Welcome

You are at: INTERNET/networking/safe computing

- PDF of slides is at:
  - http://johnloop.com:808/pccitizen_course/pccitizen_course.pdf
- Open Office “Impress” format slides are at
  - http://johnloop.com:808/pccitizen_course/pccitizen_course.odp
- Microsoft PowerPoint format slides are at
  - http://johnloop.com:808/pccitizen_course/pccitizen_course.ppt

...This is a vast subject, how much can we cover?

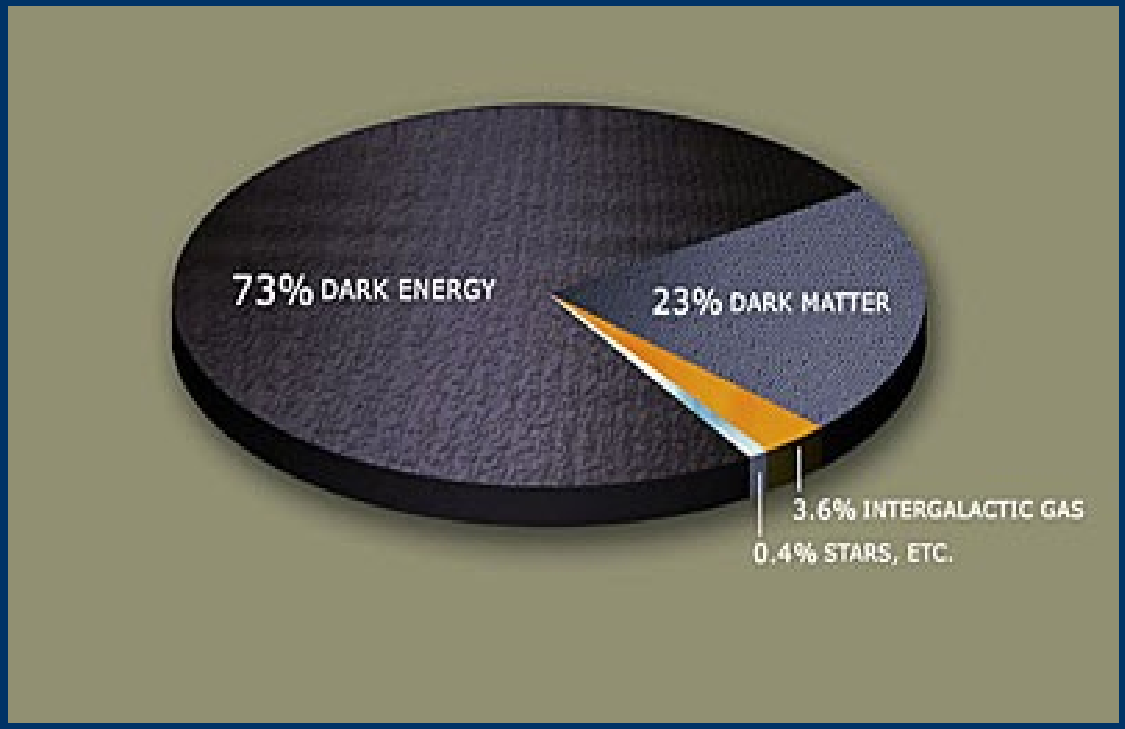
The INTERNET, Safe Computing and Home Networking

Our Cyber world is mimicking our real world

- Viruses, trojans, phishes, rootkits, spam, worms,
  - keystroke loggers, botnets, terrorists, mafiosi
- Advertising run amuck
- Full of people who want to steal your secrets
- Information overload and bloat
- Open (so far), with benefits and detriments
- Fertile for innovation
- Complexity increasing without bound
- MYSTERY, CONFUSION, CHAOS all around us

Mystery

- WHERE IS EVERYTHING??

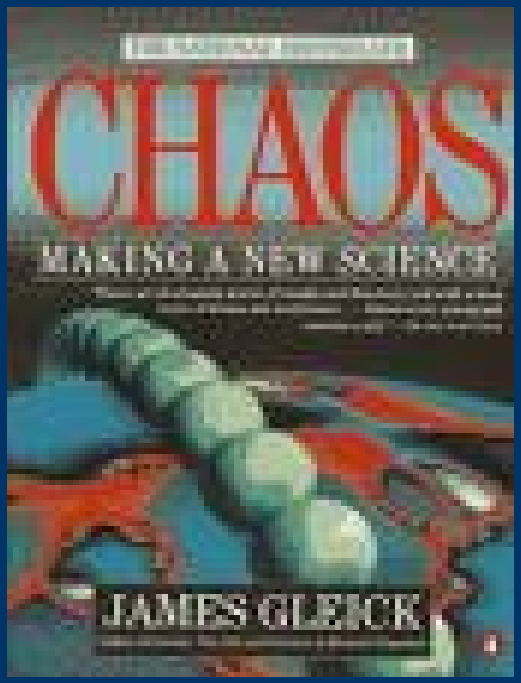


Who is in Charge?

- Certainly not us...

Chaos prevails

- It really does, we have a science of it



Some sobering thots/quotes

- Bruce Schneier Wired.com 10-07
  - ..”we really have no idea how to deal with storm. ...the antivirus companies are pretty much powerless to do anything about it.”
  - http://www.wikipedia.org/Storm_Worm
  - http://www.wired.com/politics/security/commentary/securitymatters/2007/10/securitymatters_1004
  - http://www.eweek.com/article2/0,1895,2205606,00.asp
- Information Week 10-3-07
  - About 98% of people claim to use antivirus, but only 48% of them are actively updating the antivirus signatures..
- PCWorld October 2007
  - Dismal performance of tools against new exploits!
  - http://find.pcworld.com/58303 Antispyware roundup
  - http://find.pcworld.com/58273 Antivirus roundup
- 99% of INTERNET traffic is
  - crap/spam/porn/illegal/anti-sware/updates
- Criminals have discovered the INTERNET
- Battlefield of the future
- Terrorists are not far behind
  - http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32907

Updated Dark Matter Pie Chart

Some sobering thots/quotes

- Steve Gibson 11-1-07
  - ....the idea of putting Windows [OOB Windows] on the Internet with no protection, I mean, it's just like game over. You're just taking - your Windows machine is just taken over almost immediately. Certainly, if you were also in the process of, like, trying to download updates to the original XP build, that has years of exploits wandering around the Internet right now, you would never get a chance to get Windows Update updated and up to speed.
  - http://grc.com/securitynow.html
- Internet Background Radiation
  - All those old systems compromised by all the exploits there ever was
- Go take a look!
  - ns0.sntlabs.com - probes
  - mail.sntlabs.com – junk mail
  - www2.sntlabs.com – ftp probes, looking for storage for crap

Grandiose hope

- The only hope we have for Safe Computing lies in intelligent users -
  - Users need to understand the environment :-(
  - Malware writers are keeping ahead of Microsoft and everybody else.. viz storm worm, etc.
  - If you think the gov/regulation/laws are going to be able to protect you, you are sadly mistaken (tho they will try) ...conversative vs liberal viewpoint....
  - It is truly the wild west in cyberspace
  - ***You need to be afraid*** and tread cautiously
- Just how many “intelligent users” will we have?

The Lowdown

- All this bad news doesn't mean all is hopeless
  - If you understand your environment
  - If you practice Safe Computing
  - If you have a backup strategy for catastrophes
  - If you watch your “connections”

Most of us here qualify....

It is possible to use/enjoy the INTERNET

Course guidelines

Intermediate level

- You are guinea pigs for this “course”
- Please add to the discussion (nicely)
  - Lots of experts here... :-)
- Emphasis is on INTERNET/Home network
  - Applicable to enterprise...
- Emphasis on connectivity (the network)
- Not Windows, unix Specific, no MAC, no PKI
- No Windows VISTA, no virtualization techniques
- Historical approach
  - I will be talking about IP/TCP before I explain it

Noteworthy Thots

- *If you think I understand all this stuff – you are crazy!*
- *I am a jack of all trades, a master of absolutely none!*
- *I get dumber every day*
- *Everybody else is in the same boat*
-

Course Outline

- “How the Internet Works”
  - TCP/IP for kindergartners
  - IP routing for idiots
  - Firewalls, NAT, Proxies for dummies
  - IP addressing made simple -hah!!
  - UDP/TCP applications – something we can understand?
- Vulnerabilities
  - How they come about ...
  - Client side only
- Addressing the vulnerabilities as a client/user
  - Safe computing practices

A retrospective

- Paper tape to Punchcards (batch procesing)
  - Terminal to mainframe (phone line)
    - Workstation at work/networked (ethernet)
      - Single PC at Home (standalone)
        - Single PC on dialup (second line)
          - Single PC on broadband
            - Multiple PCs on broadband
              - Multiple PCs on wireless
                - Mobile devices
  - **Today "Home Networking" - All devices work together, behind a protective barrier**

Safe Computing – a new buzzword

- The “INTERNET” is an “open place”
  - Absolutely anything “goes”
- The “Home network” must be a “safe place”
  - File and application sharing, printing
- The “Individual PC” must wear armor everywhere -even in the “Home network” to protect against vulnerabilities

“Safe Computing” is knowing what level of armor is appropriate for the situation

What are "vulnerabilities" and How do they come about?

- A Vulnerability is anything which allows others to use your PC/network for ***their*** purpose
- Vulnerabilities arise because
  - The INTERNET was originally a "trusting" place
    - No "security" built into protocols
  - Developer mindset
    - Microsoft learned too late to take the INTERNET, and security seriously, and who, until XP SP2, believed convenience more important than security.
  - ISPs and bridged modems in front of Pre XP SP2 PCs.
  - User ignorance and arrogance
    - Refuse to keep anything up to date
    - ***REALLY*** BAD computing/browsing habits

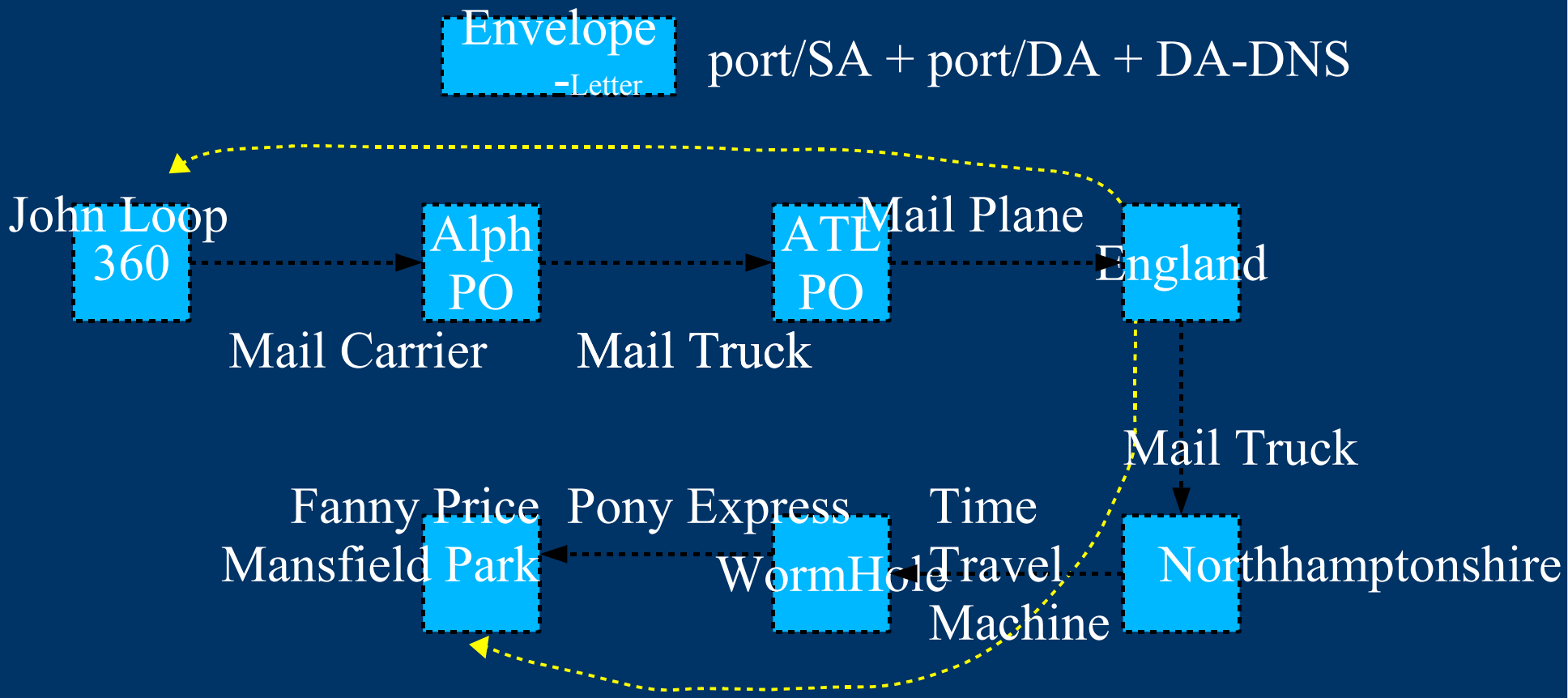
DANGER!!

- I can guarantee that your PC is compromised if you have not followed most of the safe computing principles we will talk about later.
- Unlike the early days (5 years ago..), the compromises mostly fly under the radar, and try to avoid obvious detection.
- AND it is harder to detect the compromises – 10 times as many people working on exploits
- AND the only way to clean it up is to START over
- AND the only way to prevent it is to practice safe computing

How the INTERNET Works

- Think of the INTERNET as the US postal system
  - 8th grade introduction ;-) - "network layer"
- Letters (envelope+content) = IP packets
  - Post Offices = routers for envelopes
  - TO address = IP Destination address (DA)
  - FROM address = IP Source address (SA)
  - Person = port (app at an address)
  - ZIP code = DNS lookup of name
  - Inside Letter = application (data for port)
- Many "link layers" to get letters delivered
    - (layer 2) Airplanes, trains, trucks, carriers =
      - FR, ATM, Ethernet, MPLS, ADSL
    - (layer 1) Air, roads, water: ds1, ds3, oc3c, sonet, worm hole

Link and Network Layers



The Network Layer delivers the envelope (IP packet)
Each Link layer has its own addressing/delivery mechanism.

The Letter is the app data, not touched by the network
The Envelope (IP packet) NEVER changes.

Remember

- Each Direction is ENTIRELY Independent
  - Just because you can go 1 direction does NOT mean you can go back!
- Translation from names to numbers (DNS) is an OVERLAY system, independent of network layer
  - Not “necessary” for operation
  - The “INTERNET” worked for years without it
    - Hosts files were passed around!
- All INTERNET addresses (houses) are unique
  - Notice I said INTERNET, not internet

We have MANY topics to learn

- Internet Basics (INTERNET, internet, network)
  - "internet" -> all of the above
- Ethernet Basics
- IP addressing Basics
- Routing Basics
- NAT/Firewall/Proxy Basics
- UDP/TCP Basics
- DNS Basics
- Application Basics
- Vulnerabilities, Addressing Vulnerabilities
- Safe Computing

Hold onto your Hats!!

Overall internet Basics

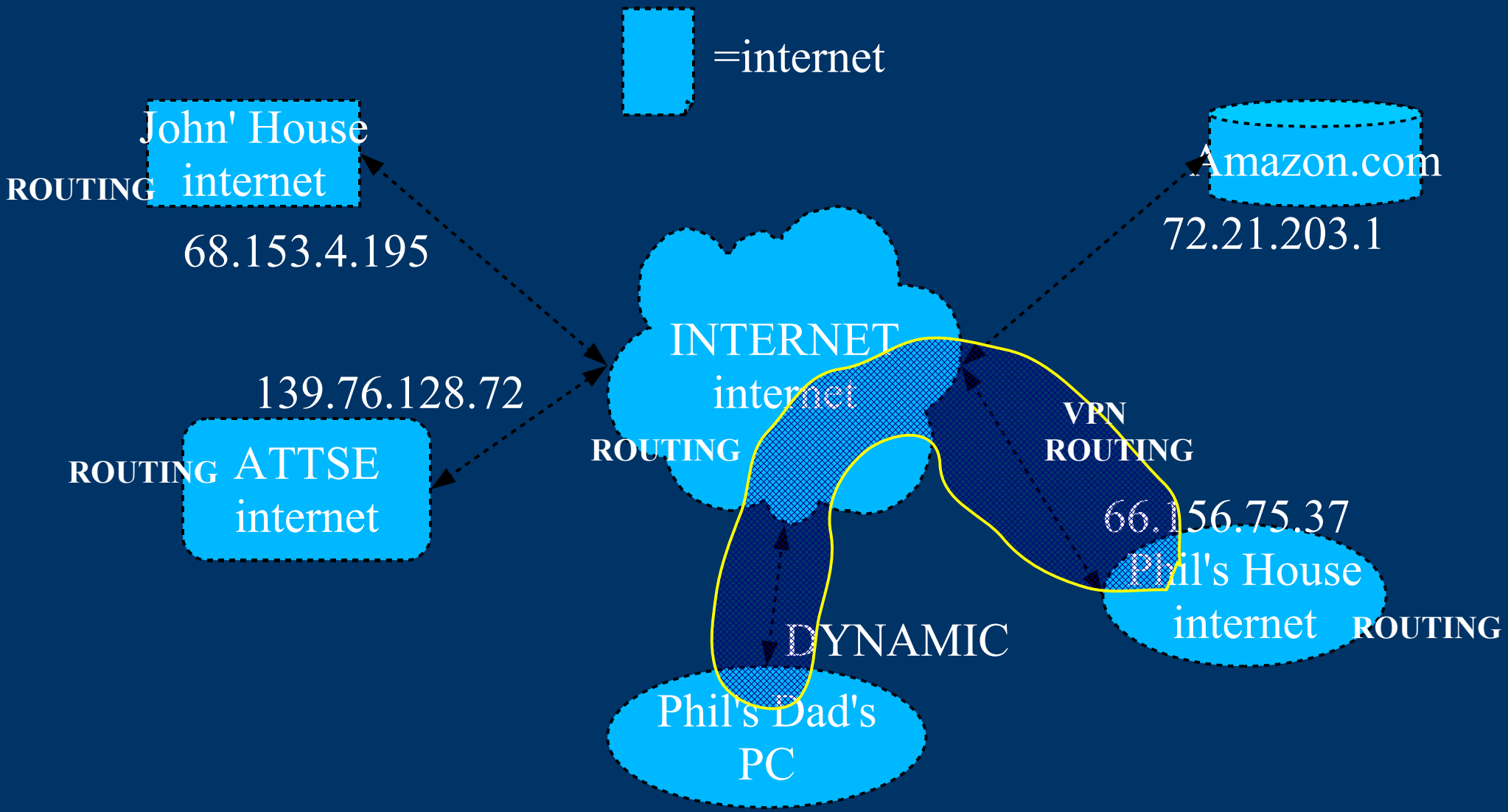
- The routers only route IP (simple view....)
  - They never look inside packet...
- The Source/Dest addresses never change, and are ***unique***! - unless we are NAT'ing or proxing
- An internet is an unreliable delivery mechanism
  - Letters get lost all the time!
- We have to use a higher layer protocol (TCP) at the ***endpoints*** to get reliable delivery
  - “connection oriented”
- We can also use unreliable delivery (UDP) at ***endpoints*** - “connectionless”

internet worlds

- “INTERNET”
  - The real thing
  - Global DA,SA addresses used in valid IP pkt
- .....”internet” -> ***generic term***
  - SA specific to internet
  - DA may be internet, or INTERNET, if exiting internet
- “VPN”
  - Can ***overlay*** above internet[s]
- .....”network”
  - A “piece of the address space”
  - ...internets have multiple networks.

Are independently routed, connected at edges

“internets”


=internet
John' House
internet
ROUTING
68.153.4.195
Amazon.com
72.21.203.1
INTERNET
internet
ROUTING
139.76.128.72
ATTSE
internet
ROUTING
VPN
ROUTING
66.156.75.37
Phil's House
internet
ROUTING
DYNAMIC
Phil's Dad's
PC

Ethernet Basics

- Now the Fundamental Link Layer
  - Replacing most every other one.... ATM, FR, TR
  - Separate source/dest addresses – MAC addresses
    - Delivery mechanism for the individual ***link***
  - ***"Protocol indicator"*** for upper layers
    - IP, ARP, BPDU, ICMP, IGMP, PPPOE, VLAN
  - Designed for ***Broadcast*** Medium
    - Telephone, ATM is a point-to-point medium
    - Adaptations for point-to-point mediums
  - Concept of ARP, VLANs
    - Address resolution, multiple broadcast domains
  - Switches and hubs, as opposed to routers.
    - Switches "route" based on MAC address

IP Address Basics 1

- IP address is unique within an “internet”
  - The INTERNET is an internet
  - Home networks, enterprises are isolated “internets”
  - 2^32 addresses (~4 billion)
  - IP addresses can repeat in the internets.
- Backbone INTERNET routes between “internets”
- Private “internets” can be NAT'd/Firewalled/Proxied to The INTERNET
  - They typically have a single appearance (IP address) on INTERNET
- “VPNs” can overlay this...
  - IPSEC, PPTP, L2TP, Hamachi, IPV6

IP Address Basics 2

- TYPES of IP ADDRESES
  - REAL internet addresses
    - Routed in INTERNET
  - PRIVATE internet addresses
    - RESERVED in RFCs
    - 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16
    - NOT (supposed to be) routed in INTERNET
    - Routed in “private” internets
  - ILLEGAL addresses
    - REAL addresses, but used in internets
    - 90.30.213.32, 222.1.1.1 e.g.
  - Multicast addresses 224.0.0.0 ->
  - Loopback address 127.0.0.1
  - Auto DHCP -> 169.254.0.0 ->

IP Address Basics 3

- CLASSES of IP ADDRESES
  - Class A 1.0.0.0 -> 126.255.255.255
    - Notice 10.0.0.0/8 private
    - 16M addresses per “network”
  - Class B 128.0.0.0 -> 191.255.255.255
    - Notice 172.16.0.0/16 private
    - 64K addresses per “network”
  - Class C 192.168.0.0 -> 223.255.255.255
    - Notice 192.168.0.0/16 private
    - 256 networks, 256 addresses per “network”
  - Class D 224.0.0.0 -> 239.255.255.255
    - Multicast (won't discuss here)

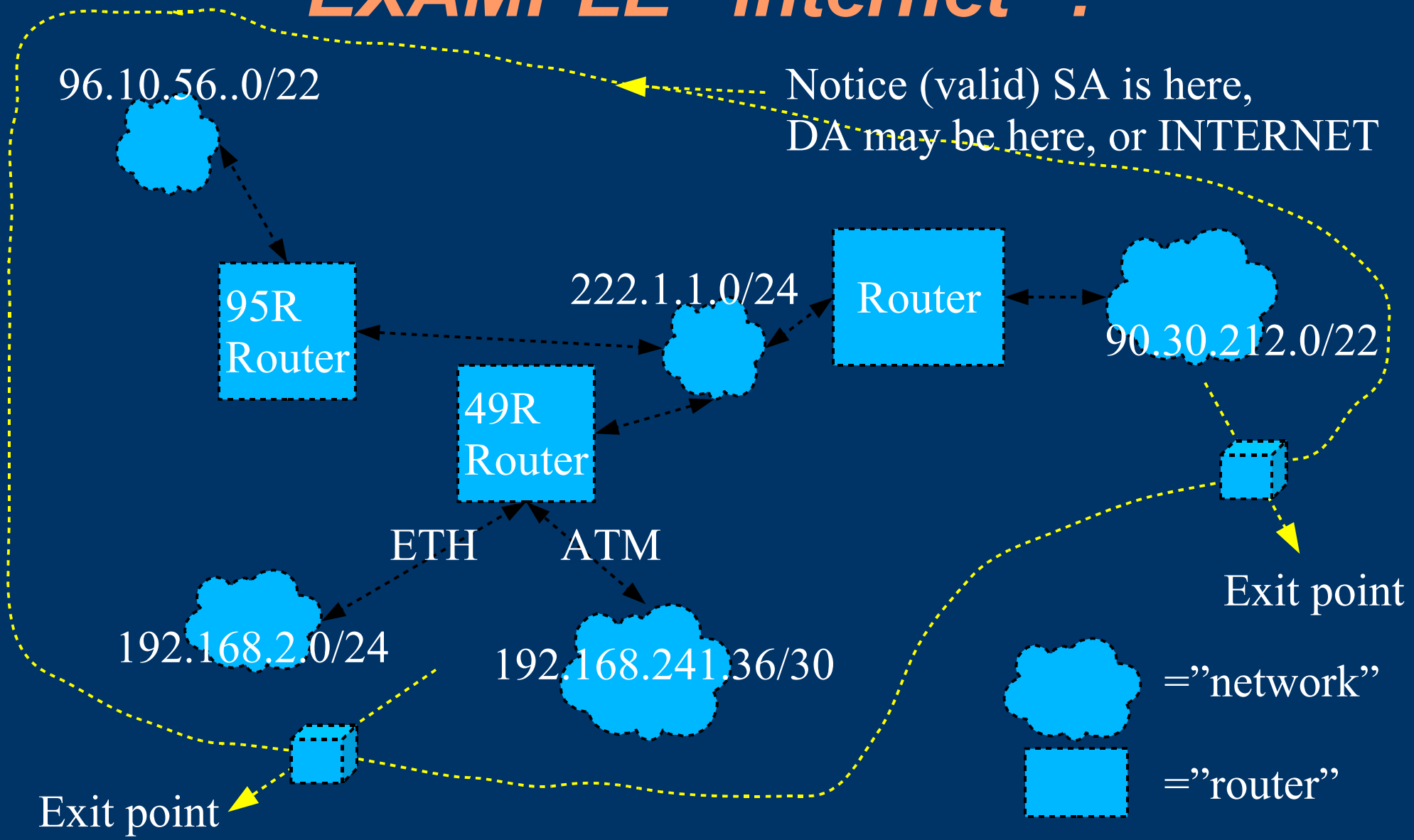
IP Routing Basics 1

- An Individual IP address is part of a “network”
- internets are composed of “networks,” and routing occurs between networks
- INTERNET or internet may have many networks
- “network” has a specific meaning!! e.g.:
  - 192.168.2.11/24 OR
  - 192.168.2.11 mask 255.255.255.0
  - THIS PC 192.168.2.11 is part of the “network”
  - 192.168.2.0/24 OR 192.168.2.0 mask 255.255.255.0

  ...another “network”:
  - 90.30.212.0/22 OR 90.30.212.0 255.255.252.0
  - 192.168.0.0/16 – supernet composed of all class C's

  We will spare you pain and NOT discuss subnet masks!

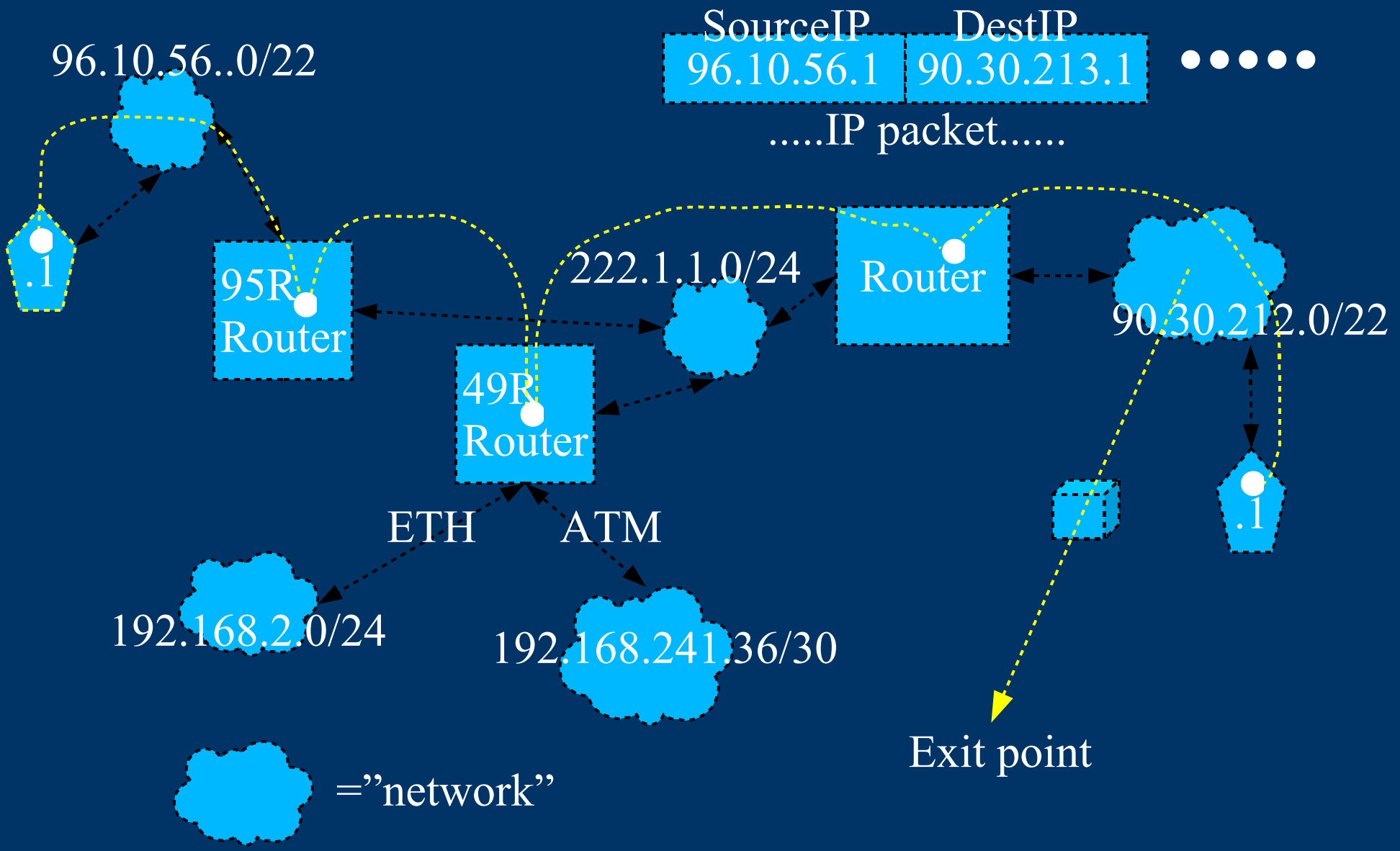
EXAMPLE “internet” :



IP Routing Basics 2

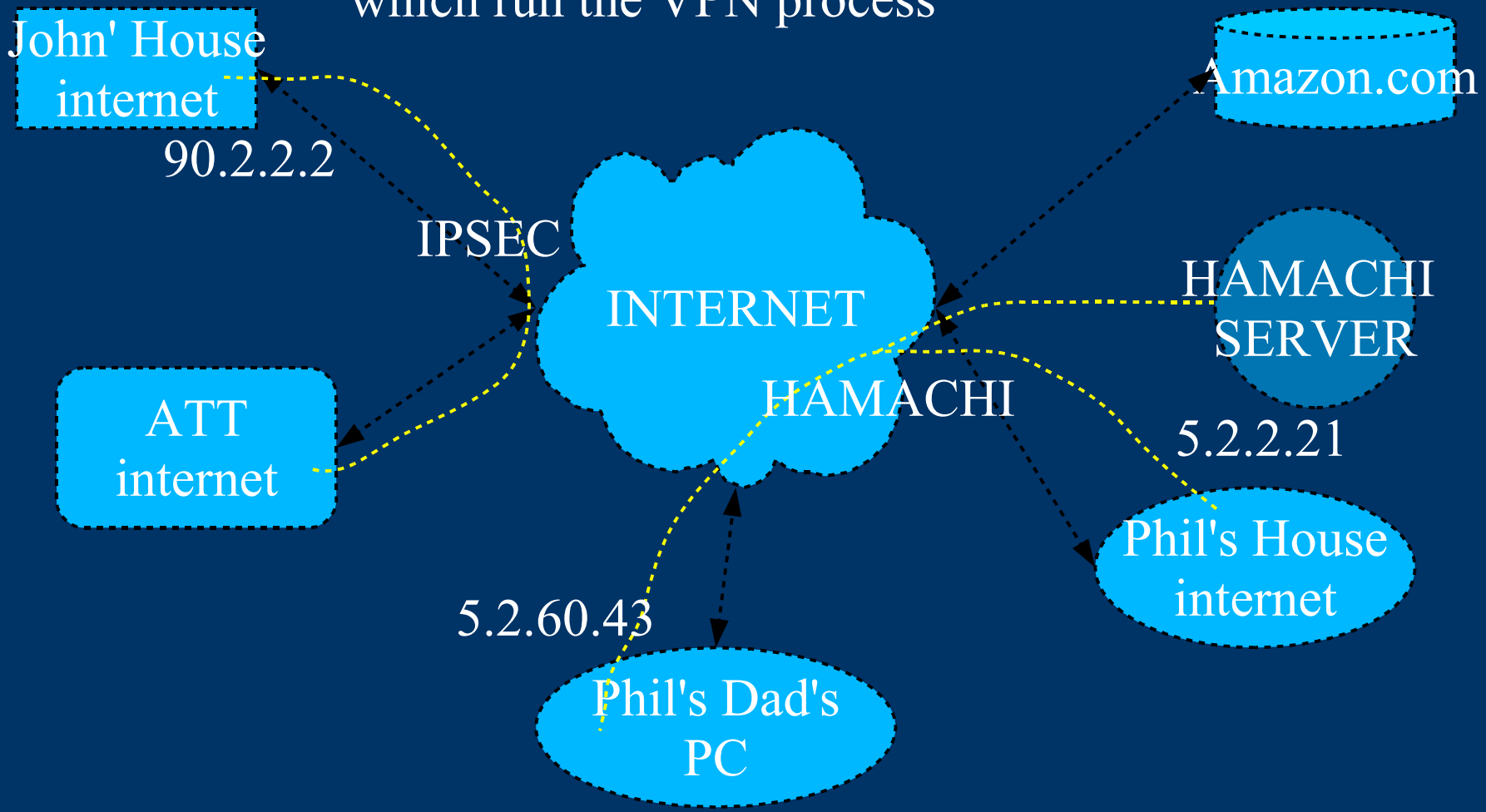
- Routing is performed based on “Routing Tables”
- Routing tables can be maintained
  - Manually
  - Routed protocols running in routers
    - RIP, OSPF, BGP – will not discuss
- Routing is “Hop by hop”
- Do a “tracert -d IP address” to see hops (PC)
- Do a “traceroute -d IP address” (linux/unix)
- “Virtual” “networks” can ***overlay*** internets
  - referred to as “VPNs” - IPSEC, pptp, l2tp, Hamachi

FOR EXAMPLE:

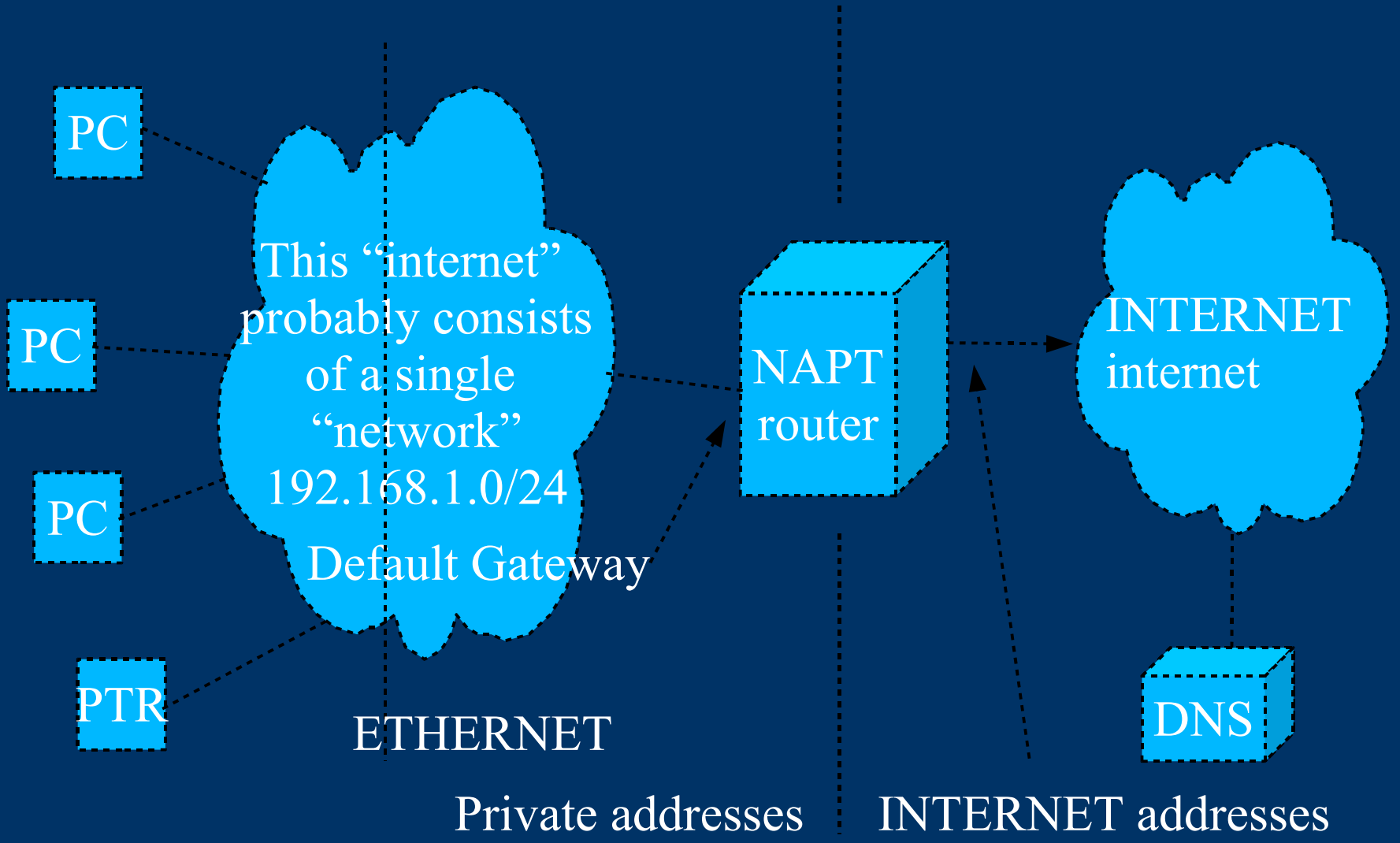

SourceIP
DestIP
96.10.56.1
90.30.213.1
.....IP packet.....
96.10.56..0/22
.1
95R
Router
222.1.1.0/24
Router
90.30.212.0/22
49R
Router
ETH
ATM
192.168.2.0/24
192.168.241.36/30
.1
Exit point
="network"

VPNs can overlay internets

VPN “IP pkts” are contained
WITHIN “regular” IP pkts – routed at endpoints
which run the VPN process



An internet which is NOT an INTERNET – home network



Rule of NAT/P

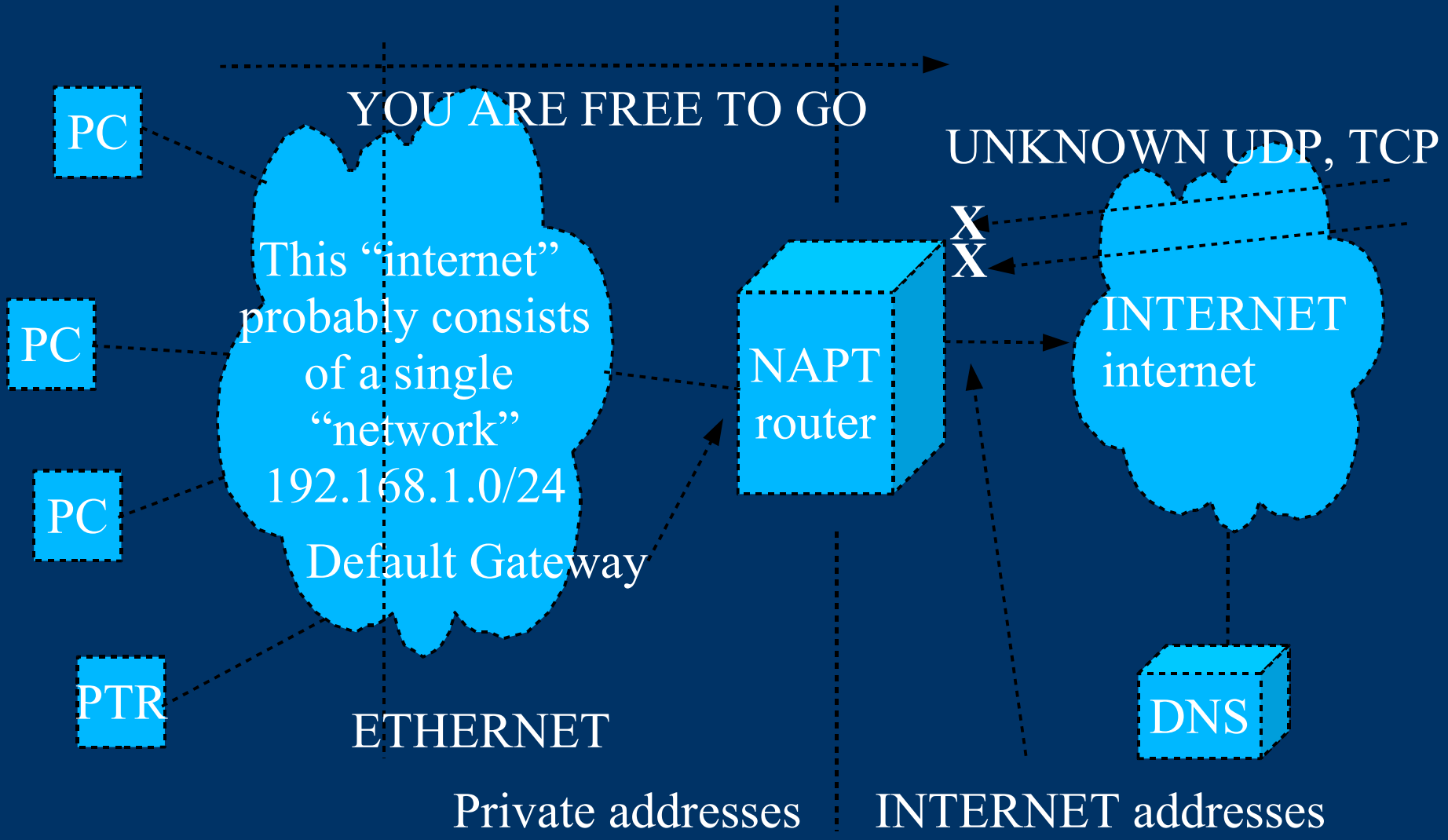
- Only RESPONSES to outgoing apps are permitted in. No UNSOLICITED input (...tbd)
  - Inside SA is UNKNOWN to INTERNET
  - EXIT SA is an INTERNET address(s)
  - SA replaced with INTERNET address on the way out, returned on the way back in.
  - Multiple inside addresses mapped to “ports”
  - Easy to track with TCP using SYN pkts (tbd)
  - UDP uses a timer to “open door” for returning pkts

Savior of the INTERNET IPV4 address space

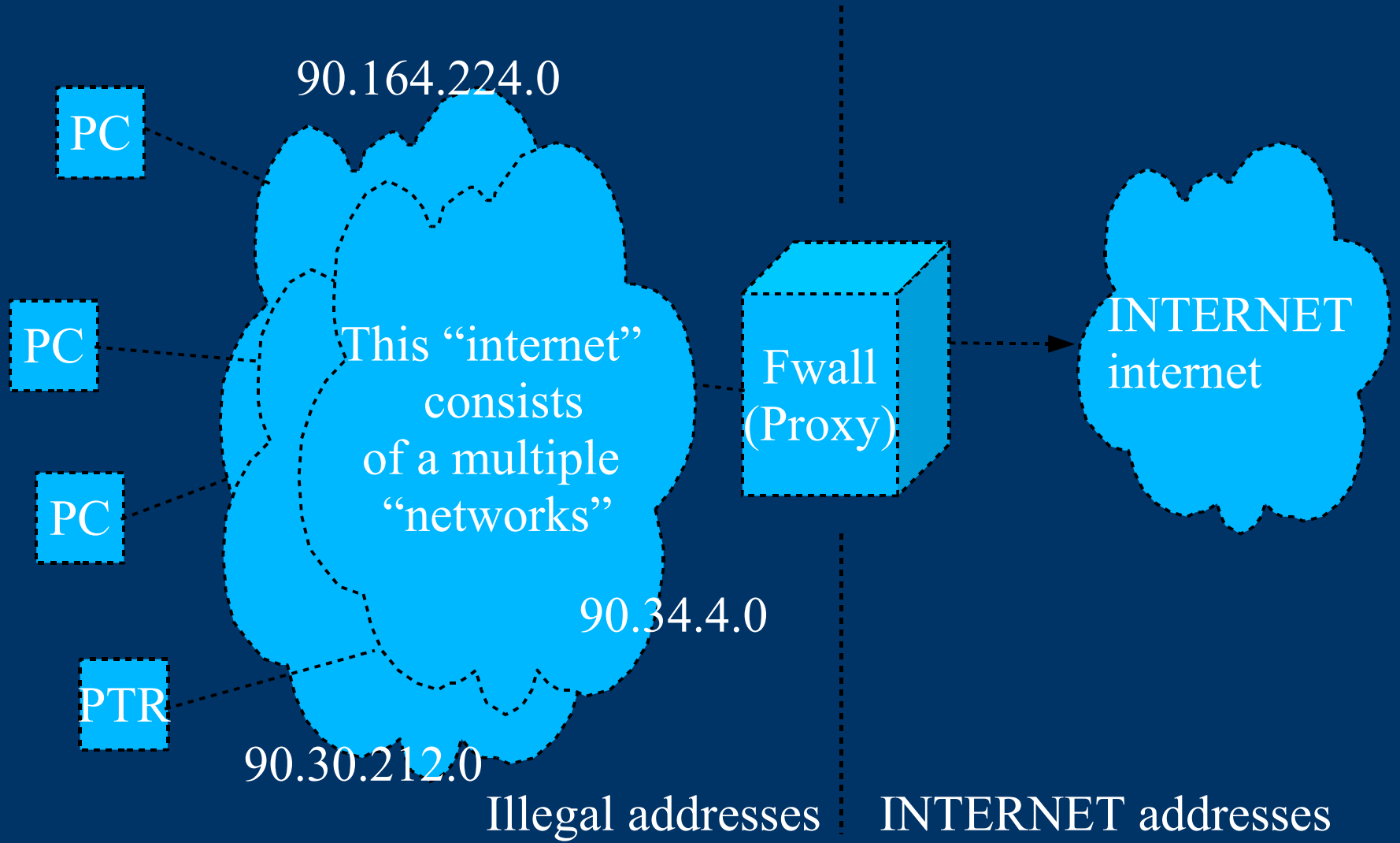
Bane of Internet purists, breaks many apps.

Savior of Windows OS

An internet NAP/T BLOCKs Unsolicited "STUFF"



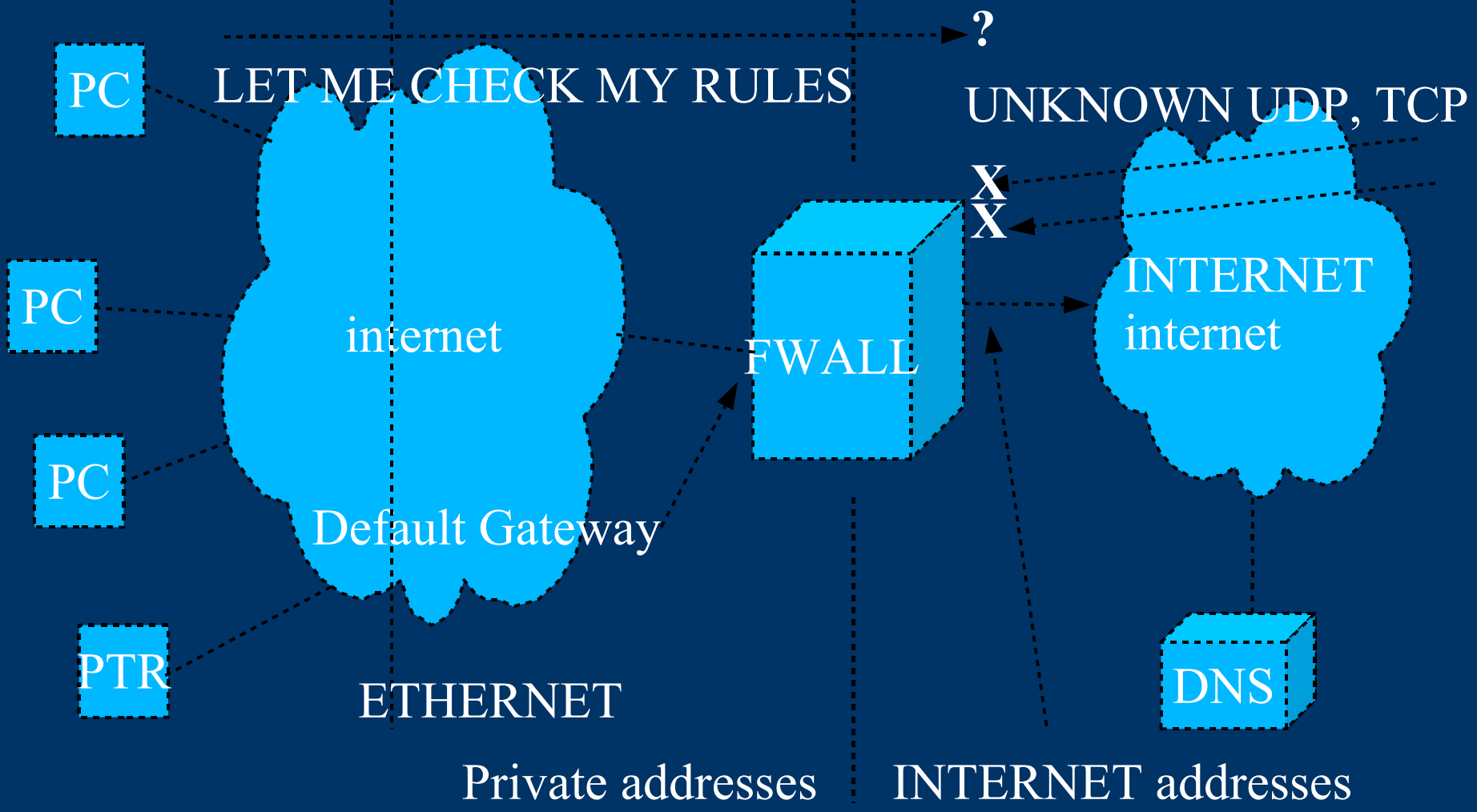
Another internet – an “enterprise”



Rule of Firewalls

- NOTHING gozzinna or gozzouta without a **RULE**
  - Defaultly DROPs
- Deep packet inspection is implied
  - i.e. Looks beyond the IP addresses into
    - Ports (applications)
    - Illegal activity – BAD IP/TCP header bits
    - Known exploits
    - Suspicious activity, DOS
    - Excessive pings, port scans
  - Extensive logging
- Often performs proxying
  - (on the way out) SA replaced with External add, like NAPT
  - Apps terminated in process, regenerated by a process, thus "proxied" to INTERNET
  - DA (supplied by endpoint) is that of PROXY device

A Firewall BLOCKS unsolicited in and outgoing without a rule



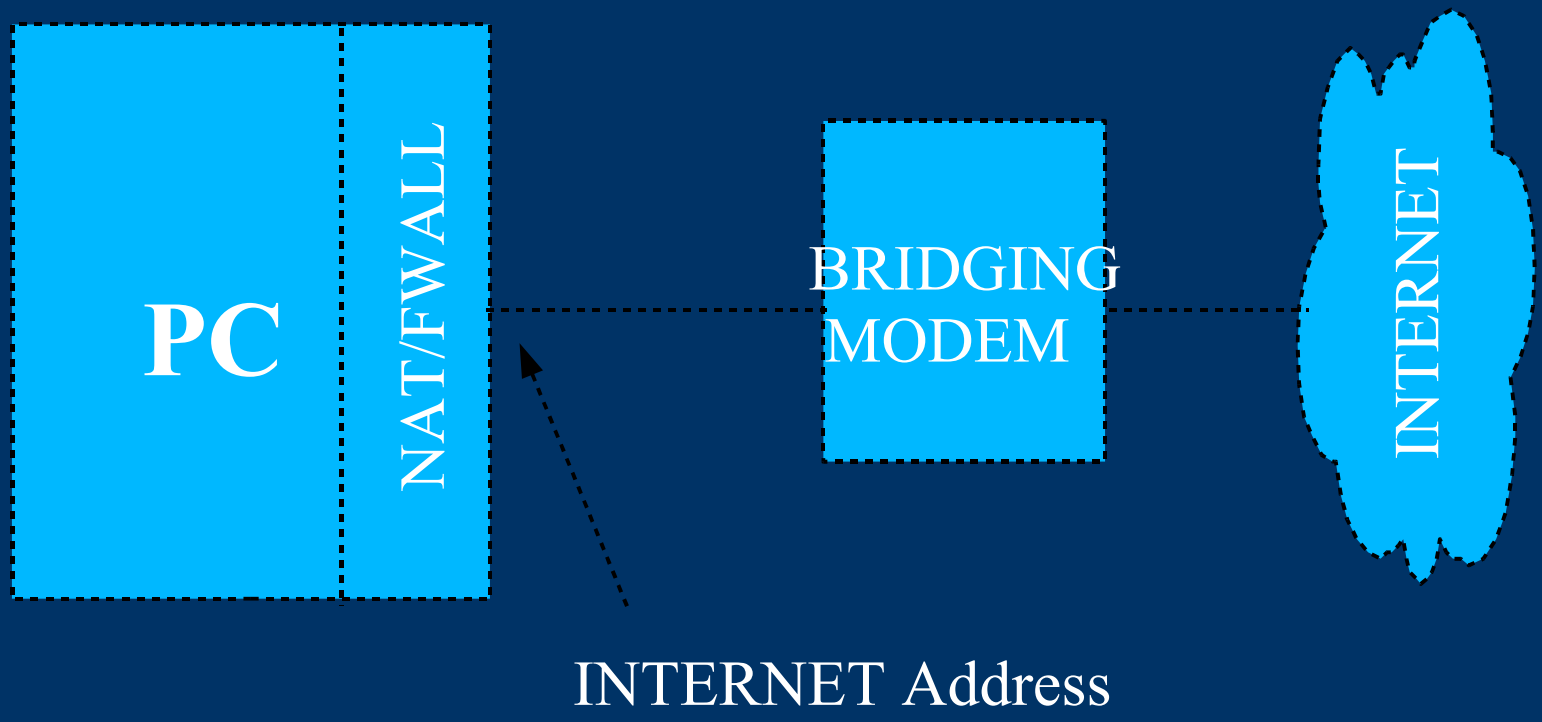
Confusion Reigns!

- The term “Firewall” is ***terribly*** abused
- Many people routinely refer to a simple NAP/T router as a “firewall” (even my hero Steve Gibson)
- Many “simple” NAP/T routers now ***come*** with ..some.. firewall capability.
- *There are terribly sophisticated hacks which can breach many NAP/Ts and “cheap” firewalls*
- Firewall capaiblities vary tremendously!
  - Home use not to worry ...tooo much
  - ATT – you better pay a fortune for your firewalls!
- After all it is only software – much like what you write – how good is that stuff?

Another category

- NAT/P included on PC
- Necessary on all Windows OS's prior 2 XPSP2
- Windows application program!
  - Bloated
  - Now part of
    - Antispam, antispyware, antivirus, antiphish etc suite
  - Can be turned OFF by malicious sware
  - updates/subscription/money
- Windows SP1: ICF/SP2: FWALL – outbound only
- Linux – Iptables + GUI front end
- Solaris – 9:? 10:?

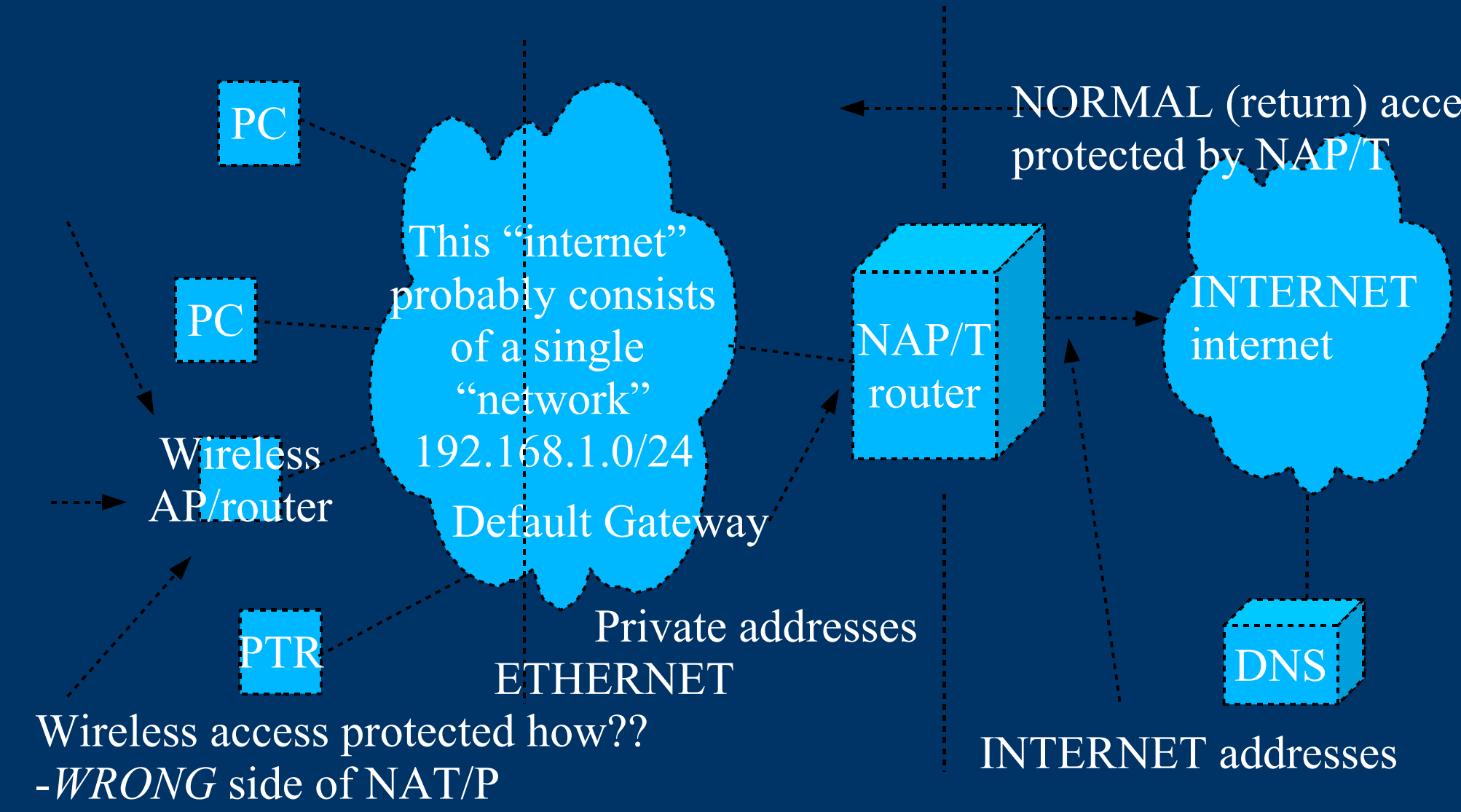
NAT included on PC



Home Network Dilemna

- We want wide wide open network at home, for easy file sharing, app communications
  - We can protect ourselves
    - As long as we practice safe computing
- We want to add wireless at home
  - Can be real security headache
    - WPA[2] only protects link access!
    - No longer protected by home NAT/fwall
- We want to move laptops
  - between home/work/starbucks
    - Each has different risks
      - Home – hopefully safe....
      - Work – I can infect others...
      - Starbucks – others can infect me...

Adding wireless – home network



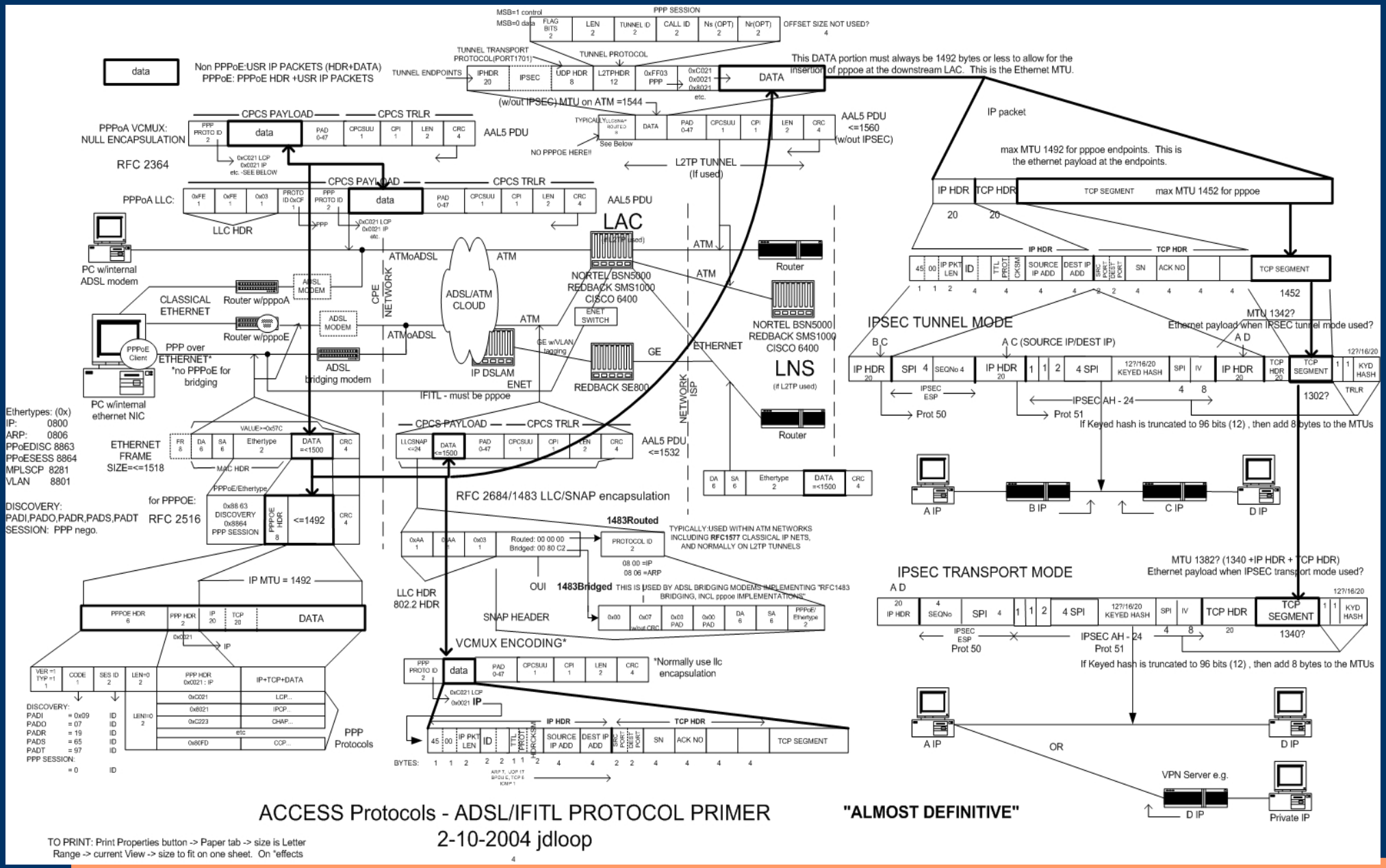
Talk about protocols

- IP
- TCP UDP

Protocols

- We understand “Networking”- network layer
- We understand NAT/P, FWALLS
- Now we need to understand “protocols”
  - This how NEs, applications talk over the networks
- Layer 2 protocols – link layer networking
  - Largely ethernet – ARP, BPDU, ST
- Layer 3 protocols – routing and debugging
  - Largely IP – IP, ICMP
- Layer 4 protocols – transport
  - UDP, TCP
- Layer 5 -> protocols - application
  - HTTP, SMTP, POP3, SNMP, SIP, DNS, etc.
- C:\Documents and Settings\John\My Documents\AdslprotocoVisio5Letter.jpg

CHECK this out!



Processing of IP packet

- Once an IP packet winds up at my PC, now what?
  - MAC address decided this was for me
  - IP address says this is for me
- Your IP protocol stack sware looks for type:
  - UDP (17)
  - TCP (6)
  - ICMP (1)
  - ARP (7)
  - IGMP (2)
  - BPDU (E)
  - IPSEC ESP (50)
    - Then sends to process handling protocol

ICMP processing

- ICMP
  - Endpoint processes this, not an app (NO PORT)
  - Ping echo request, echo reply pkts.
    - Checks basic IP connectivity between 2 endpoints
    - Not fooled by physical loop
  - Service (port) not available
  - Host unreachable – via router upstream
  - Redirect – via router upstream
  - Time exceeded – pkt bounced around, timed out
  - Fragmentation required, but you told me NOT to

  Beware intervening routers NOT responding to ICMP!
    - Pppoe and MTU problems
    - Cannot ping www.microsoft.com

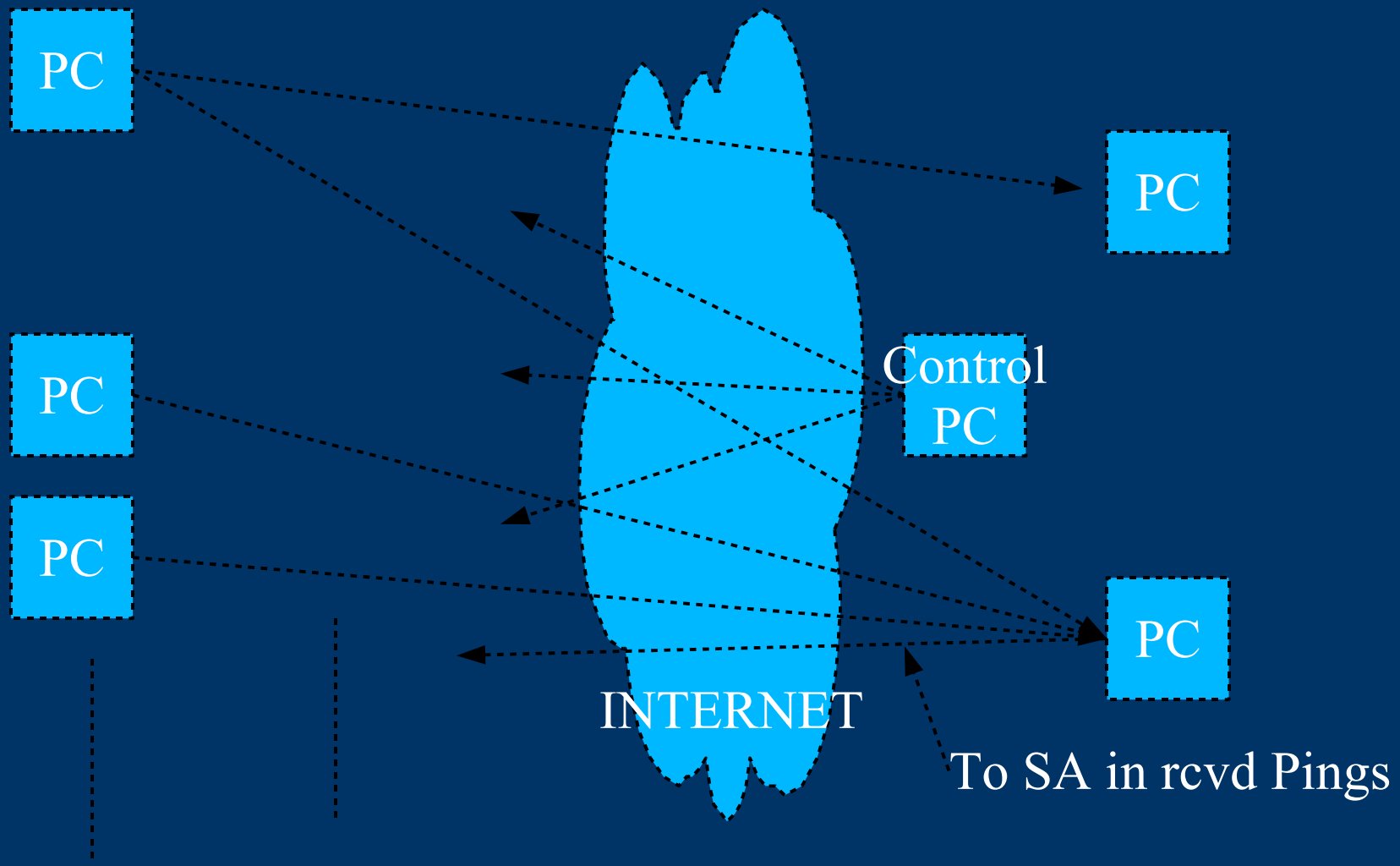
UDP Processing

- UDP
  - Fancy IP packet at transport layer
  - Directed at a particular service (port)
  - Connectionless, unreliable, *no delivery guarantee*
- DNS query/response is good example
  - Port 53 is bind service running on DNS servers
  - DNS query pkt is UDP to port 53
  - DNS response is UDP to port 53
- SNMP another
  - *No way to guarantee* SNMP delivery
- No traffic shaping/throttling of UDP
  - Very dangerous uses – DOS, DDOS
  - Used for transaction type services, streaming

Dangerous UDP....

- More efficient/less overhead
  - 8 bytes overhead, compared to 20 (TCP)
- DOS and DDOS
- Buffer overruns
- Lost Packets
  - Application must provide “reliable flow”
- No Flow Control
  - Application must traffic shape
- How do I determine origination?
    - A letter can show up from anywhere..
      - SA can be spoofed!
    - A phone call comes from one “person”
      - SA cannot be spoofed

DOS/DDOS/ReflectedDOS



Good ole TCP

- Point-to-point
  - Setup procedure needed
- TCP guarantees delivery/order
- TCP guarantees accuracy of content
  - Eth has cksum, IP only cksum over header.
- TCP will “fit” delivery speed to pipe size
- Does NOT address all concerns
  - Not a “secure” form of communication
  - Man-in-the-middle attacks
  - Content NOT encrypted
  - Can reliably determine origination
- -> TCP can be abused however, if we don't care about establishing true pt-to-pt communication!

TCP setup procedure

- Outgoing IP packet
  - TCP content
    - Service port
      - SYN -> like dialing a phone number --->>
      - SYN-ACK far end returns “hello” <<---
      - ACK “hello” --->>
- TCP connection is now UP
  - Data can be exchanged between processes
    - Especially behind NAT/P
    - Not behind a firewall unless RULE exists
  - Only ***two*** endpoints involved in connection
  - ***I can distinguish WHO initiated connection***

TCP applications

- HTTP port 80, HTTPS port 443
- SMTP port 25
- POP3 port 110
- Telnet port 22, SSH port 23
- FTP port 21, 20
- SMB port 139, 445
- VNC port 5900, RDP 3389
- IRC 6667
- www.grc.com/<port no> to find info

Now You can Understand NAT/P!

- NAT/P routers “simply” look for “SYN” bit
- Outgoing pkts with single SYN -> OK
  - Track this connection, let all succeeding incoming
  - Outgoing pkts
- Incoming pkts with single SYN -> DROP
  - Incoming pkts with BAD TCP headers -drop
- Incoming pkts with ACK or SYN/ACK -> OK
  - Watch for hack attempt- sequence # must match
- For UDP, a timer is used
- NAT/P routers allow pinholes/port mapping
  - Often have “firewalls”
  - Are getting VERY complicated
  - Can run “stealth” (turn off ICMP replies...)

Your friend "Netstat"
The tell-all utility

- Lists ALL TCP/UDP sockets + processses
  - Windows "netstat -an[bv]"
  - Linux "netstat -aplunt"
  - Solaris "netstat -an |more"
- You ***NEED*** to learn this cmd
  - Easier GUI version on windows -> "tcpview"
- Run it from startup, and "always on top"

  - COURSE in tcpview and netstat.... using bittorrent

Netstat Examples

MY IP:port ***REM IP:port*** ***STATE***

- TCP 90.30.323.32:3318 222.1.1.55:22 ESTABLISHED
  - My PC is exchanging data with 222 port 22
- TCP 127.0.0.1:1024 127.0.0.1:1089 ESTABLISHED
  - Two processes on my PC are communicating via TCP thru the loopback port
- TCP 127.0.0.1:25 0.0.0.0:* LISTENING
  - The Mail server is listening for mail, but only locally
- UDP 205.152.56.182:53 *.*:53
  - My machine is running named (DNS) – I am DNS server
- TCP 90.30.213.32:53957 90.30.214.173:6000 ESTABLISHED
  - Running X server to 173
- TCP 90.30.213.32:42231 222.1.1.61:3389 ESTABLISHD
  - Running RDP to 222

DNS Basics

- We don't ***NEED*** DNS, but it is nice....
- Completely ***SEPARATE*** from everything we have talked about – it is an ***OVERLAY mechanism***
- You PC is given a "DNS server" to handle all the hard work xlating names – ***IPaddress***
  - Try number on browser, then name
  - Try numbers in different formats!!
- DNS server is always given as an ***Ipaddress***
- ***First thing I always check is "can I ping it by Ipaddress" - keep one in your brain!***
  - ***If this works, I know the INTERNET is OK, it is just DNS problems. 205.152.56.129***
  - ***And Believe me, this is BIG problem***

Real time DNS education

- Hosts Table – IP to name translations
  - \windows\system32\etc\drivers\hosts
  - \etc\hosts - unix
- DNS on Router?
  - Hard coded or via DHCP?
- DNS on PC?
  - Hard coded or via DHCP?
- Use DNS tools
  - Nslookup “host”, dig (linux)
  - Ipconfig [/flushdns /displaydns]
- Browser DNS cache
- DNS hijacking/Hosts table hijacking
  - *THIS* is scary

Wireshark (Ethereal) is your friend

- Local Protocol analyzer
  http://www.wireshark.org/
- Ethereal education.....
  - Pick NIC
  - Enter “host Ipadress” or “[udp|tcp] port 53
  - Update in real time
  - start
  - Watch IP addresses, ports
    - Great education

Midterm Summary

- We understand networking and transport :-)
- Prior to XP SP2, most exploits were via open ports
  - "Solved" by NAT routers/XP SP2 "fwall"
  - "Solved" by Microsoft taking security seriously
  - "Solved" by antivirus/antispyware/antithis-that sware
    - Huge industry born to "protect" us from malware
    - Huge "industry" born to infect us
- ***Still***, if you have open ports/unpatched OS – you will be compromised in minutes on INTERNET
  - A majority of people are still not industrious in protecting themselves

New Malware avenues of infection

- Post XP SP2 – email scams, phishing, malware web sites loaded by email links
  - How does it happen?
  - Running behind NAT/P
  - Up to date OS
  - Up to date virus/scumware/phishing

  For Example:
  - You run OE in auto preview mode (bad), and click on link in a piece of SPAM – say one of those e-card greetings this summer (storm worm)...
  - IF YOU HAVE A VULNERABILITY, you are toast!
    - You probably have a vulnerability if
      - Antivurus NOT uptodate (or malware has morphed...)
      - Windows NOT uptodate, ActiveX, javascript enabled
      - ZERO DAY exploit exists

How it compromises you

- Since you don't run OE in txt only, it fetches all the links to display email, including the malicious web site, most likely hidden in a zero GIF.
- You have NOT disabled ActiveX, so the downloaded script from the malicious web site simply loads in the attack vector for the exploit....
  - Stack overflow against vulnerability
- antivirus does NOT catch this because there is no virus in the email. Your NAT/P does not block it because it is originating from the inside.
- Firewall doesn't catch it because http is allowed
- Antisware ***may*** catch it if it is uptodate....
  - AND if the malware hasn't morphed...

Browser Scripting

- ActiveX – most dangerous
  - Free rein to PC
  - “signed” to control creation – bad guys can sign too!!
  - Portable Windows code, needed for microsoft apps
- Javascript
  - Downloaded with browser
- Java
  - Interpreted code
  - Least vulnerable
- IE has many knobs to control these
  - Very confusing

More botnets...

- http://www.darkreading.com/document.asp?doc_id=138610&WT.svl=news1_1

MySpace Hack

- http://www.informationweek.com/security/showAr
- http://www.youtube.com/watch?v=VipylmHnII

IE protections

- Switch to firefox http://www.mozilla.com/en-US/ or opera
  - No ActiveX, but keep it updated!
- IE:
  - Internet options – security - internet – high
    - No pdfs, flash?,
  - Add sites to trusted zone as you go along...
    - ***OR default the zones, and us***e
  - Use IE7 in safe mode – hidden in:
    - Start -programs-accessories-system tools-IE no addons
    - OR run “iexplore.exe -extoff”
      - Meant to recover a hosed IE, but usable by itself
    - Keep as a ***separate*** link
    - Not much works here, but you can switch back
    - Only available in recent Windows updates!!
    - http://blogs.msdn.com/ie/archive/2006/06/12/628499.aspx

OE protections

- Use thunderbird http://www.mozilla.com/en-US/
- OE:
  - Tools-options-read-
    - !"auto download in preview pane"
    - Read all in txt (if you can stand it)
      - Links, but no images
  - Tools-options-send
    - Mail sending plain txt
  - Tools-options-security
    - OE put in IE restricted zone (default)
      - Displayed html may be OK here, but don't click on link!
  - Add "preview" button to toolbar
  - **NEVER** click on links in email
  - Make Firefox default browser invoked by OE

MAC attack

- http://www.eweek.com/prestitial/0,,,00.asp?success_page=/article2/0,1895,2210900,00.asp
- Porn come-on, followed by malicious site, followed by bad sware, followed by DNS hoist, followed by spoofed sites to phish
  - Includes rooted component to reinstall bad DNS!

Just a few Links

- www.kb.cert.org/vuls
- http://www.cve.mitre.org/
- http://nvd.nist.gov
- http://www.us-cert.gov/reading_room/securing_browser
- http://www.cert.org/tech_tips/home_networks.html
- http://cert.org/homeusers/HomeComputerSecurity/
- http://www.cert.org/tech_tips/malicious_code_FAQ.html
- http://www.cert.org/archive/pdf/activeX_report.pdf
- http://www.microsoft.com/security/default.mspx
- http://www.grc.com/securitynow.html
- htt://www.darkreading.com
- http://www.kaspersky.com/scanforvirus Use online scan
- http://www.microsoft.com/downloads/details.aspx?FamilyId=4B4ABA06-B5F9-4
  - online? security scanner
- **http://psi.seconia.com/ - use online tool**
- http://onecare.live.com/site/en-US/center/howsafe.htm?s_cid=mscom_msrt
  - Use the malicious software online scan tool

Safe Computing top 10

- Run PC behind NAT/P or fwall
  - Use SP2 fwall if necessary!
- Do NOT visit “questionable” sites
- Alternate OS? Use MacOS/linux/knoppix
- Alternate App? Use firefox?/thunderbird?
  - Or OE and IE locked down
- Run simple antivirus (AVG)
  - Avoid the bloat packages
- Run TCPVIEW, keep it on top
- Keep OS/apps up to date
- Avoid wireless..... :-(
  - ALWAYS turn on PC fwall if you use wireless
  - Make sure you use WPA/WPA2

Safe Computing top 10

- Know when to turn that “FW” on (..dialup)
  - Leave it on if you're not home networking..
- Conduct NO private business on public/other PCs
  - And watch for keystroke loggers/trojans how?
- On public LANs, private business only via VPN
  - Fwall always on when your PC is on diff LAN!
- Make sure UPNP is off
  - Anything on your PC(bad) can use it!
- Use a Password lockbox with a huge passwd
  - http://passwordsafe.sourceforge.net/
- Avoid laptops – or chain them to your person

Safe Computing top 10

- Watch for the https, check the certs
  - right-click on the page, look at the page properties, then click on View Certificate to see the certificate. Then look at the chain of trust to see who signed that certificate.
- Enter link info, don't click (paranoia mode)
- Don't let anybody else use your PC
  - Or use dual boot or virtualization.....
- Crush old hard drives before trashing
- List of about 50 at
  - http://www.pccitizen.com/safecomputing.html
- For God's sake, dump that win9x/ME/2000
- Read every episode http://www.grc.com/securitynow.html