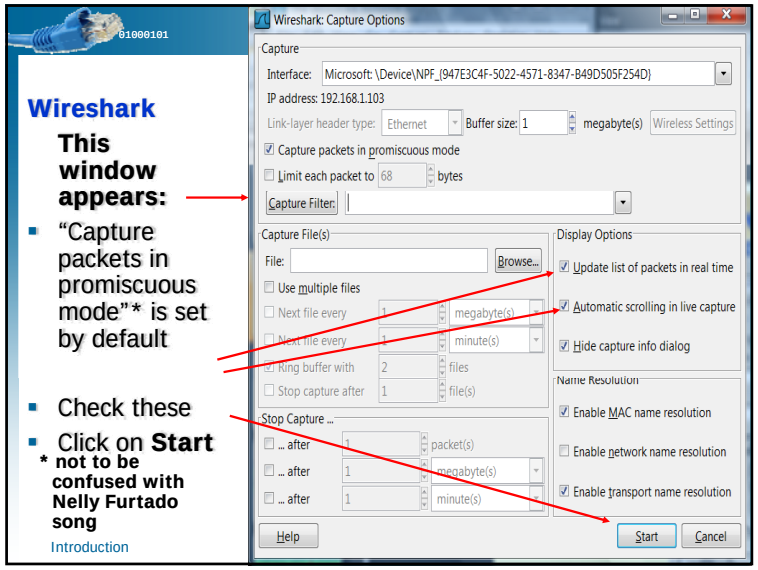
Using Wireshark to see the 3-way handshake

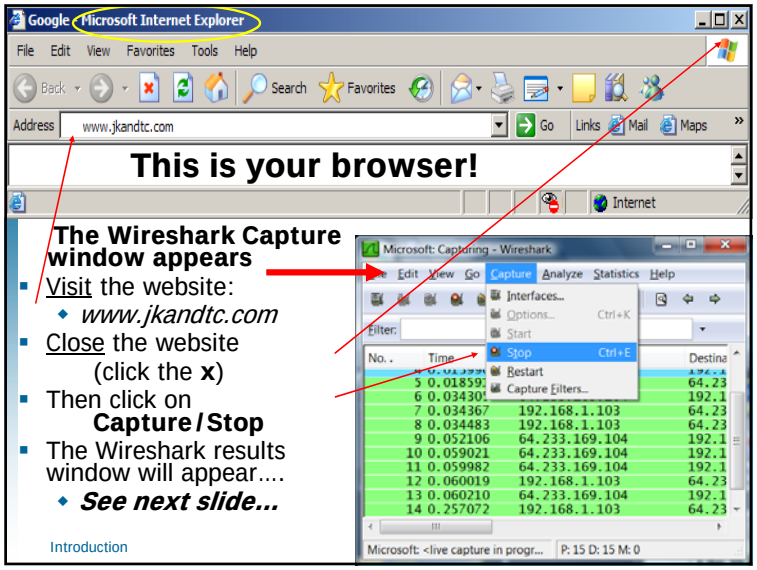
- *The names of the network interfaces will vary!*
- Select the interface you want
- Click on the **Options** for that interface
  - **x** = 101 to 254

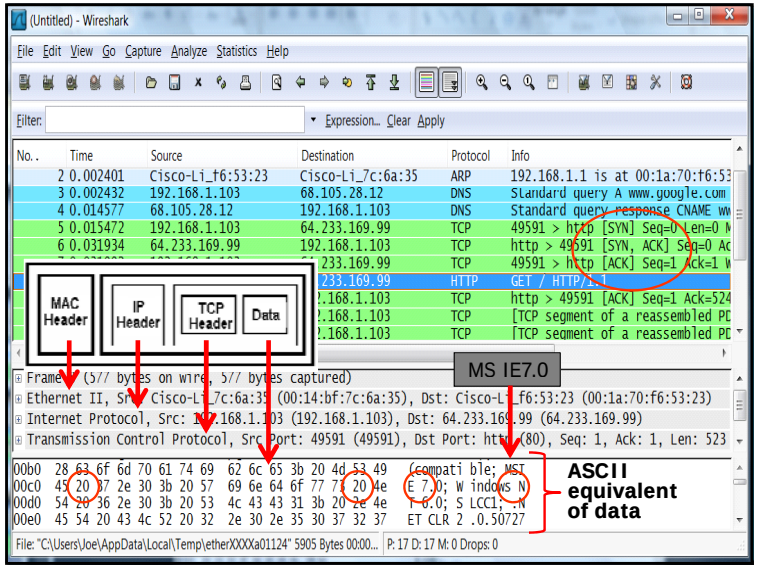


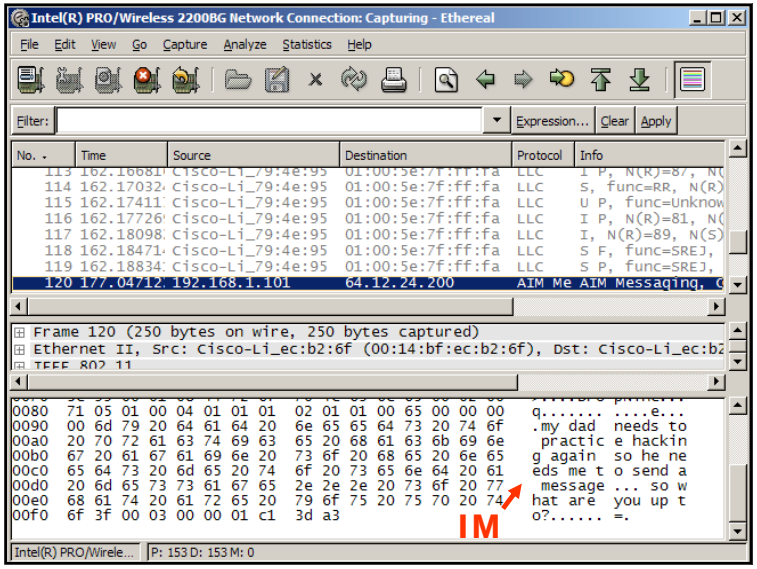
NOTE: Wireshark works on most wireless LANs!

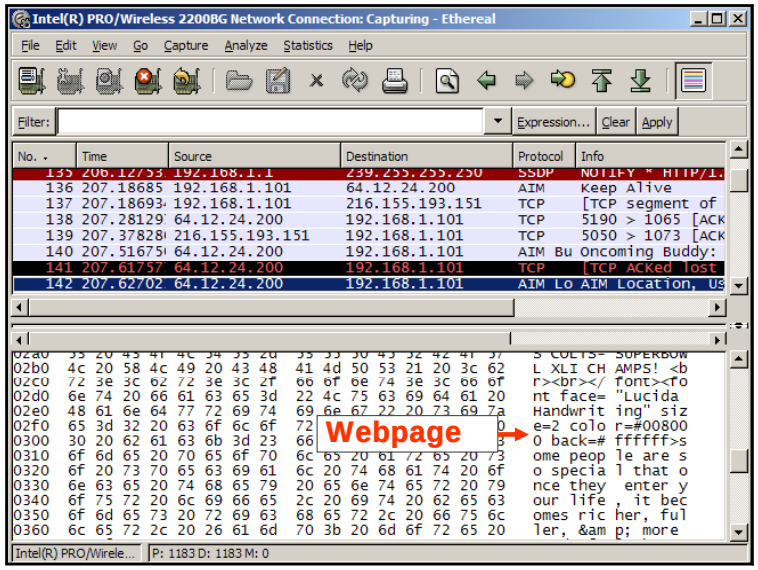
Introduction 72


Wireshark
This window appears:
"Capture packets in promiscuous mode"* is set by default
Check these
Click on Start
* not to be confused with Nelly Furtado song
Introduction
Wireshark: Capture Options
Capture
Interface: Microsoft: \Device\NPF_{947E3C4F-5022-4571-8347-B49D505F254D}
IP address: 192.168.1.103
Capture packets in promiscuous mode
Limit each packet to 68 bytes
Capture Filter:
Capture File(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Stop Capture ...
Help
Start
Cancel


Google - Microsoft Internet Explorer
This is your browser!
The Wireshark Capture window appears
Visit the website:
www.jkandtc.com
Close the website (click the x)
Then click on Capture / Stop
The Wireshark results window will appear....
See next slide...
Introduction
Microsoft: Capturing - Wireshark
Interfaces...
Options... Ctrl+K
Start
Stop Ctrl+E
Restart
Capture Filters...


(Untitled) - Wireshark
MAC Header
IP Header
TCP Header
Data
MS IE7.0
ASCII equivalent of data


Intel(R) PRO/Wireless 2200BG Network Connection: Capturing - Ethereal
IM



Wireshark Fluency

- Packet captures as a diagnostic tool
- Most tickets for network problems – are wrong
  - Configuration error (Wrong Interface or port)
  - Programming error
  - Version errors (DLL's)
  - External site is offline
  - Permissions/Credential error
  - Infected host
  - ID10T error (Typo, Power button off)
  - **Learn to Use Wireshark**
  - **What happens on your computer?**

Networking Lab

Networking Review Labs

- DOS & CLI review- find the SAM
- ipconfig & netstat- get ip address, mac, open ports
- Linux review lab

Initial Security Labs

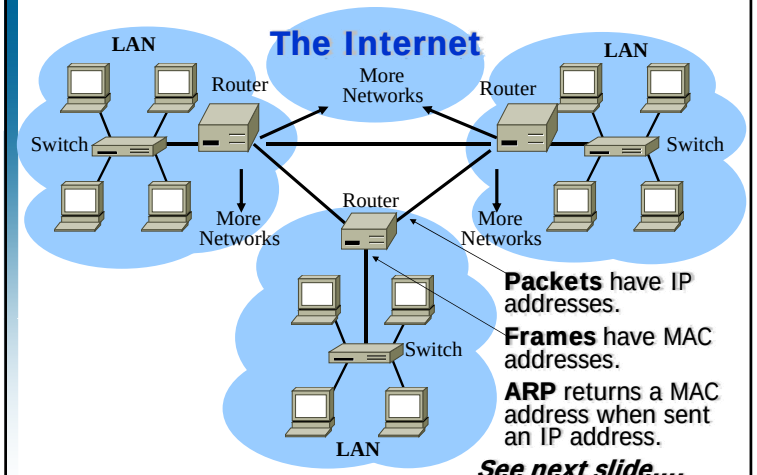
- wireshark – packet capture, decode
- Sysinternals – malware recovery (Windows)
- Google Hacking – GIYF (homework)

First Lab That Can Bite

- Shodan (homework)

Note: labs and order subject to change

Address Resolution Protocol



Packets have IP addresses.

Frames have MAC addresses.

ARP returns a MAC address when sent an IP address.

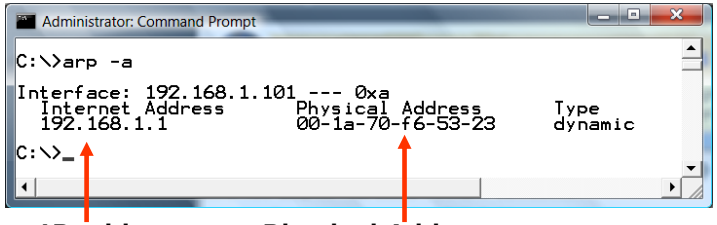
See next slide....

Address Resolution Protocol

- ARP maps IP addresses to LAN MAC addresses.
- Ethernet LAN applications need MAC addresses, not IP addresses, to connect to a host on a LAN.
- MAC vs. IP: Local vs Global Address
- When an application (or edge router) knows only the IP address of the destination. Solution: ARP
- 192.168.0.23 = 00-0E-35-56-60-FA
- This will be an important concept later, when we talk about ARP cache poisoning!
- Wireshark will show you ARP packets

Address Resolution Protocol

In DOS, to view (all of) the ARP cache, enter:
`arp -a`



IP address **Physical Address = MAC address = NIC address**

An ARP announcement (also known as "Gratuitous ARP") is usually an ARP Request sent to update the arp caches of hosts that receive it.

Mini-Lab: ARP

1. **Open a DOS window.**
2. **Get your IP address:**
   > ipconfig
3. **Share your IP address with your neighbors.**
4. **Ping your neighbors. For example, Enter:**
   > ping 192.168.0.100
   > ping 192.168.0.101 **Examples only!**
   > ping 192.168.0.102
4. **Your neighbors' computers will respond with echo frames that include their MAC address as well as IP addresses, thus populating your ARP table.**
5. **Now Enter:**
   > arp –a ← See the IP address/MAC address pairs

NAT (Network Address Translation)

- An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box (often the edge router) located where the LAN meets the Internet makes all necessary IP address translations.
- NAT serves two main purposes:
- Enables a company to use more internal IP addresses. Since they're only used internally, there's no possibility of conflict with IP addresses used by other companies and organizations.
- Provides a type of firewall by hiding internal IP addresses, leaving web & mail servers, etc., visible to the world.
- Most NAT is really PAT – Port address translation

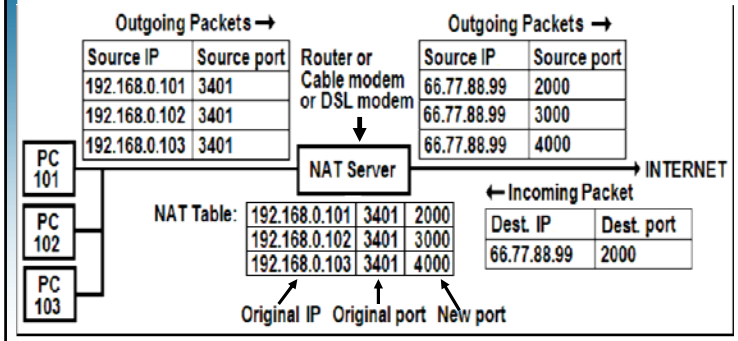
NAT

NAT (Network Address Translation)

All of the PCs share the one routable IP address: 66.77.88.99

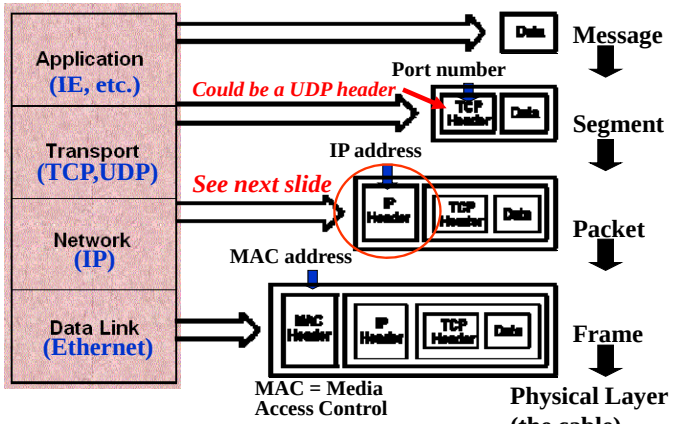
By coincidence, they all chose the same random source port.

The non-routable IP addresses (192.168.0.x) cannot be scanned!

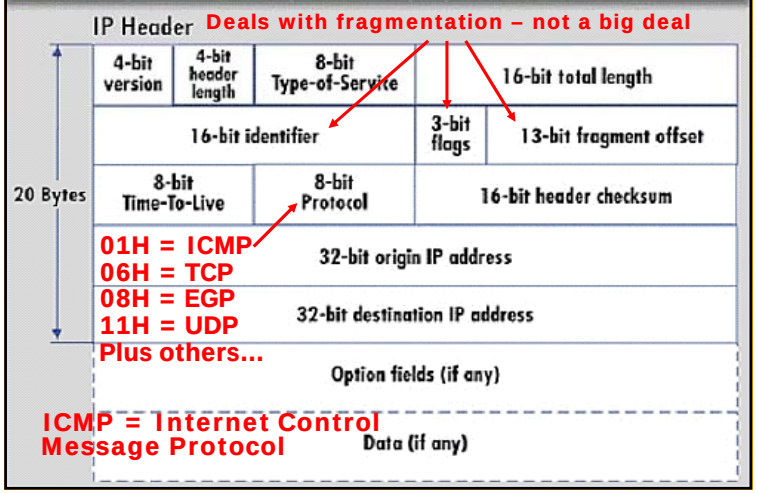


Headers

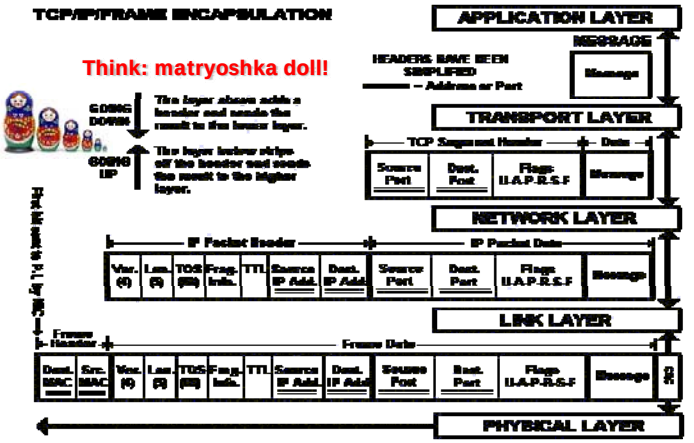
TCP/IP Protocol Stack



IP Header



ENCAPSULATION



Fragmentation Happens

MTU (Maximum transmission unit in a frame)

RFC 791 says the maximum MTU is 65,535 min is 68.
Ethernet = 1500 802.3 = 1492
Fragmentation only occurs on the data portion of the packet
Fragmentation must occur on an 8 byte boundary

If you have an ATM backbone - 53 byte packets (48 payload)
- then an MTU of 1488 can save 3% bandwidth

Jabber is the transmission of a packet larger than network MTU,
Usually from faulty hardware

ping -f (don't set fragment size) -l size (send buffer size)
can be used to determine optimal MTU size.

16-bit header checksum - is just that - header only

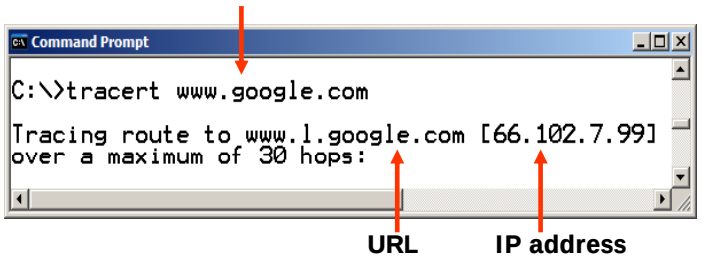
DNS – Domain Name Service

- Similar to the way ARP maps IP addresses to LAN MAC addresses, DNS maps URLs (Uniform Resource Locator) to IP addresses.
- Ethernet LAN applications need MAC addresses, not IP addresses, to connect to a host on a LAN.
- Browsers need IP addresses (e.g. 64.233.161.99), not URLs (e.g. www.google.com) to connect to a website.
- www.google.com = 64.233.161.99
- ***More when we cover DNS attacks***

DNS – Domain Name Service

Converts the URL entered into an **Address** field into an IP address

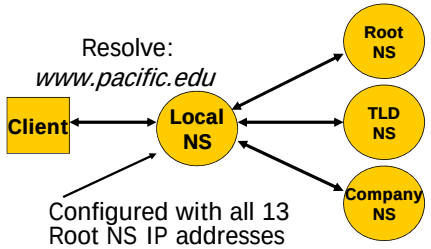
- This is the DOS ***traceroute*** command



The tracert program made a DNS request!

DNS – Domain Name Service

- Converts URLs (*www.uop.edu*) into IP addresses – requesting the conversion from DNS servers
- DNS servers query each other to resolve names into addresses
- To lower traffic, DNS servers cache answers



Each root NS stores IP addresses of 100s of TLD NSs

Top Level Domain name servers, e.g. .com, .edu, .net

Local **authoritative** name servers, e.g. cs.pacific.edu

IP Spoofing

- Any host can send packets pretending to be from any IP address
- Replies will be routed to the appropriate subnet
- Route asymmetry
- Attacker will not get replies if not on same subnet
- For some attacks this is not important

Analogy

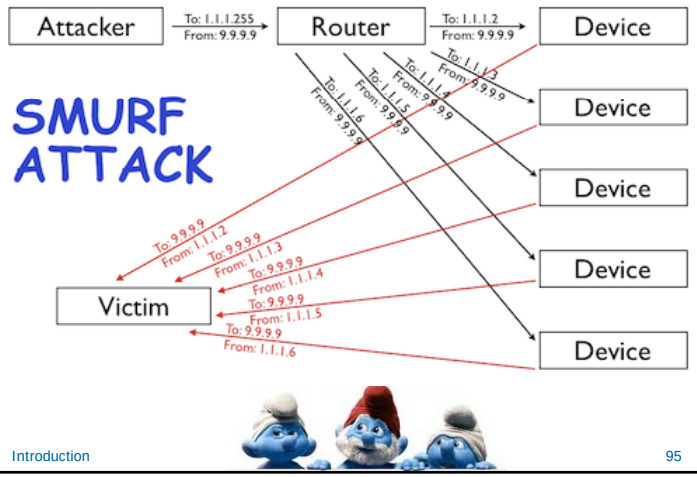
- Nothing prevents you from sending a letter with an invalid return address, or someone else's
- Likewise, packets can be inserted in the network with invalid or other IP addresses

IP Spoofing With Amplification

- Use broadcasts claiming to originate from victim
- All replies go back to victim
- Class B broadcast: 253^2 = 64,009 replies
  - Assuming class C subnetting
- This may use any IP protocol (ICMP, TCP, UDP)
- Any application/service that replies using these protocols
- Famous attack: Smurf (using ICMP) DoS

- Cisco IOS 12.0 + no ip directed-broadcast
- Directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast

Smurf



Smurf/Fraggle

- Ping a broadcast address
  - with spoofed IP of a victim as source address
- All hosts on the network respond to the victim
  - The victim is overwhelmed

- A protocol vulnerability - patched by violating the protocol specification (e.g. to ignore pings to broadcast addresses)
- ICMP echo just used for convenience
- All ICMP messages can be abused this way
- Fraggle is the UDP equivalent
- Traffic aimed at ports 7 (echo) and 19 (chargen)

Spoofing Defense

- Ingress filtering
  - Forbid inbound broadcasts from internet
  - Forbid inbound packets from non-routable networks
- Egress filtering
  - Prevent hosts in your network from spoofing IPs from other networks by dropping their outbound packets
  - Drop outbound broadcasts
- Make your network a less attractive/useful target for attackers that want to launch other attacks
- Be a good internet citizen (reputation is important)

RFC 2267

TCP / IP Packets

Let's look at a real Internet packet…

At 05:30 UTC on January 25, 2003, a single UDP packet with destination port 1434 appeared on a MS Windows computer running SQL server and look like a request to find a database. The request should have been 16 bytes and ended with a 00. It didn't - and caused a buffer overflow, and the remainder of the packet overwrites the stack. The reprogrammed stack generates a random IP address and points to its own code to send. This process loops, creating a stream of exploit code.

The Slammer Packet

```
4500  0194  aa13  0000  0111  386d  c0e4  8b2f
e2b9  a70b  0408  059a  0180  5b6a  0401  0101
0101  0101  0101  0101  0101  0101  0101  0101
0101  0101  0101  0101  0101  0101  0101  0101
0101  0101  0101  0101  0101  0101  0101  0101
0101  0101  0101  0101  0101  0101  0101  0101
0101  0101  0101  0101  0101  0101  0101  0101
0101  0101  0101  0101  0101  0101  01dc  c9b0
42eb  0e01  0101  0101  0101  70ae  4201  70ae
4290  9090  9090  9090  9068  dcc9  b042  b801
0101  0131  c9b1  1850  e2fd  3501  0101  0550
89e5  5168  2e64  6c6c  6865  6c33  3268  6b65
726e  5168  6f75  6e74  6869  636b  4368  4765
7454  66b9  6c6c  5168  3332  2e64  6877  7332
5f66  b965  7451  6873  6f63  6b66  b974  6f51
6873  656e  64be  1810  ae42  8d45  d450  ff16
508d  45e0  508d  45f0  50ff  1650  be10  10ae
428b  1e8b  033d  558b  ec51  7405  be1c  10ae
42ff  16ff  d031  c951  5150  81f1  0301  049b
81f1  0101  0101  518d  45cc  508b  45c0  50ff
166a  116a  026a  02ff  d050  8d45  c450  8b45
c050  ff16  89c6  09db  81f3  3c61  d9ff  8b45
b48d  0c40  8d14  88c1  e204  01c2  c1e2  0829
c28d  0490  01d8  8945  b46a  108d  45b0  5031
c951  6681  f178  0151  8d45  0350  8b45  ac50
ffd6  ebca  0000
```

20-byte IP Header

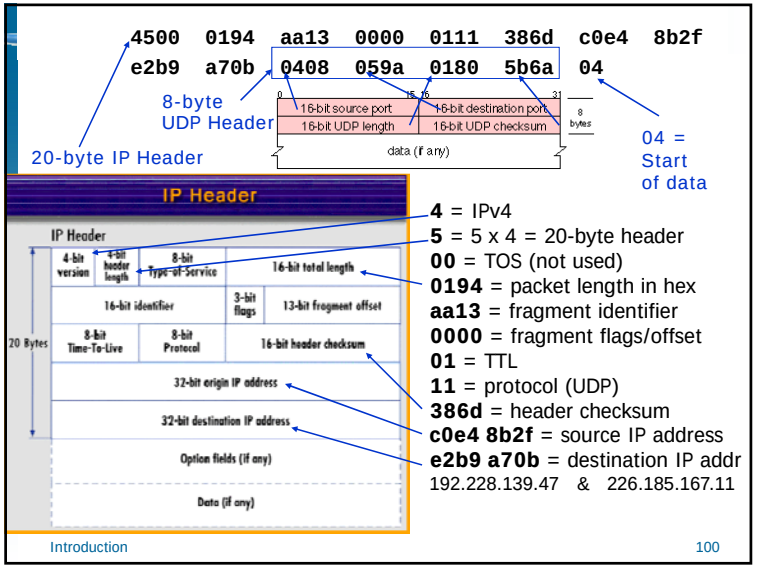
8-byte UDP Header

0101… overflows a buffer

04 = Start of data

It's all really just 1s and 0s!

Note that the packet is terminated with a 00 byte (NULL character)



4 = IPv4
5 = 5 x 4 = 20-byte header
00 = TOS (not used)
0194 = packet length in hex
aa13 = fragment identifier
0000 = fragment flags/offset
01 = TTL
11 = protocol (UDP)
386d = header checksum
c0e4 8b2f = source IP address
e2b9 a70b = destination IP addr
192.228.139.47 & 226.185.167.11

Slammer – One Freaking Packet

Was the fastest computer worm in history
Code Red/others needed a connection - latency slowed spread
As it began spreading it doubled in size every 8.5 sec.
Infected more than 90 percent of vulnerable hosts within 10 minutes
Targeted MS SQL Server/Desktop engine (XP Pro, Visio, VStudio)
55 million scans per second after 3 minutes
Scanner/worm total size 376 bytes + headers = 404 byte UDP packet
The scanning clogged circuits and overloaded routers
BofA's 13,000 ATMs were down
Continental Airlines canceled airline flights, flight delays
Microsoft patches were inaccessible
911 service disruptions
5 root servers disrupted
Countries lost Internet service for up to a day
Slammer packets are still seen on the Internet today

Structured Attacks

- Most attacks are after something, and use more efficient approaches.
- The initial step: **research**
  - Survey - gather information (“ID” the box)
  - Physical access (insider assistance, supply chain, breakin)
  - Human access (social engineering)
  - LAN access (insider assistance)
  - Remote access (Nmap, Nessus, custom tools)
  - Purchase/trade desired information (new way)

Structured Attacks

The followup step: **exploit**

- Infiltration, stealthy storage
- Maintain access, persistence
- Cover tracks
- Collection
- Exfiltration (getting data out)

Preventing exfiltration is a growing vendorspace

- **DLP** Data Loss Prevention
- Whether in use, motion, or at rest
- Using Deep Content Inspection