i310

Introduction to Networks

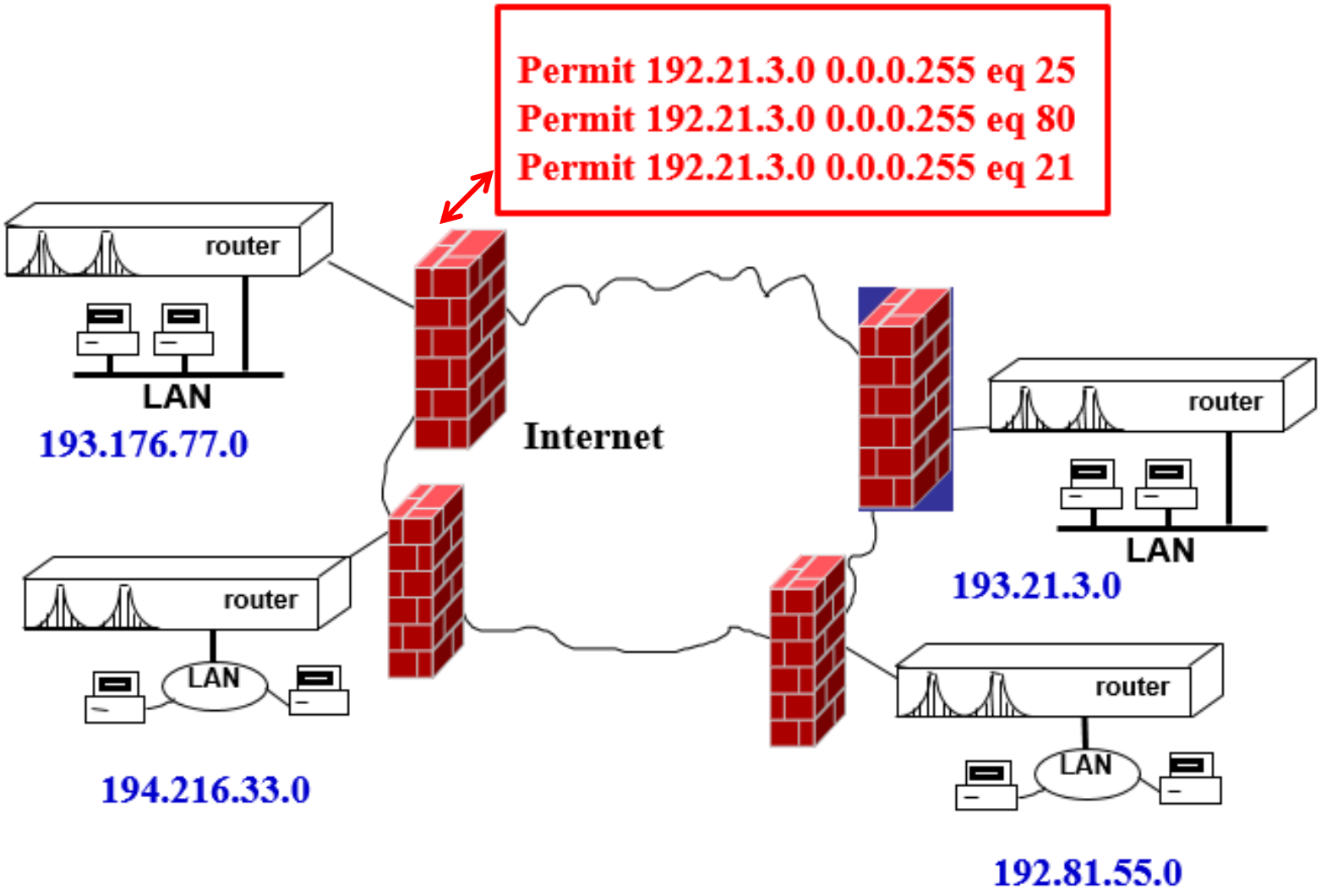
Instructor: James Farricker

Why Are Networks Important ?

They are the nucleus that tie together components, systems, companies, governments and countries.

Why Understanding Networks Important in i310 ?

The majority of security mechanisms in use today are network-centric, that is - based on network related technologies such as firewalls that permit/deny IP addresses or networks, packet filters which have rules tying IP addresses to specific network applications by TCP/UDP ports etc.

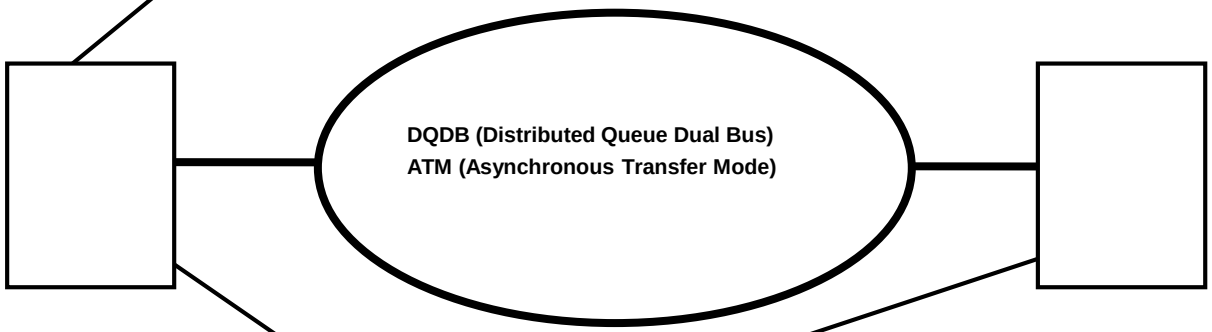

Permit 192.21.3.0 0.0.0.255 eq 25
Permit 192.21.3.0 0.0.0.255 eq 80
Permit 192.21.3.0 0.0.0.255 eq 21
router
LAN
193.176.77.0
Internet
router
LAN
193.21.3.0
router
LAN
194.216.33.0
router
LAN
192.81.55.0

NETWORK TYPES

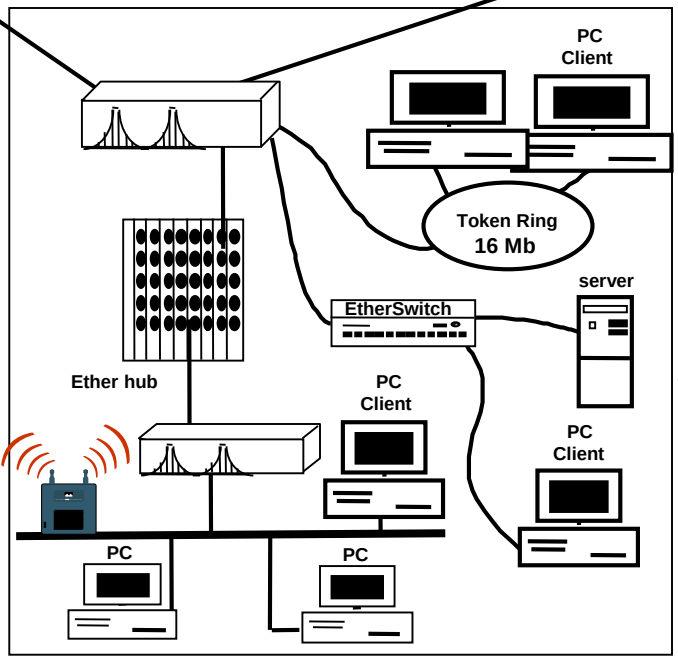
Wide Area Networks (WANs)

SONET & ATM
Dedicated Circuits (T1, fractional T1, T3, OC-n)
Frame Relay
Public Telephone Circuits
VPNs and MPLS
Cellular – 3G, 4G

Metropolitan Area Networks (MANs)



Local Area Networks (LANs)



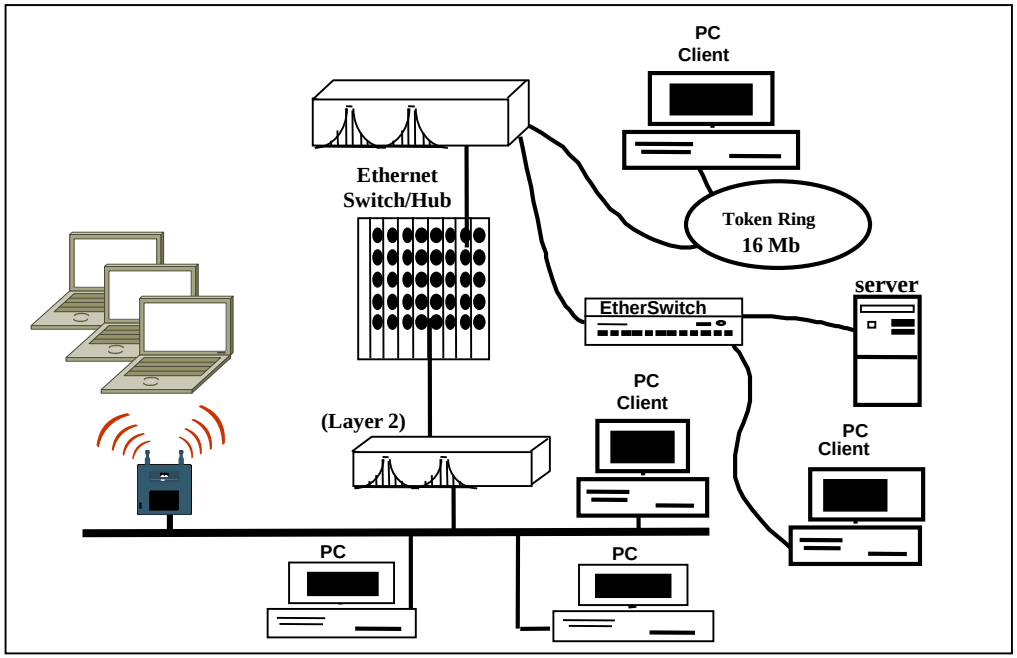
Ethernet (10/100/1000/10000 Mb)

Token Ring

FDDI

802.11 (Wireless LANs)

Local Area Networks (LANs):

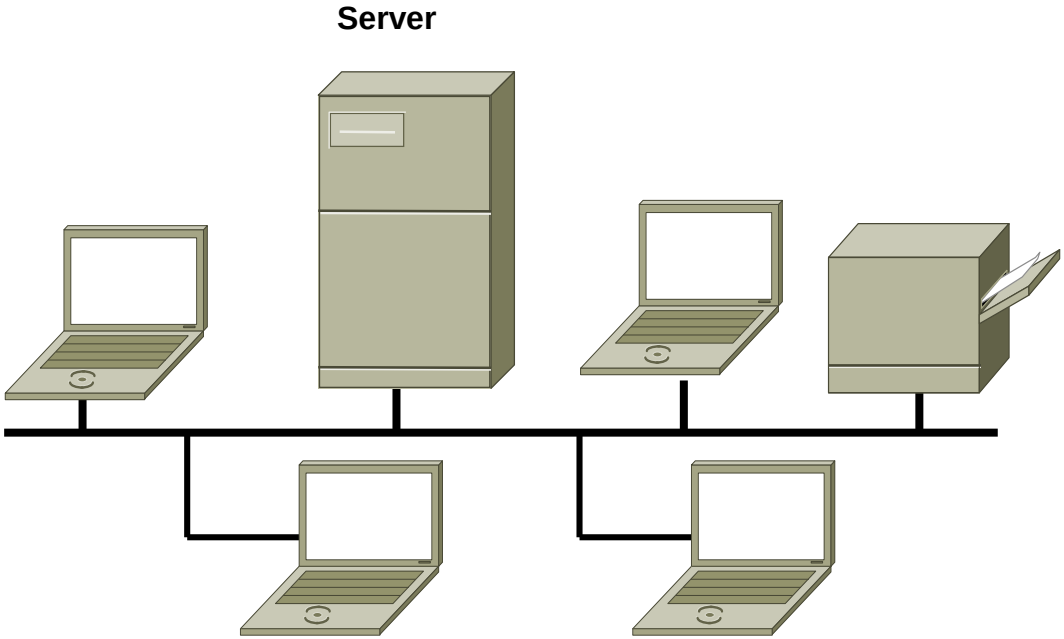


Basic characteristics of a LAN :

Geographically limited to building or campus
Privately owned
High Speed
Shared Media

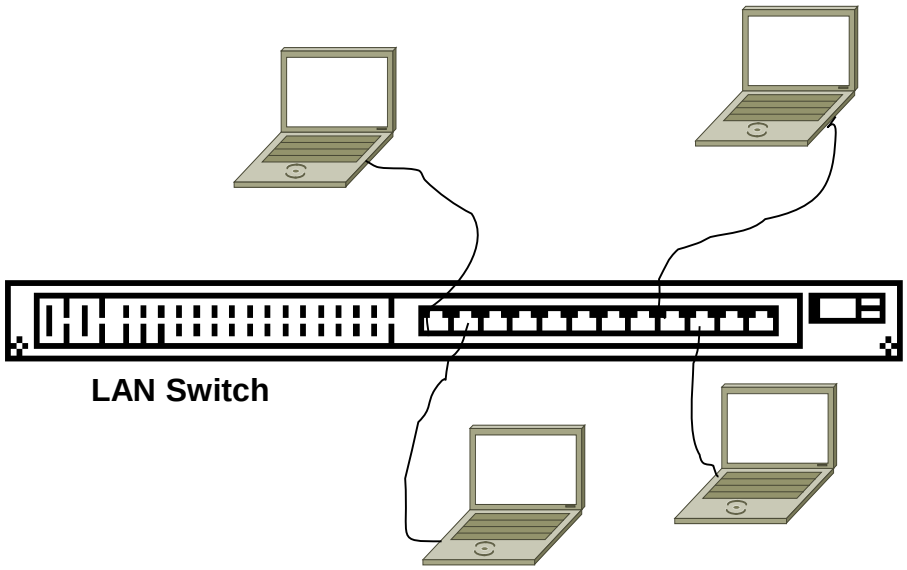
Network Topologies

Bus Topology: (Example – ThickNet Ethernet)



Broadcast-oriented – all transmissions heard by all stations
Multipoint medium
Transmission propagates throughout medium

Star Topology: (Example – Ethernet Hub & Switched LANs, WANs)



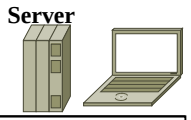
Each station connected directly to central node
Physical star, logical bus
Central control and management

Network Architectures & Protocols

Introduction to Networking

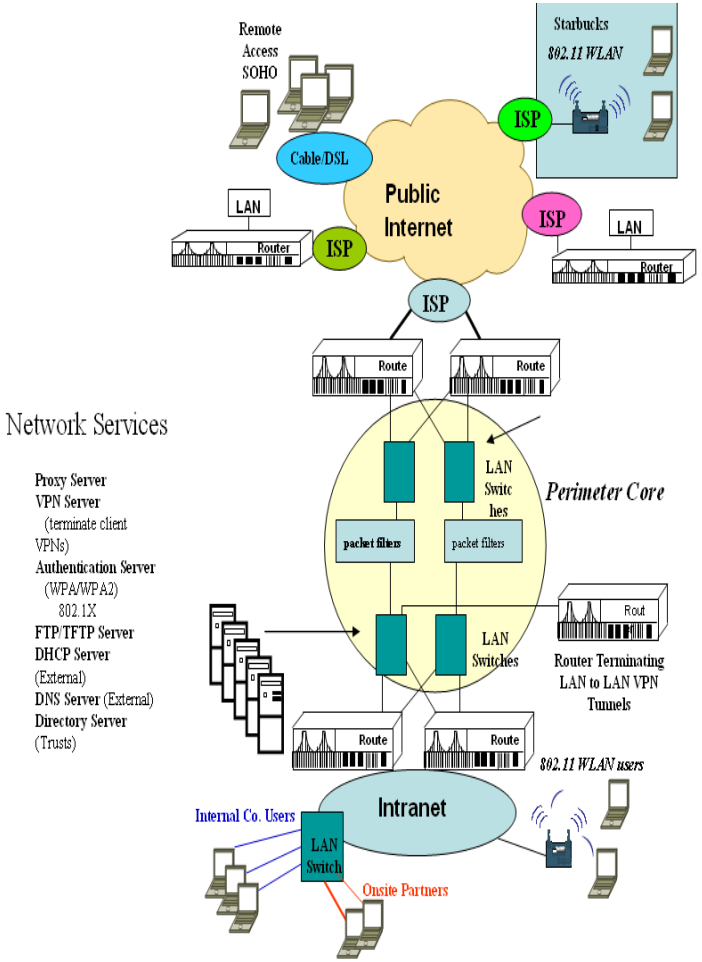
Network Architectures & Protocols

OSI Reference Model

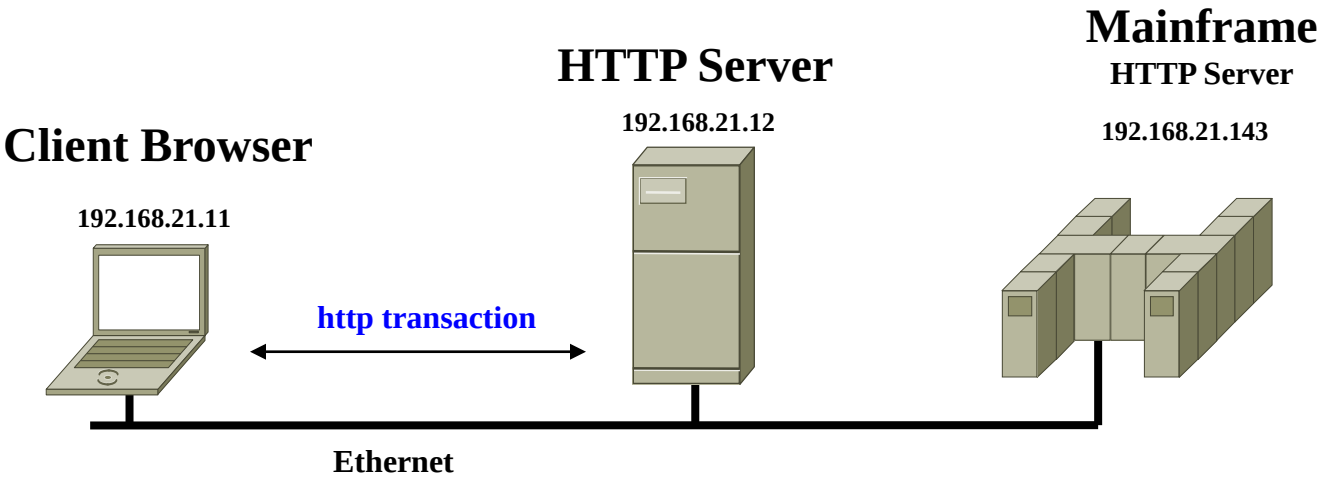


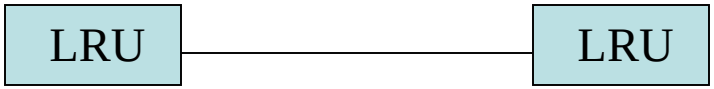
Application	End User Interface to net.
Presentation	Data Transform
Session	Synch end to end conversation
Transport	End to end service quality
Network	Routing data
LLC (Logical Link)	Framing, Error Detect/Correct
MAC (Media Access)	NIC (MAC add)
Physical	Media contention: CSMA/CSMA-CD

Physical Medium: UTP/Coax/Fiber/RF



Data Communications/Network Usage



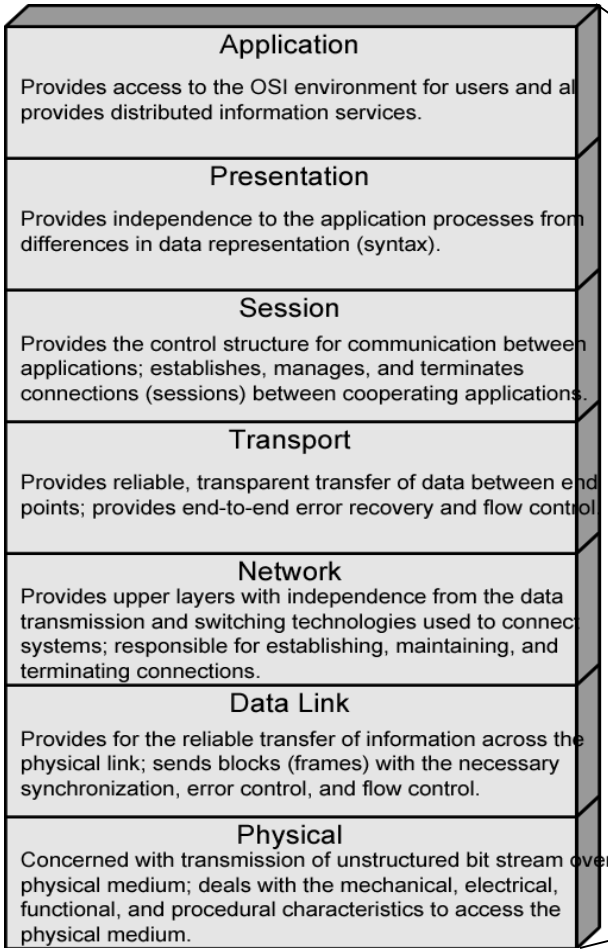


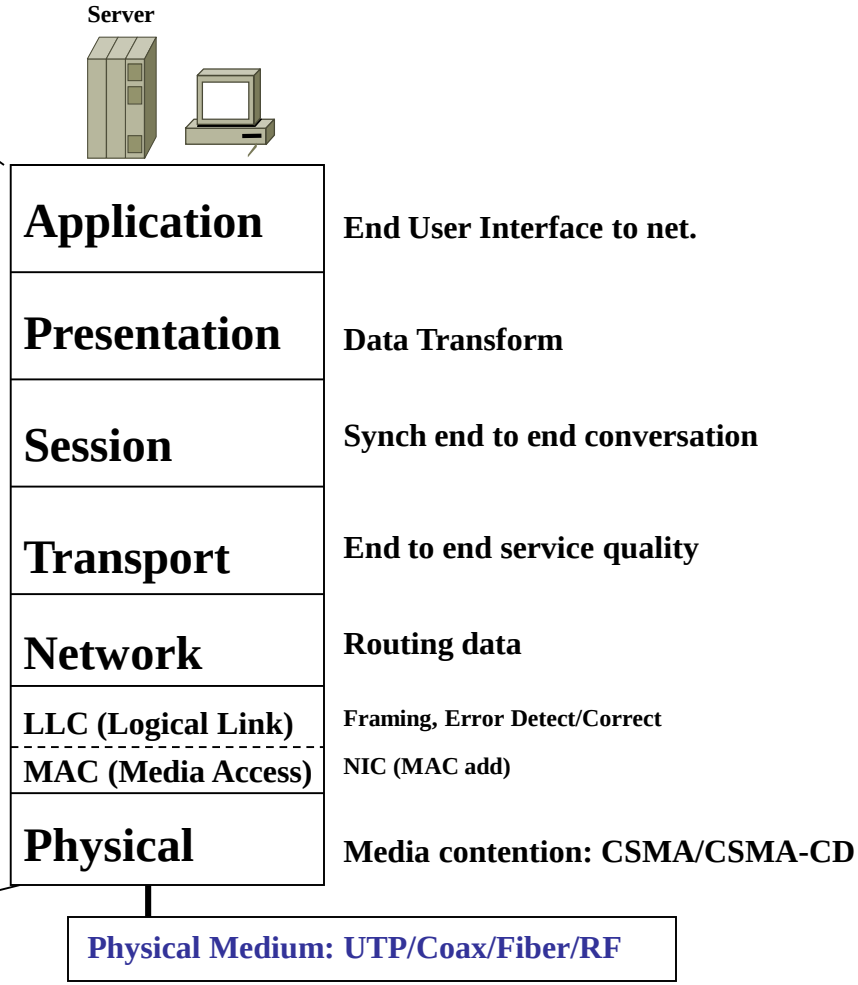
Point-to-point Ethernet

ARINC 429, 629
AFDX

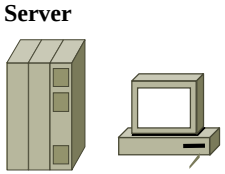
3G, 4G Cellular

OSI Reference Model





OSI Reference Model



Format recognizable to end system/appl.

upper layer protocols

lower layer protocols

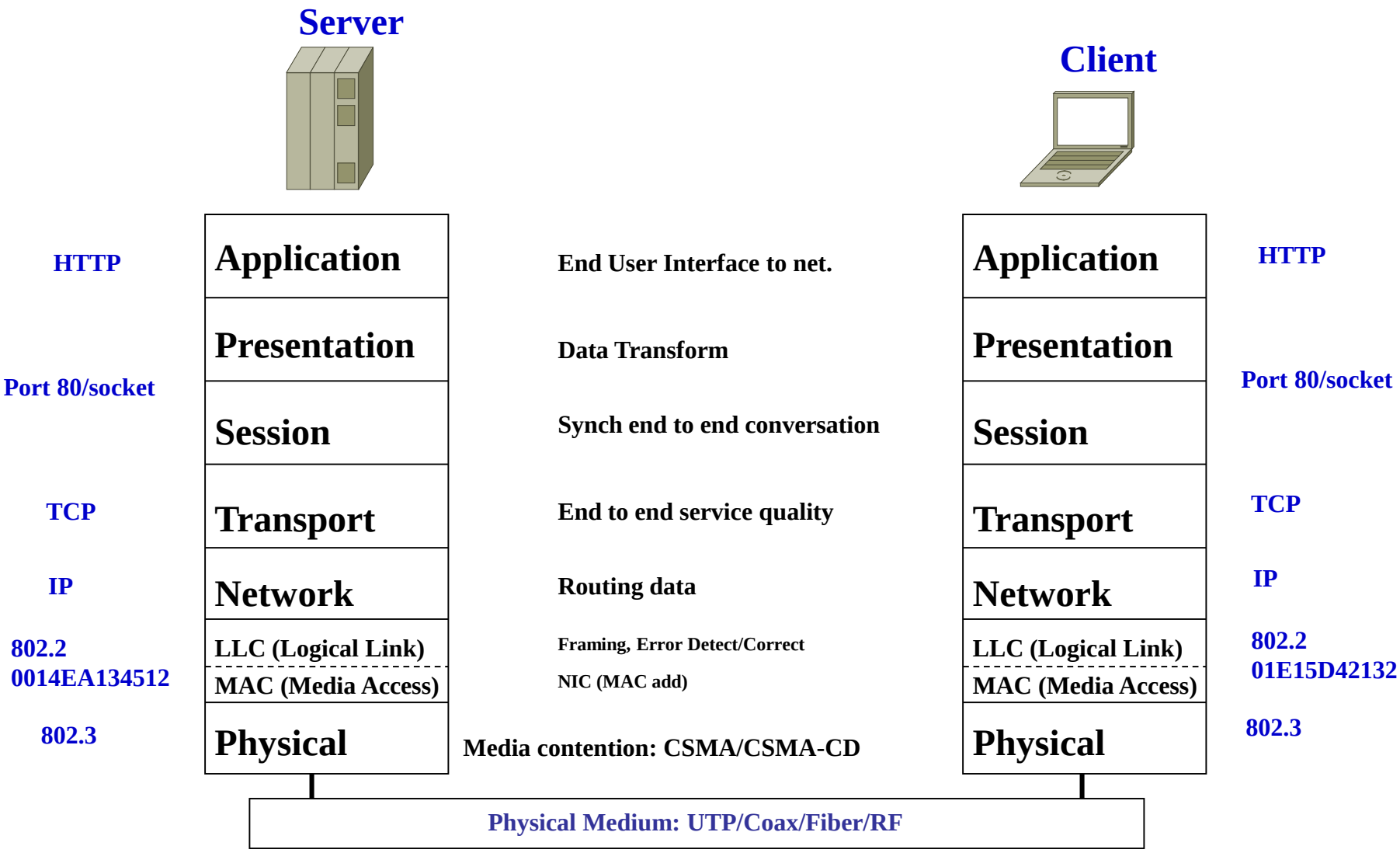
Fast, error free comm.

Application	**End User Interface to net.**
Presentation	**Data Transform**
Session	**Synch end to end conversation**
Transport	**End to end service quality**
Network	**Routing data**
LLC (Logical Link)	**Framing, Error Detect/Correct**
MAC (Media Access)	**NIC (MAC add)**
Physical	**Media contention: CSMA/CSMA-CD**

Physical Medium: UTP/Coax/Fiber/RF

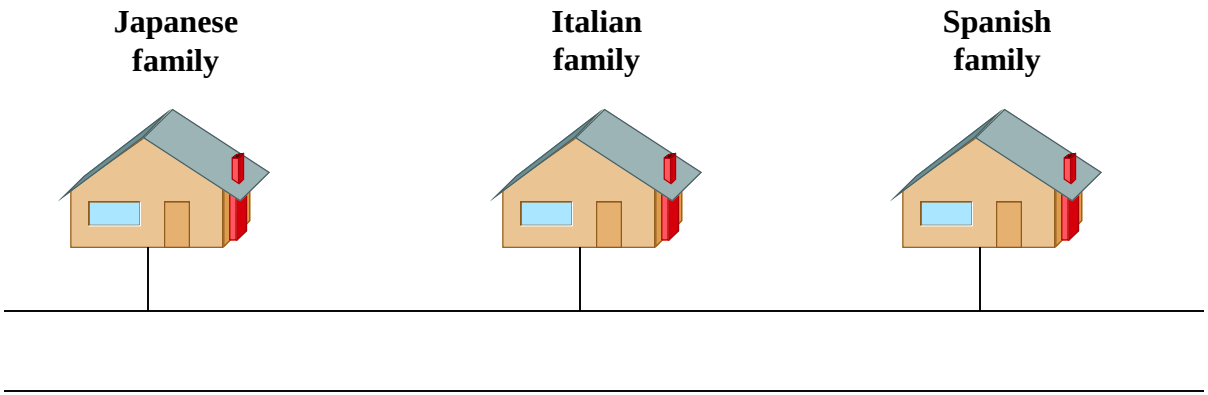
What protocols do you know ?

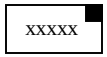
HTTP Session in Context of OSI Reference Model



Protocol Layering/Enveloping

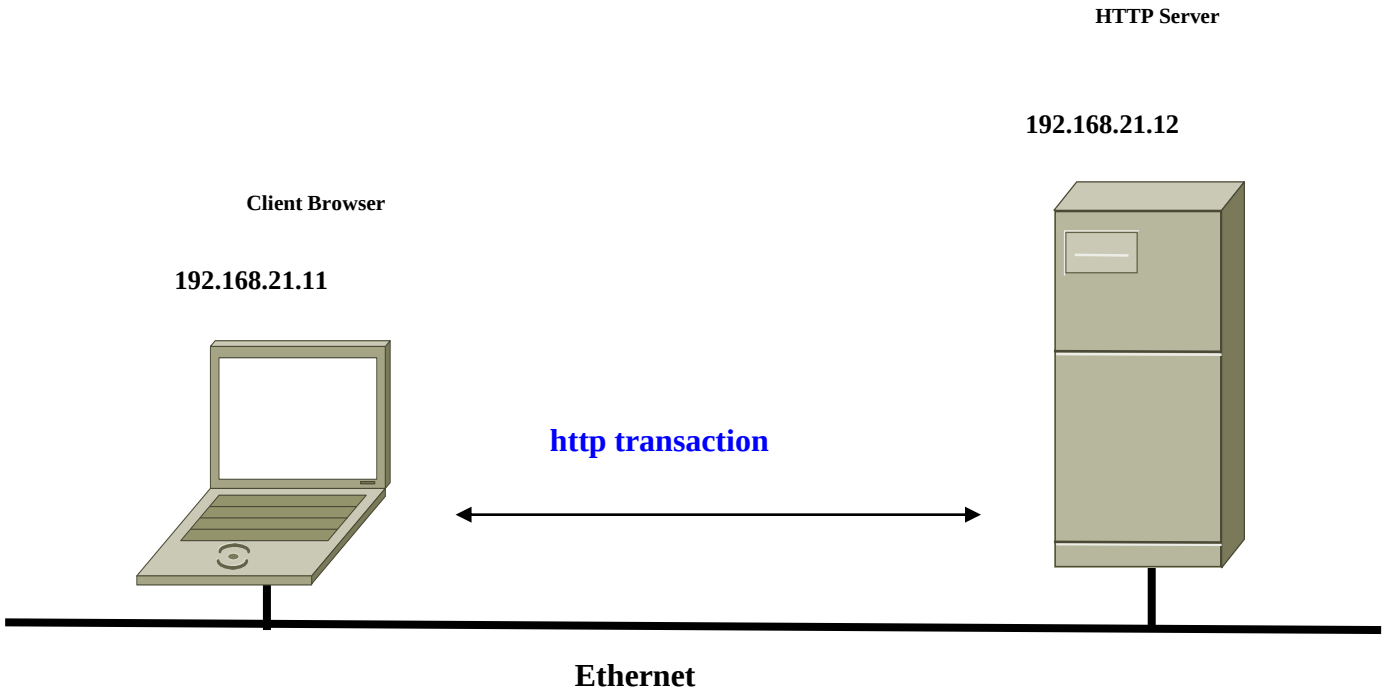
Anytown, USA



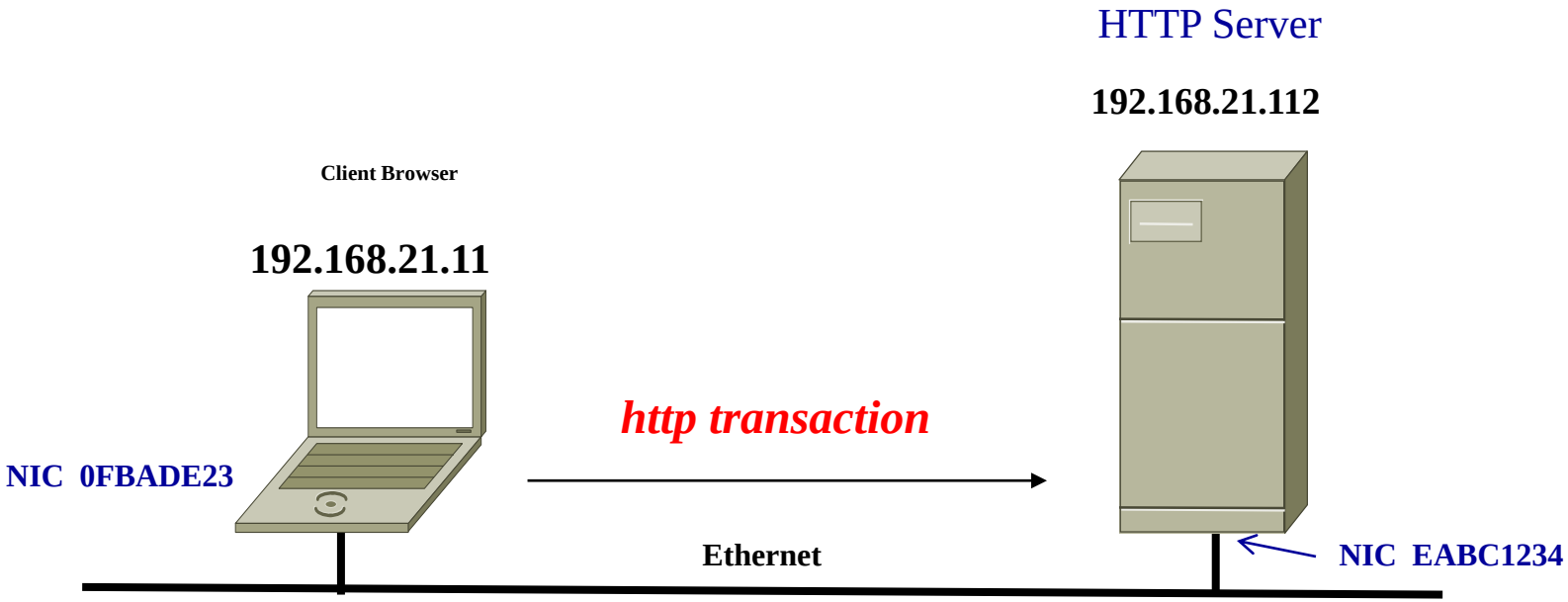


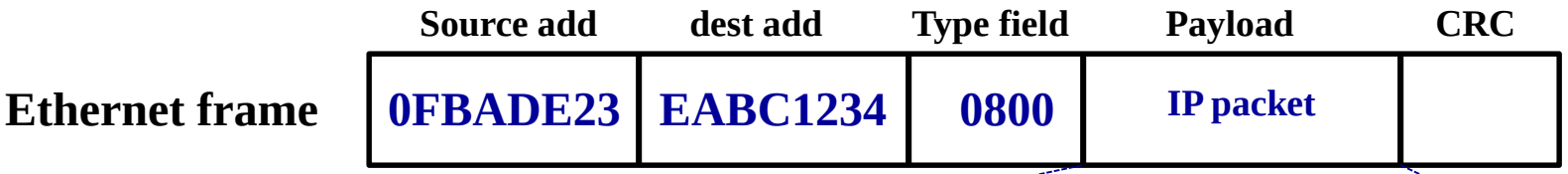
International Letter

Making Sense of the OSI Reference Model – Why do I Care ?

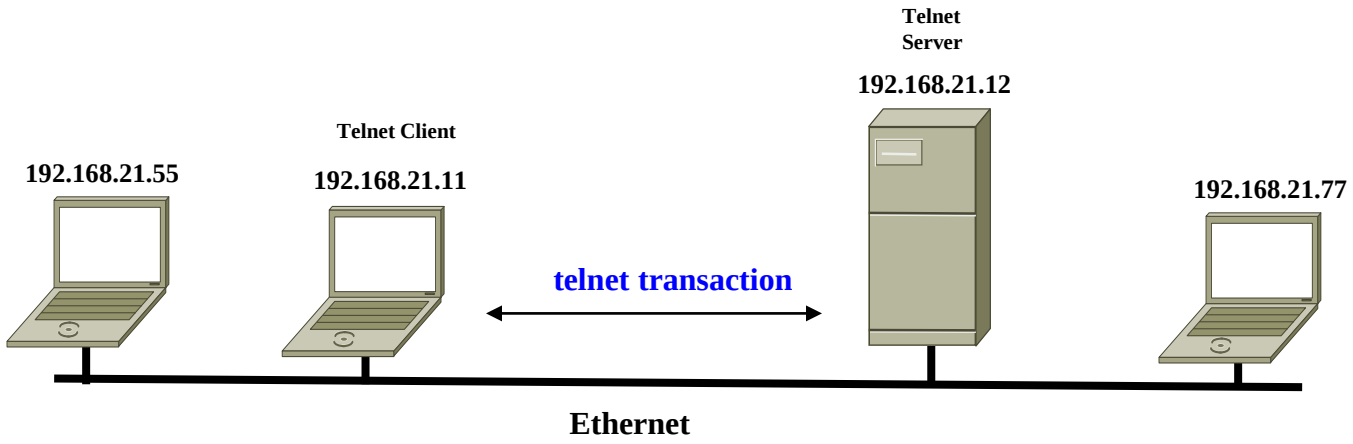


Making Sense of the OSI Reference Model – Why do I Care ?



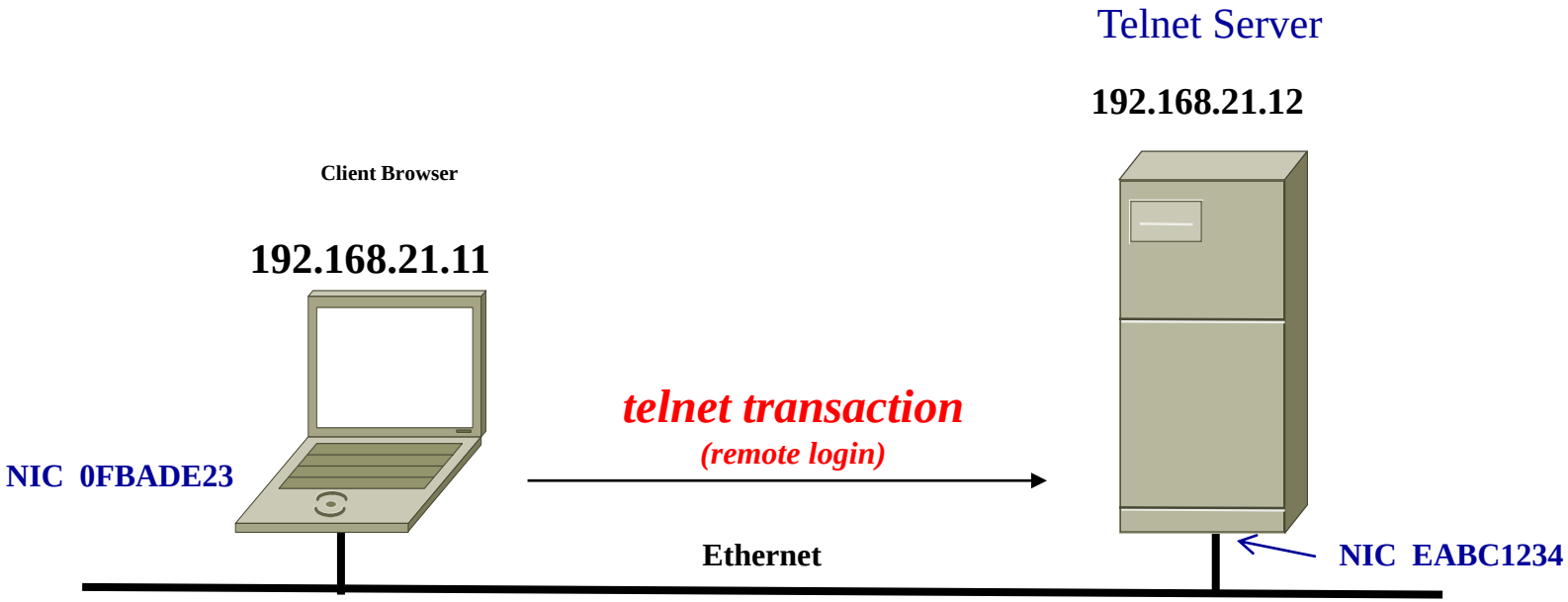


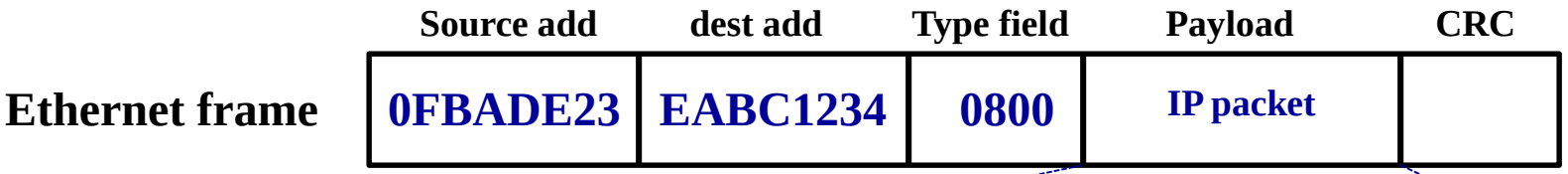
Making Sense of the OSI Reference Model – Why do I Care ?

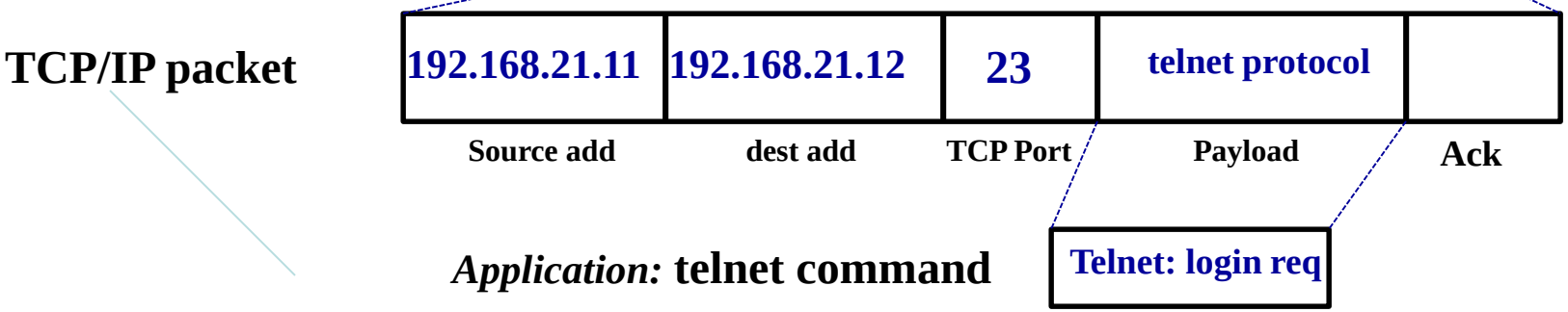


*** Telnet is an application which permits a device to remotely login**

Making Sense of the OSI Reference Model – Why do I Care ?







MAC Level Network Addressing

MAC Address Formats:

Source address & Destination Address:

Broadcast Address: Intended for everyone on the network**.**

Multicast Address: Intended for a subset of users on the network

Unicast: Intended for a single address on the network.

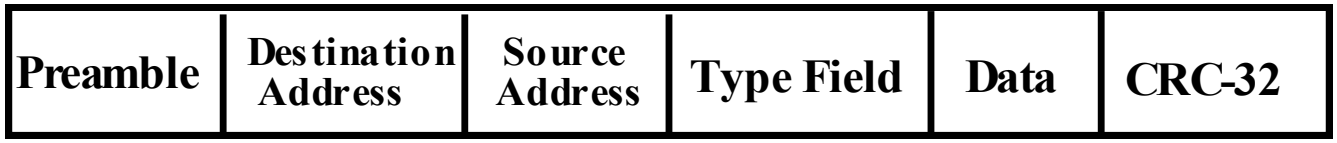
MAC Address Administration**:**

Globally administered addresses: are the addresses each LAN manufacturer assigns to each NIC (Network Interface Card) administered/allocated by the IEEE..

Locally Administered Address: using locally administered addresses, the network administrator or installer wants to assign a unique MAC address (many SNA Gateway)

Local administered addressing requires more overhead, does provide easier cutover methods, recognition of key MAC devices (by Address), possible convention map local administered address to building/floor/ location.

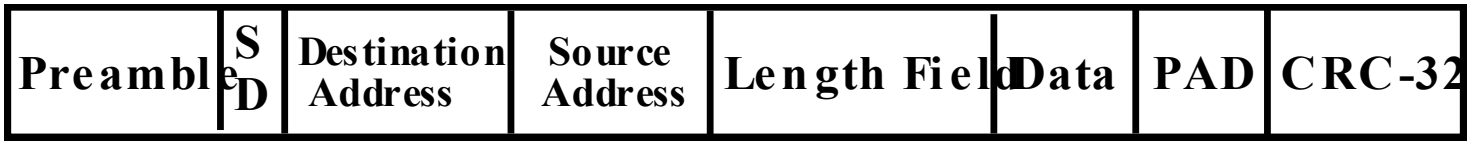
MAC Address Formats:



Ethernet (DIX) V2.0 Frame:

Preamble: Ethernet uses an 8 octet preamble & no starting delimiter, actual bit pattern being the same as the 802.3 format.

Type Field: The type field identifies the upper layer protocol carried within the frame. Vendors (manufacturers) are assigned 2 Octet type fields for each major protocol they register with Xerox.



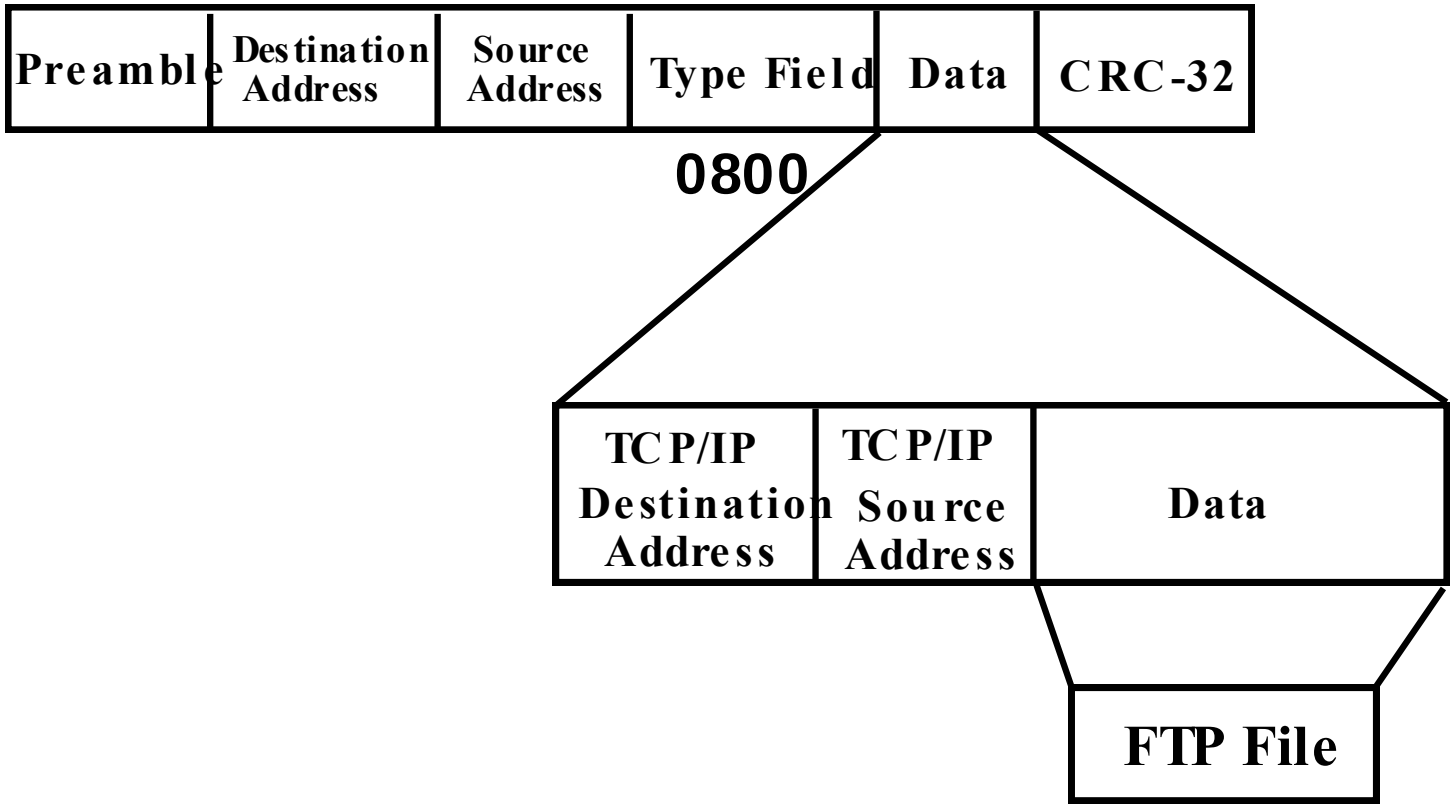
IEEE 802.3 Frame :

Preamble: 7 Octets used for bit synchronization (Alt 1s and 0s)
SD (Start Delimiter): 1 octet used for character synchronization
Destination Add: 6 octets (MAC Address)
Source Add: 6 octets (MAC Address)
Length: 2 octets used to indicated length of data field. * (Valid Range 3 - 1500 Bytes)
PAD (0 to 46 octets) Required
CRC - Cyclic Redundancy Check: standard Frame Check Sequence to validate integrity of the Ethernet frame.

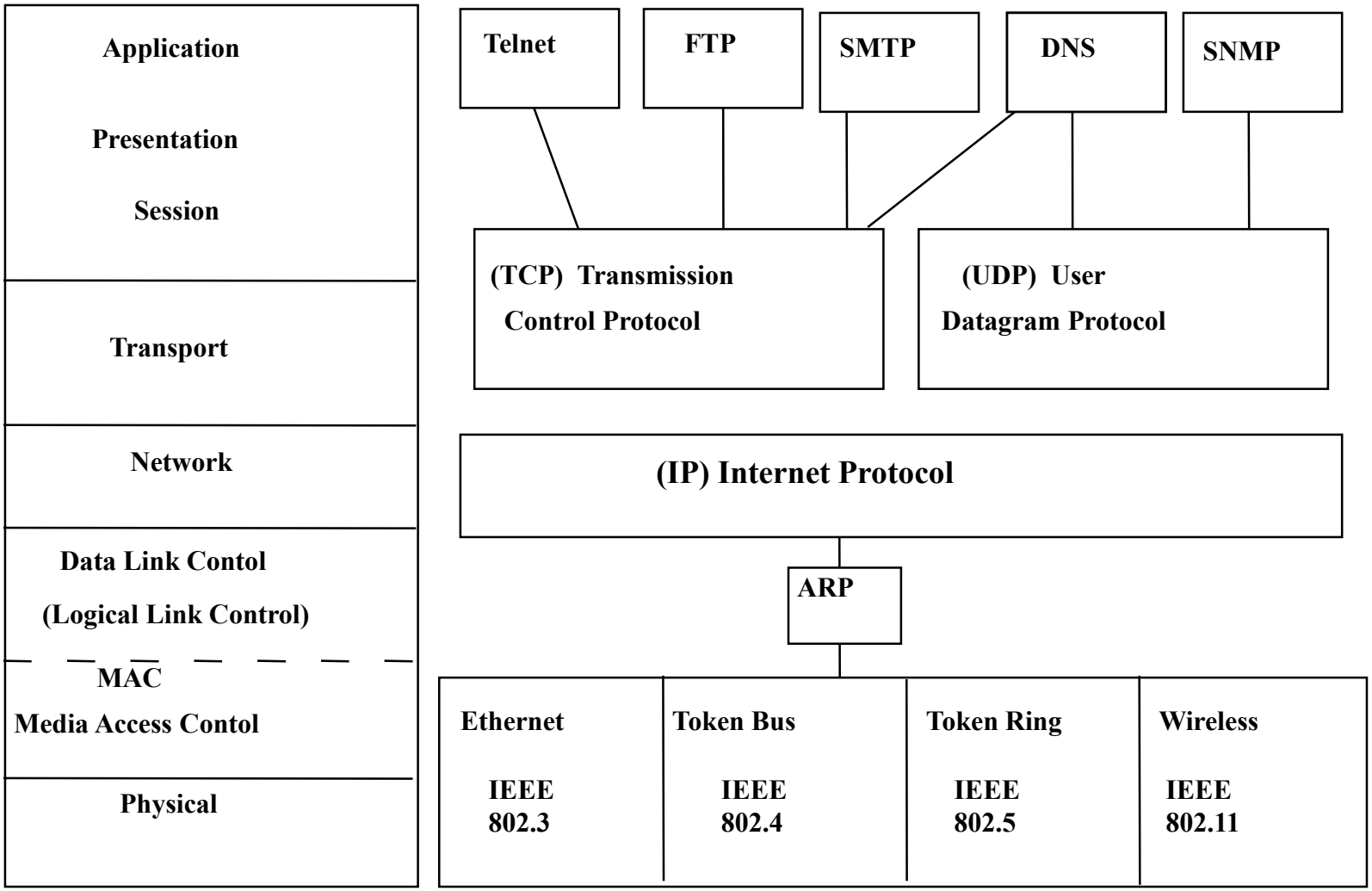
PDU (Protocol Data Unit)

The Data section of an Ethernet Packet may contain about anything in any format. Ethernet does not interpret the data section, except to look at the protocol type field or length. The data section must be a minimum length of 46 bytes, even if there is only 1 byte to send, and may be as large as 1500 bytes. Typically the data section would contain the protocol packet used by upper layer software such as TCP/IP, XNS, IPX, SNA, MOP, LAT....

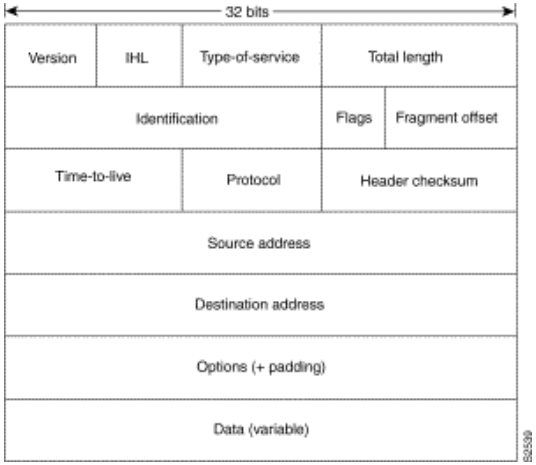
The following diagram illustrates a FTP request from an end user in a TCP/IP frame over an Ethernet network.



TCP/IP Protocol Suite



TCP/IP Packet



Fields comprising an IP packet.

- ***Version-***--Indicates the version of IP currently used.
- ***IP Header Length*** *(*IHL)---Indicates the datagram header length in 32-bit words.
- ***Type-of-Service***--Specifies how an upper-layer protocol would like a current datagram to be handled, assigns priority lvl.
- ***Total Length-***-Specifies the length, in bytes, of the entire IP packet, including the data and header.
- ***Identification***--Contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.
- ***Flags---***3-bit field of which the two low-order (least-significant) bits control fragmentation. Low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets.
- ***Fragment Offset***--Indicates the position of the fragment's data relative to the beginning of the data in the original datagram.
- ***Time-to-Live---***Maintains counter gradually decrements down to zero, then datagram is discarded. Keeps packets from looping.
- ***Protocol***--Indicates which upper-layer protocol receives incoming packets after IP processing is complete.
- ***Header Checksum-***--Helps ensure IP header integrity.
- ***Source Address***--Specifies the sending node.
- ***Destination Address***--Specifies the receiving node.
- ***Options***--Allows IP to support various options, such as security.
- ***Data***--Contains upper-layer information.

TCP/IP Application Layer Protocols

FTP (File Transfer Protocol) - allows the user to send or retrieve entire files interactively. FTP follows a client/server mode; a client send commands and interacts with the user, a server receives and responds to the commands.

SMTP (Simple Mail Transfer Protocol) is an electronic mail protocol which uses a TCP virtual circuit to transmit and relay mail. SMTP implementations usually return undeliverable mail automatically.

TELNET (Remote Access Protocol) is an interactive, remote access, terminal protocol, allowing the user to log in and use a remote computer system on the network as though your terminal were directly connected to the remote machine.

Domain Name Services (DNS) enables a device to be referenced by a special name (as opposed to a TCP/IP number). In this manner a computer such as homer (homer@u.washington.edu) can be accessed by a common naming system.

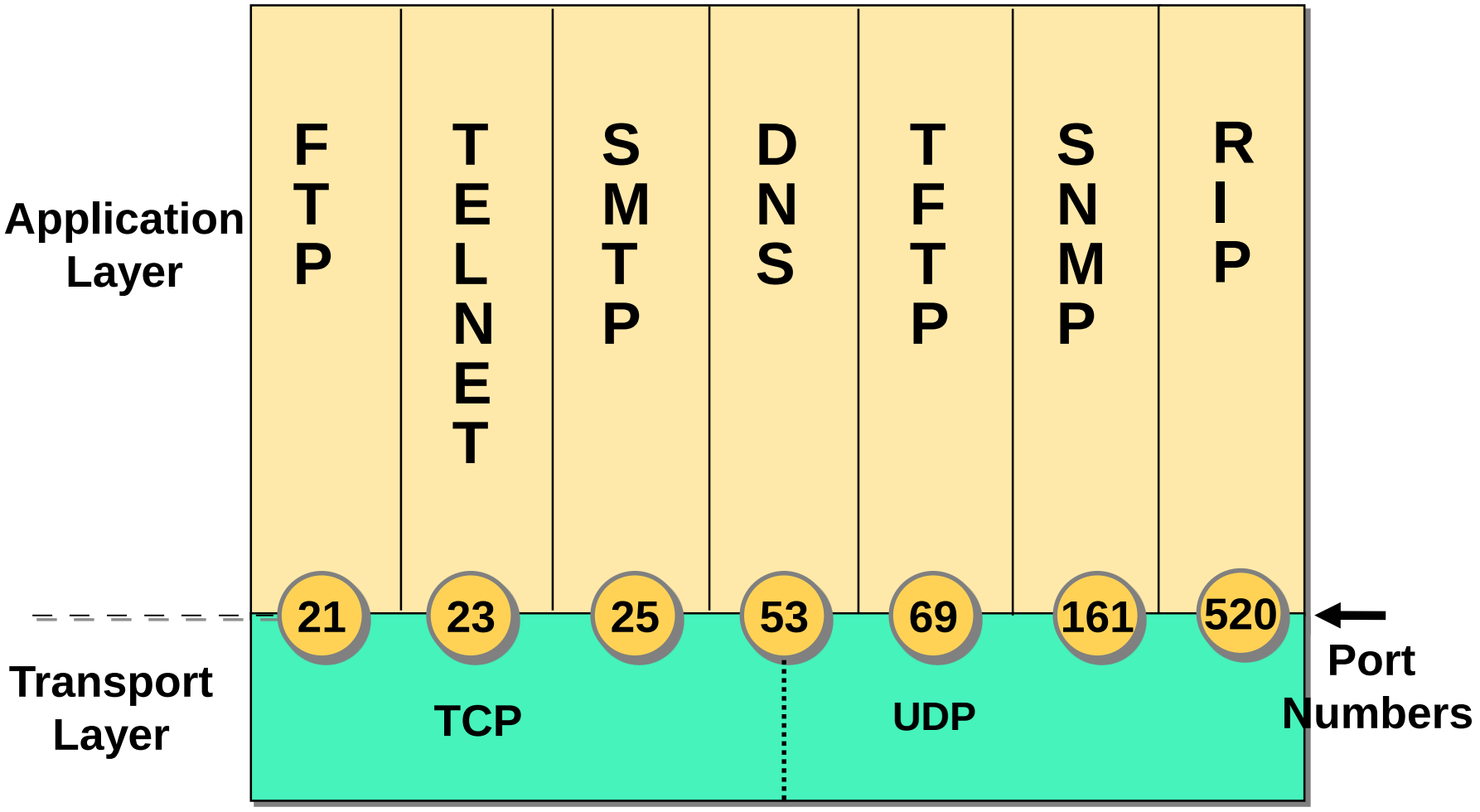
Simple Network Management Protocol (SNMP) uses SNMP agents that reside in network devices (concentrators, bridges, routers, servers) collects data (statistics) that are transported back over UDP to a SNMP Manager.

Network File Server (NFS) is a set of protocols developed by Sun Microsystems to allow multiple devices to access each others directories (the interconnected devices files/directories appear as if they are locally attached). NFS is commonly used by larger UNIX workstations and typically places extremely large bandwidth requirements on the network supporting it. Extremely difficult to support well over a WAN (Wide Area Network) environment.

Remote Procedure Calls (RPCs) are functions that enable applications to communicate with other machines (typically servers). RPCs provide for programming functions, return codes and variables (user definable) to support distributed computing.

Trivial File Transfer Protocol (TFTP) is a simple, unsophisticated file transfer protocol that lacks error checking (uses UDP). TFTP is typically used to download images (software/microcode) to flash memory in bridges, routers or PCs.

Port Numbers



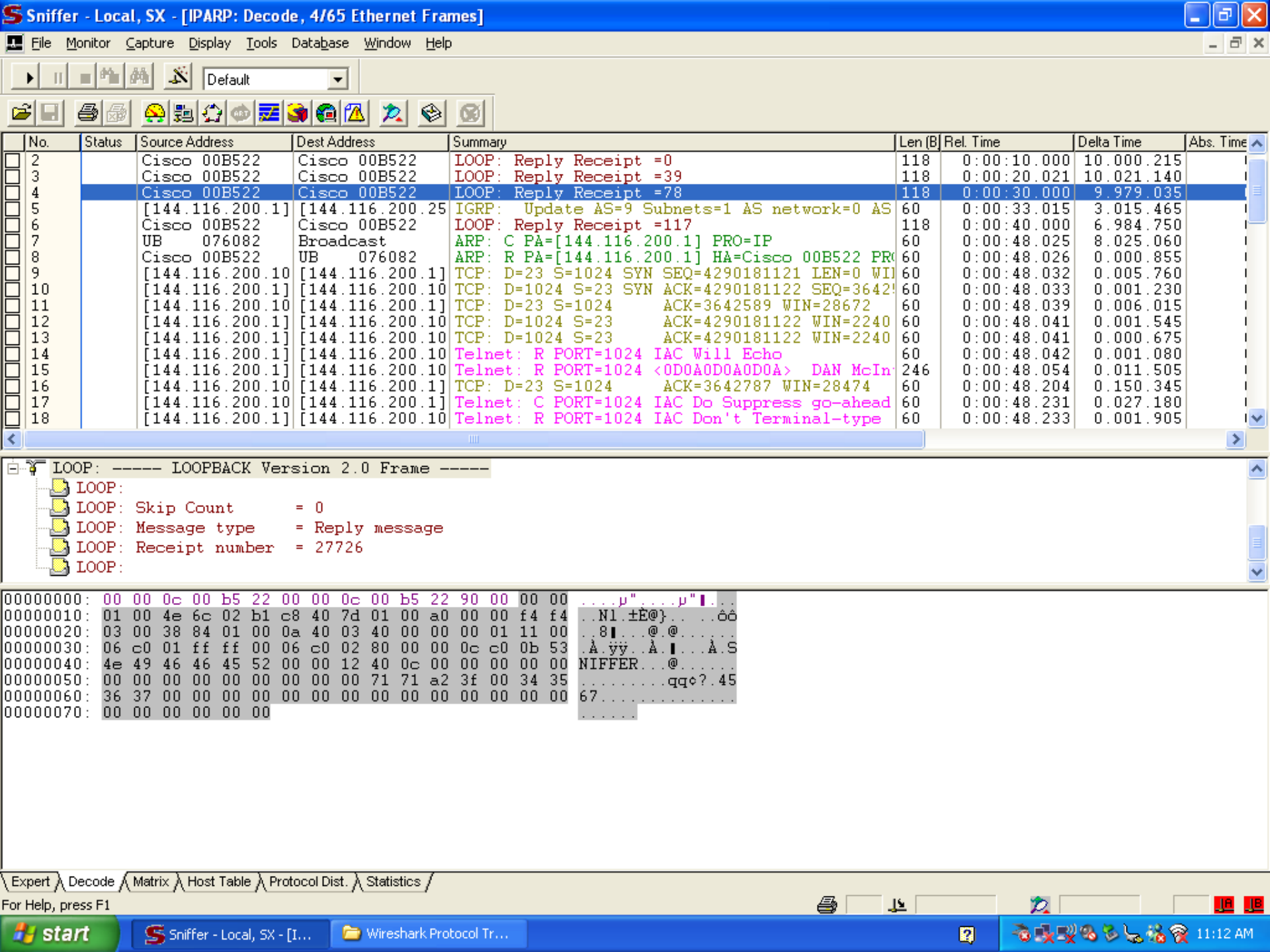
Key Takeaway

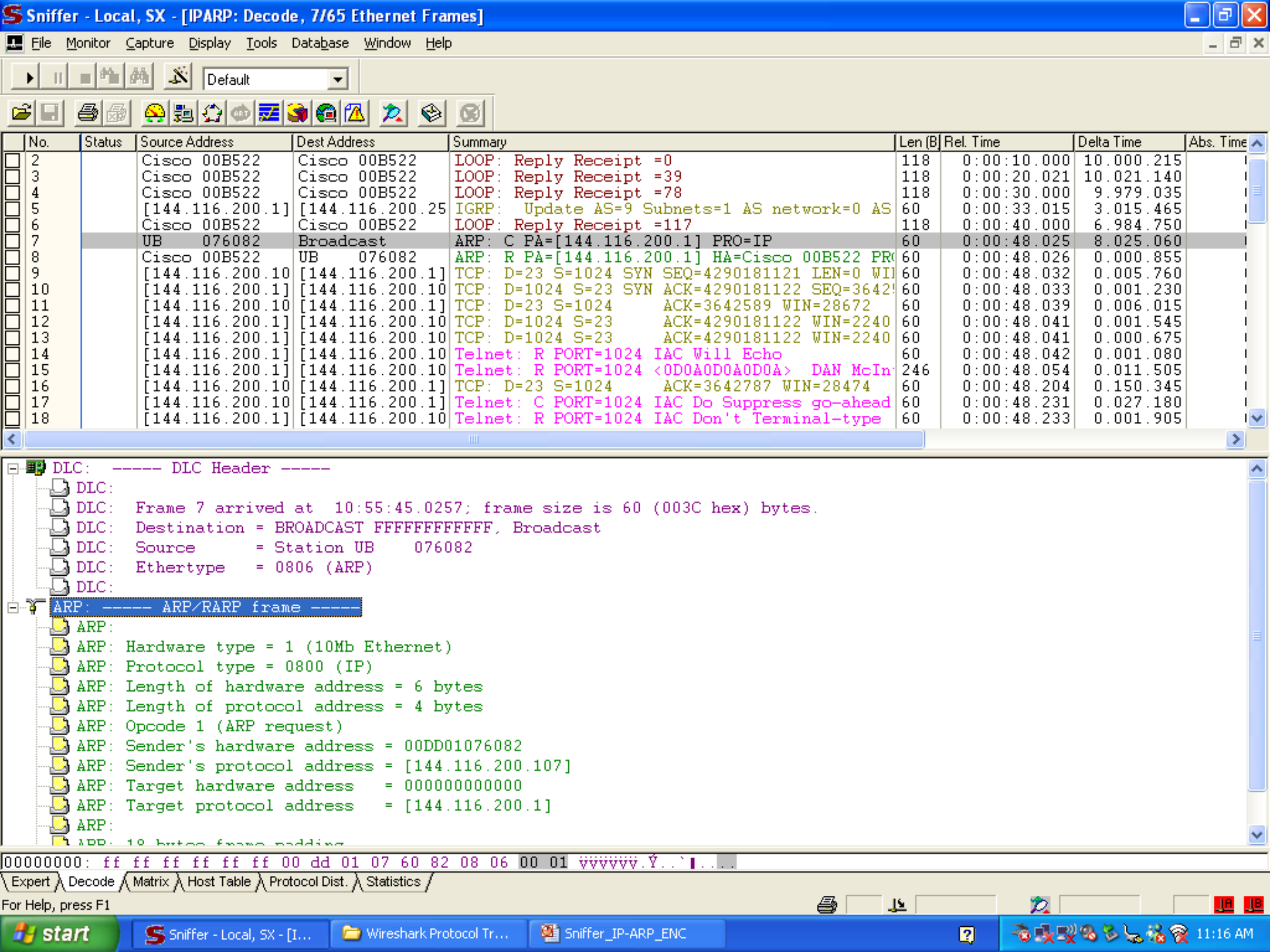
The primary components and strategies of cyber security/IA are network centric based.

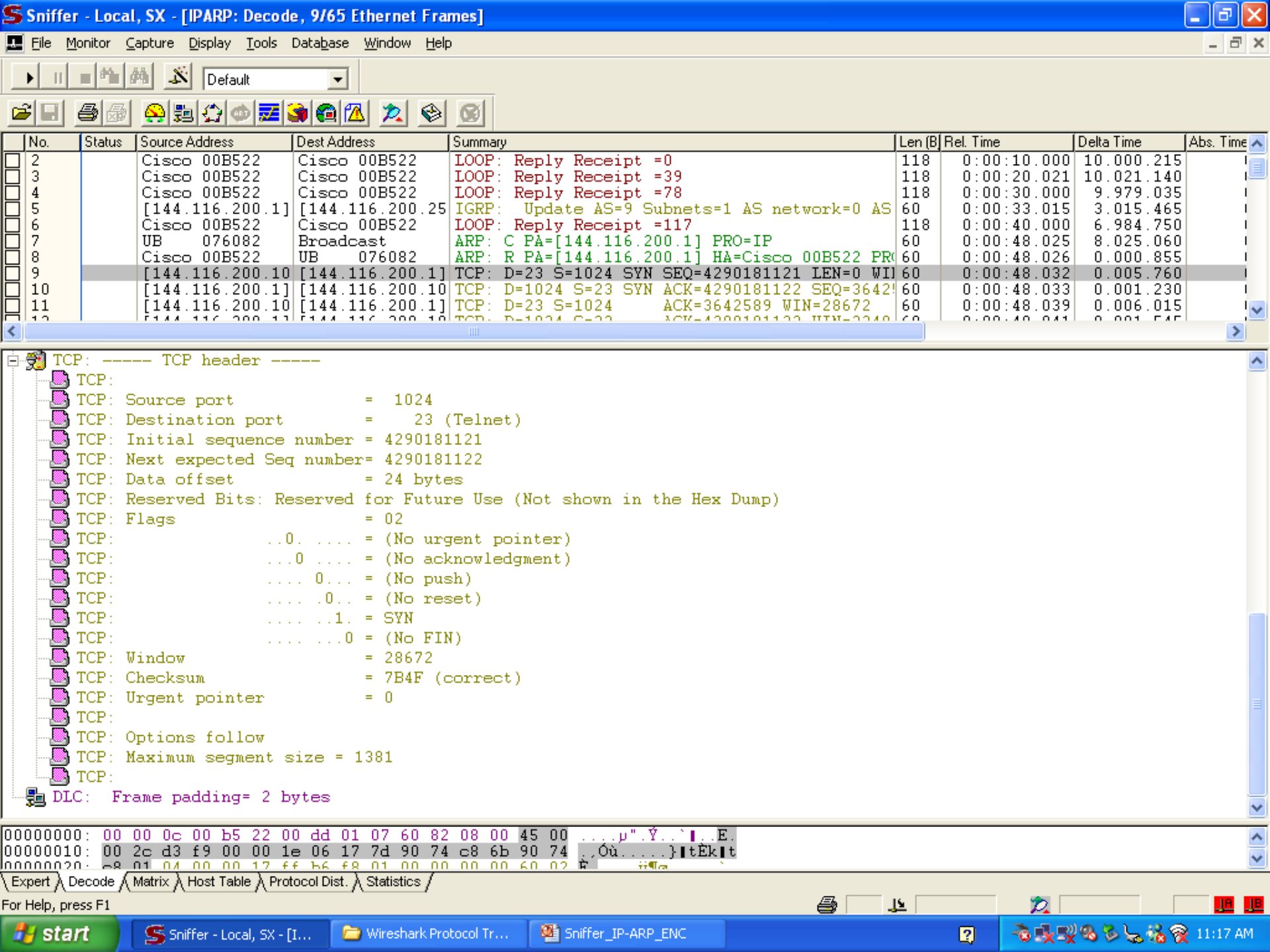
They attempt to inspect, monitor, filter/block traffic on network based mechanisms;

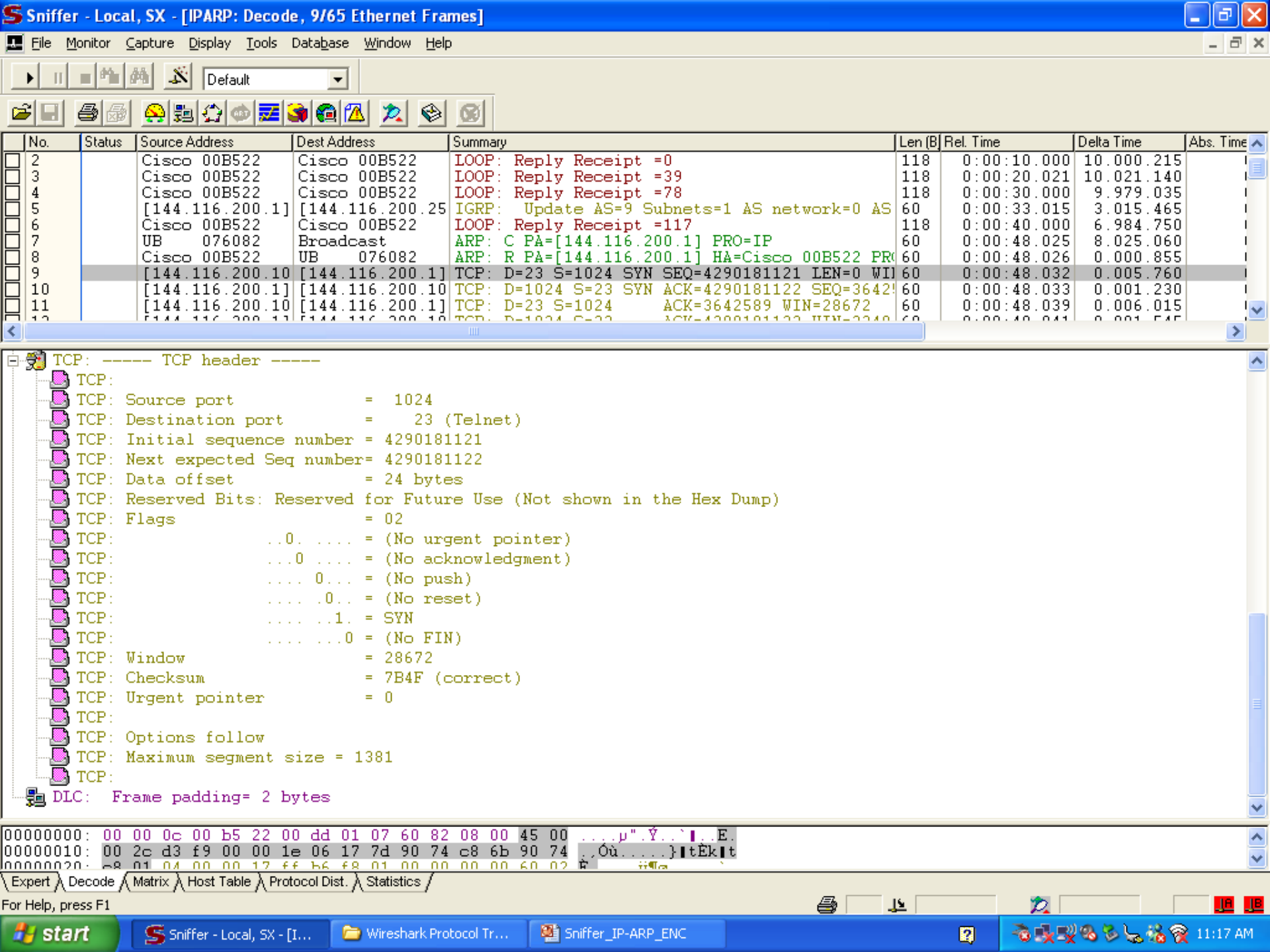
- **internet protocol (IP) address**
- **IP TCP/UDP port**
- **network access control lists (ACLs)**

Ethernet frames and TCP/IP Packets

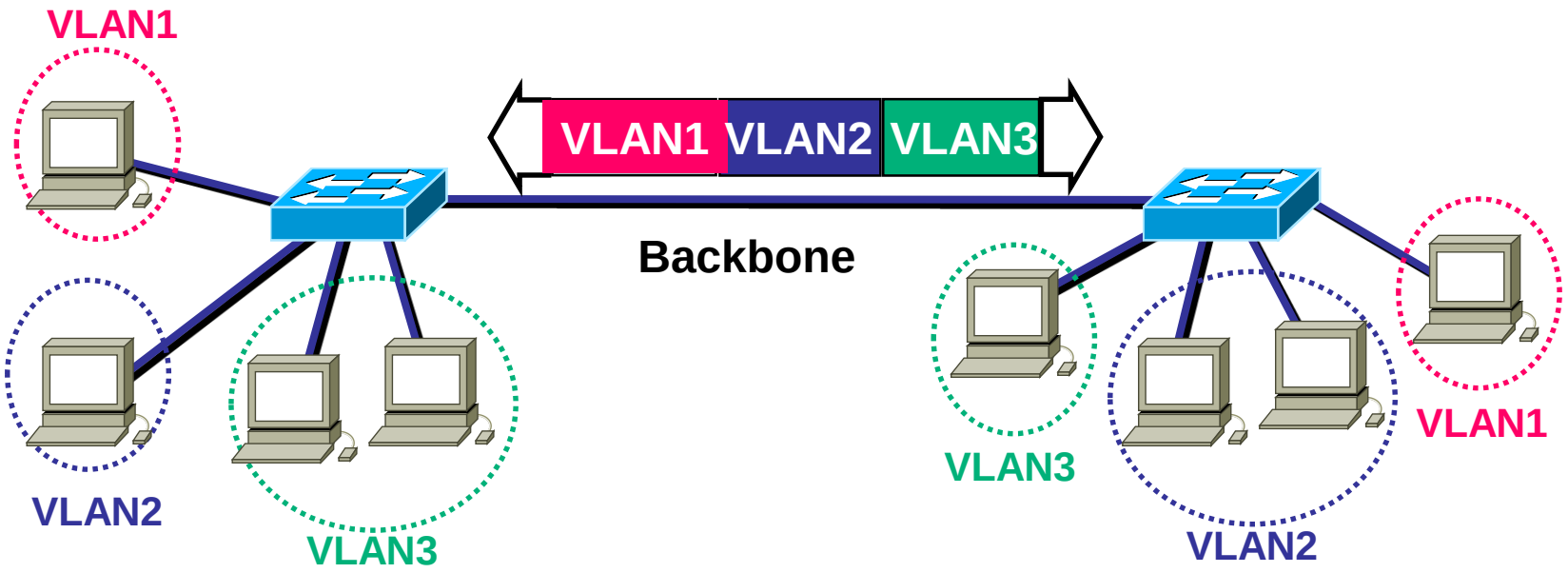

Sniffer - Local, SX - [IPARP: Decode, 4/65 Ethernet Frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len (B Rel. Time Delta Time Abs. Time
2 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =0 118 0:00:10.000 10.000.215
3 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =39 118 0:00:20.021 10.021.140
4 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =78 118 0:00:30.000 9.979.035
5 [144.116.200.1] [144.116.200.25 IGRP: Update AS=9 Subnets=1 AS network=0 AS 60 0:00:33.015 3.015.465
6 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =117 118 0:00:40.000 6.984.750
7 UB 076082 Broadcast ARP: C PA=[144.116.200.1] PRO=IP 60 0:00:48.025 8.025.060
8 Cisco 00B522 UB 076082 ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR 60 0:00:48.026 0.000.855
9 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI 60 0:00:48.032 0.005.760
10 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642 60 0:00:48.033 0.001.230
11 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 ACK=3642589 WIN=28672 60 0:00:48.039 0.006.015
12 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 ACK=4290181122 WIN=2240 60 0:00:48.041 0.001.545
13 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 ACK=4290181122 WIN=2240 60 0:00:48.041 0.000.675
14 [144.116.200.1] [144.116.200.10 Telnet: R PORT=1024 IAC Will Echo 60 0:00:48.042 0.001.080
15 [144.116.200.1] [144.116.200.10 Telnet: R PORT=1024 <0D0A0D0A0D0A> DAN McIn 246 0:00:48.054 0.011.505
16 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 ACK=3642787 WIN=28474 60 0:00:48.204 0.150.345
17 [144.116.200.10 [144.116.200.1] Telnet: C PORT=1024 IAC Do Suppress go-ahead 60 0:00:48.231 0.027.180
18 [144.116.200.1] [144.116.200.10 Telnet: R PORT=1024 IAC Don't Terminal-type 60 0:00:48.233 0.001.905
LOOP: ----- LOOPBACK Version 2.0 Frame -----
LOOP:
LOOP: Skip Count = 0
LOOP: Message type = Reply message
LOOP: Receipt number = 27726
LOOP:
00000000: 00 00 0c 00 b5 22 00 00 0c 00 b5 22 90 00 00 00 ....µ"....µ"▌...
00000010: 01 00 4e 6c 02 b1 c8 40 7d 01 00 a0 00 00 f4 f4 ..Nl.±È@}.. ..ôô
00000020: 03 00 38 84 01 00 0a 40 03 40 00 00 00 01 11 00 ..8▌...@.@......
00000030: 06 c0 01 ff ff 00 06 c0 02 80 00 00 0c c0 0b 53 .À.ÿÿ..À.▌...À.S
00000040: 4e 49 46 46 45 52 00 00 12 40 0c 00 00 00 00 00 NIFFER...@......
00000050: 00 00 00 00 00 00 00 00 00 71 71 a2 3f 00 34 35 ....qq¢?.45
00000060: 36 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 67..............
00000070: 00 00 00 00 00 00 ......
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
start
Sniffer - Local, SX - [I...
Wireshark Protocol Tr...
11:12 AM


Sniffer - Local, SX - [IPARP: Decode, 7/65 Ethernet Frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len (B Rel. Time Delta Time Abs. Time
2 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =0 118 0:00:10.000 10.000.215
3 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =39 118 0:00:20.021 10.021.140
4 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =78 118 0:00:30.000 9.979.035
5 [144.116.200.1] [144.116.200.25 IGRP: Update AS=9 Subnets=1 AS network=0 AS 60 0:00:33.015 3.015.465
6 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =117 118 0:00:40.000 6.984.750
7 UB 076082 Broadcast ARP: C PA=[144.116.200.1] PRO=IP 60 0:00:48.025 8.025.060
8 Cisco 00B522 UB 076082 ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR 60 0:00:48.026 0.000.855
9 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI 60 0:00:48.032 0.005.760
10 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642 60 0:00:48.033 0.001.230
11 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 ACK=3642589 WIN=28672 60 0:00:48.039 0.006.015
12 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 ACK=4290181122 WIN=2240 60 0:00:48.041 0.001.545
13 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 ACK=4290181122 WIN=2240 60 0:00:48.041 0.000.675
14 [144.116.200.1] [144.116.200.10 Telnet: R PORT=1024 IAC Will Echo 60 0:00:48.042 0.001.080
15 [144.116.200.1] [144.116.200.10 Telnet: R PORT=1024 <0D0A0D0A0D0A> DAN McIn 246 0:00:48.054 0.011.505
16 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 ACK=3642787 WIN=28474 60 0:00:48.204 0.150.345
17 [144.116.200.10 [144.116.200.1] Telnet: C PORT=1024 IAC Do Suppress go-ahead 60 0:00:48.231 0.027.180
18 [144.116.200.1] [144.116.200.10 Telnet: R PORT=1024 IAC Don't Terminal-type 60 0:00:48.233 0.001.905
DLC: ----- DLC Header -----
DLC:
DLC: Frame 7 arrived at 10:55:45.0257; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station UB 076082
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 1 (ARP request)
ARP: Sender's hardware address = 00DD01076082
ARP: Sender's protocol address = [144.116.200.107]
ARP: Target hardware address = 000000000000
ARP: Target protocol address = [144.116.200.1]
ARP:
00000000: ff ff ff ff ff ff 00 dd 01 07 60 82 08 06 00 01
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
start
Sniffer - Local, SX - [I...
Wireshark Protocol Tr...
Sniffer_IP-ARP_ENC
11:16 AM


Sniffer - Local, SX - [IPARP: Decode, 9/65 Ethernet Frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len (B Rel. Time Delta Time Abs. Time
2 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =0 118 0:00:10.000 10.000.215
3 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =39 118 0:00:20.021 10.021.140
4 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =78 118 0:00:30.000 9.979.035
5 [144.116.200.1] [144.116.200.25 IGRP: Update AS=9 Subnets=1 AS network=0 AS 60 0:00:33.015 3.015.465
6 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =117 118 0:00:40.000 6.984.750
7 UB 076082 Broadcast ARP: C PA=[144.116.200.1] PRO=IP 60 0:00:48.025 8.025.060
8 Cisco 00B522 UB 076082 ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR 60 0:00:48.026 0.000.855
9 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI 60 0:00:48.032 0.005.760
10 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642 60 0:00:48.033 0.001.230
11 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 ACK=3642589 WIN=28672 60 0:00:48.039 0.006.015
TCP: ----- TCP header -----
TCP:
TCP: Source port = 1024
TCP: Destination port = 23 (Telnet)
TCP: Initial sequence number = 4290181121
TCP: Next expected Seq number= 4290181122
TCP: Data offset = 24 bytes
TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
TCP: Flags = 02
TCP: ..0. .... = (No urgent pointer)
TCP: ...0 .... = (No acknowledgment)
TCP: .... 0... = (No push)
TCP: .... .0.. = (No reset)
TCP: .... ..1. = SYN
TCP: ....0 = (No FIN)
TCP: Window = 28672
TCP: Checksum = 7B4F (correct)
TCP: Urgent pointer = 0
TCP:
TCP: Options follow
TCP: Maximum segment size = 1381
TCP:
DLC: Frame padding= 2 bytes
00000000: 00 00 0c 00 b5 22 00 dd 01 07 60 82 08 00 45 00 ....µ".Ý..`‚..E.
00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74 .,Óù.....}tÈk.t
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
start
Sniffer - Local, SX - [I...
Wireshark Protocol Tr...
Sniffer_IP-ARP_ENC
11:17 AM


Sniffer - Local, SX - [IPARP: Decode, 9/65 Ethernet Frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len (B Rel. Time Delta Time Abs. Time
2 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =0 118 0:00:10.000 10.000.215
3 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =39 118 0:00:20.021 10.021.140
4 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =78 118 0:00:30.000 9.979.035
5 [144.116.200.1] [144.116.200.25 IGRP: Update AS=9 Subnets=1 AS network=0 AS 60 0:00:33.015 3.015.465
6 Cisco 00B522 Cisco 00B522 LOOP: Reply Receipt =117 118 0:00:40.000 6.984.750
7 UB 076082 Broadcast ARP: C PA=[144.116.200.1] PRO=IP 60 0:00:48.025 8.025.060
8 Cisco 00B522 UB 076082 ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR 60 0:00:48.026 0.000.855
9 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI 60 0:00:48.032 0.005.760
10 [144.116.200.1] [144.116.200.10 TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642 60 0:00:48.033 0.001.230
11 [144.116.200.10 [144.116.200.1] TCP: D=23 S=1024 ACK=3642589 WIN=28672 60 0:00:48.039 0.006.015
TCP: ----- TCP header -----
TCP:
TCP: Source port = 1024
TCP: Destination port = 23 (Telnet)
TCP: Initial sequence number = 4290181121
TCP: Next expected Seq number= 4290181122
TCP: Data offset = 24 bytes
TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
TCP: Flags = 02
TCP: ..0. .... = (No urgent pointer)
TCP: ...0 .... = (No acknowledgment)
TCP: .... 0... = (No push)
TCP: .... .0.. = (No reset)
TCP: .... ..1. = SYN
TCP: ....0 = (No FIN)
TCP: Window = 28672
TCP: Checksum = 7B4F (correct)
TCP: Urgent pointer = 0
TCP:
TCP: Options follow
TCP: Maximum segment size = 1381
TCP:
DLC: Frame padding= 2 bytes
00000000: 00 00 0c 00 b5 22 00 dd 01 07 60 82 08 00 45 00 ....µ".Ý..`‚..E.
00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74 .,Óù.....}tÈk.t
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
start
Sniffer - Local, SX - [I...
Wireshark Protocol Tr...
Sniffer_IP-ARP_ENC
11:17 AM

VLAN Frame Identification



- Specifically developed for multi-VLAN, inter-switch communications
- Places a unique identifier in header of each frame
- Functions at Layer 2

Routers Forward Traffic

Routing protocols maintain neighbor relationships with adjacent (connected) routers

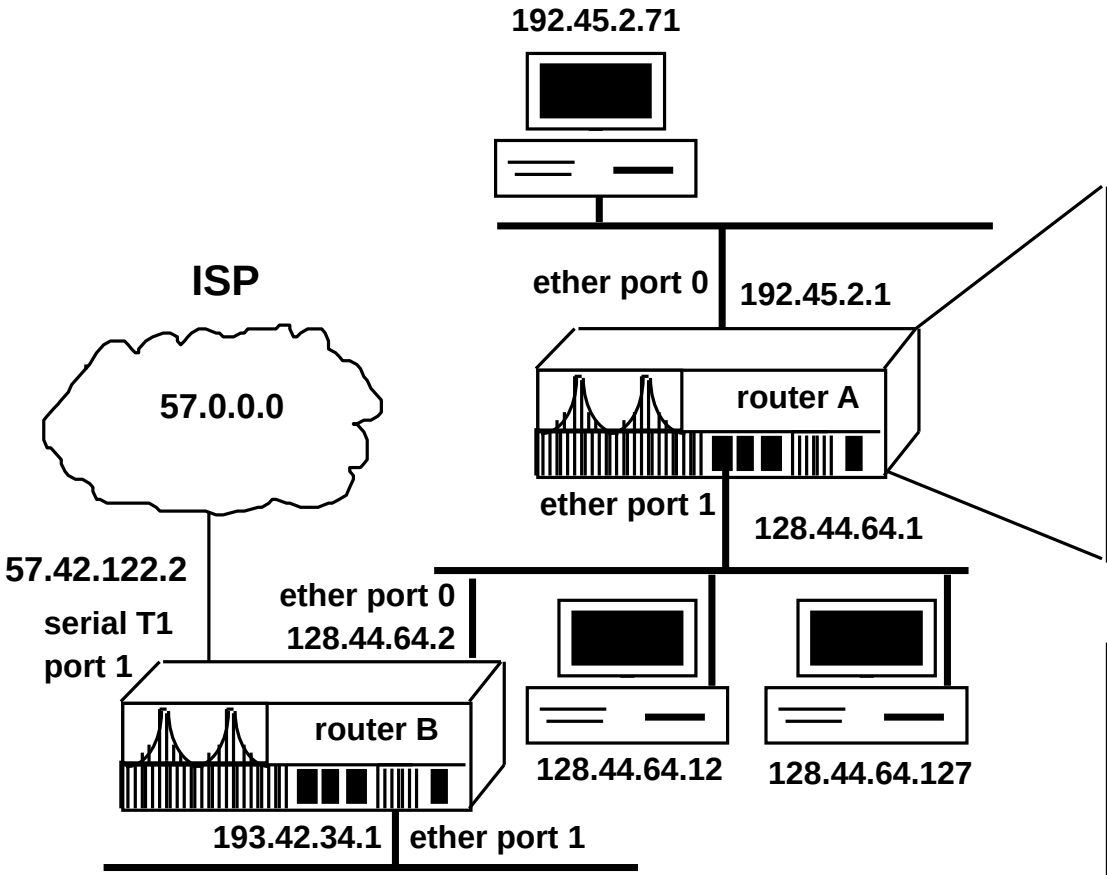
Neighboring routers and routing protocols exchange frames containing either:

- **Hello packets**
- **Routing update packets**

Routing tables contain routes learned from neighboring routers

Routers forward traffic to the destination network by passing packets to the next-hop logical device (router) in the delivery path

LAN Interconnection – Routing

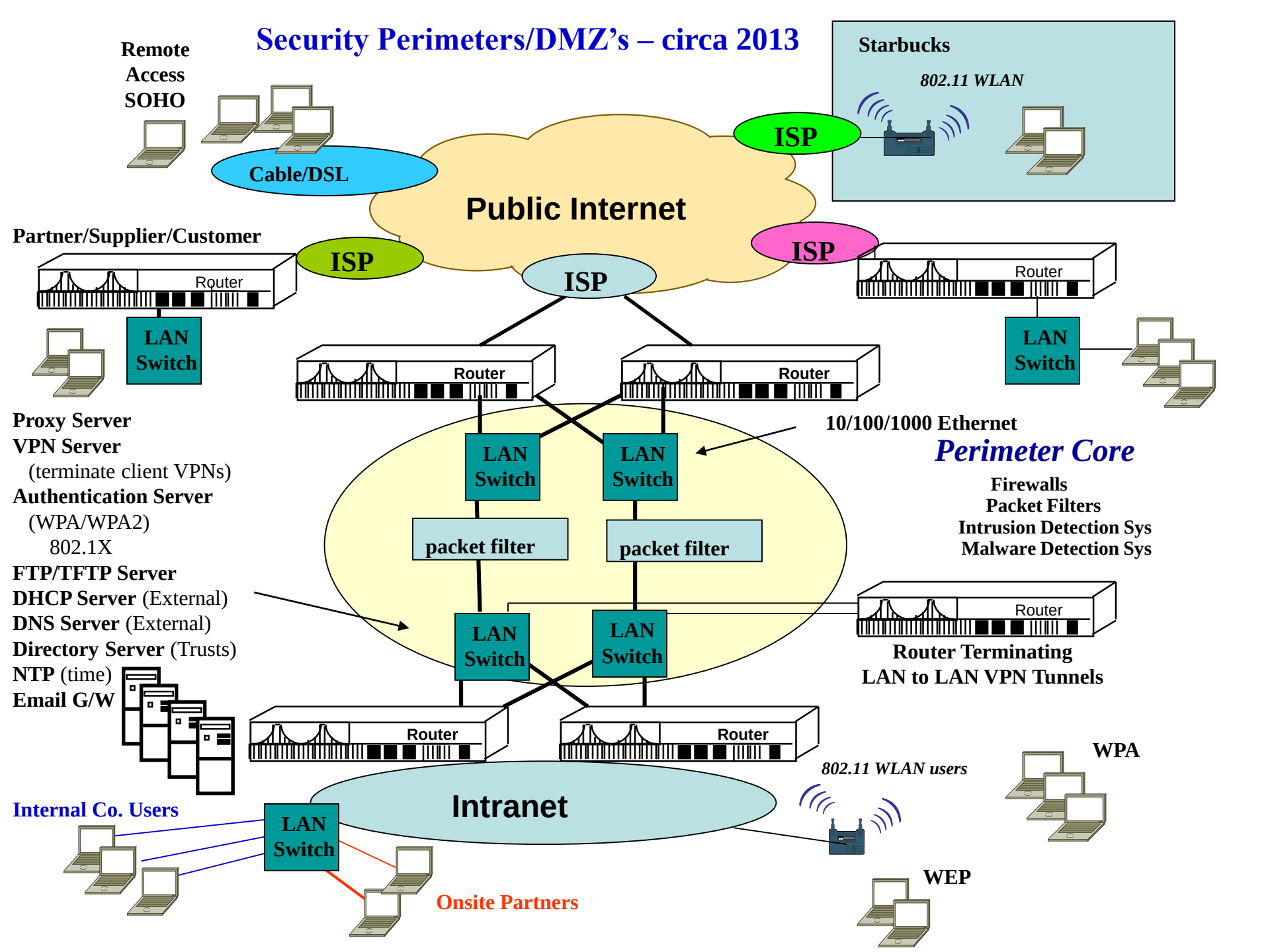


Route Table (Router A)

network add	router port
192.45.2.0	ether port 0
128.144.0.0	ether port 1
57.0.0.0	ether port 1
193.42.34.0	ether port 1

ARP Table Router A

IP Address	MAC Address
192.45.2.1	000c42310bb1
192.45.2.71	00c3445602da
128.44.64.1	000c75240ca1
128.44.64.2	00ca545402ca
128.44.64.12	aa0c23546767
128.44.64.127	00c405061abb2

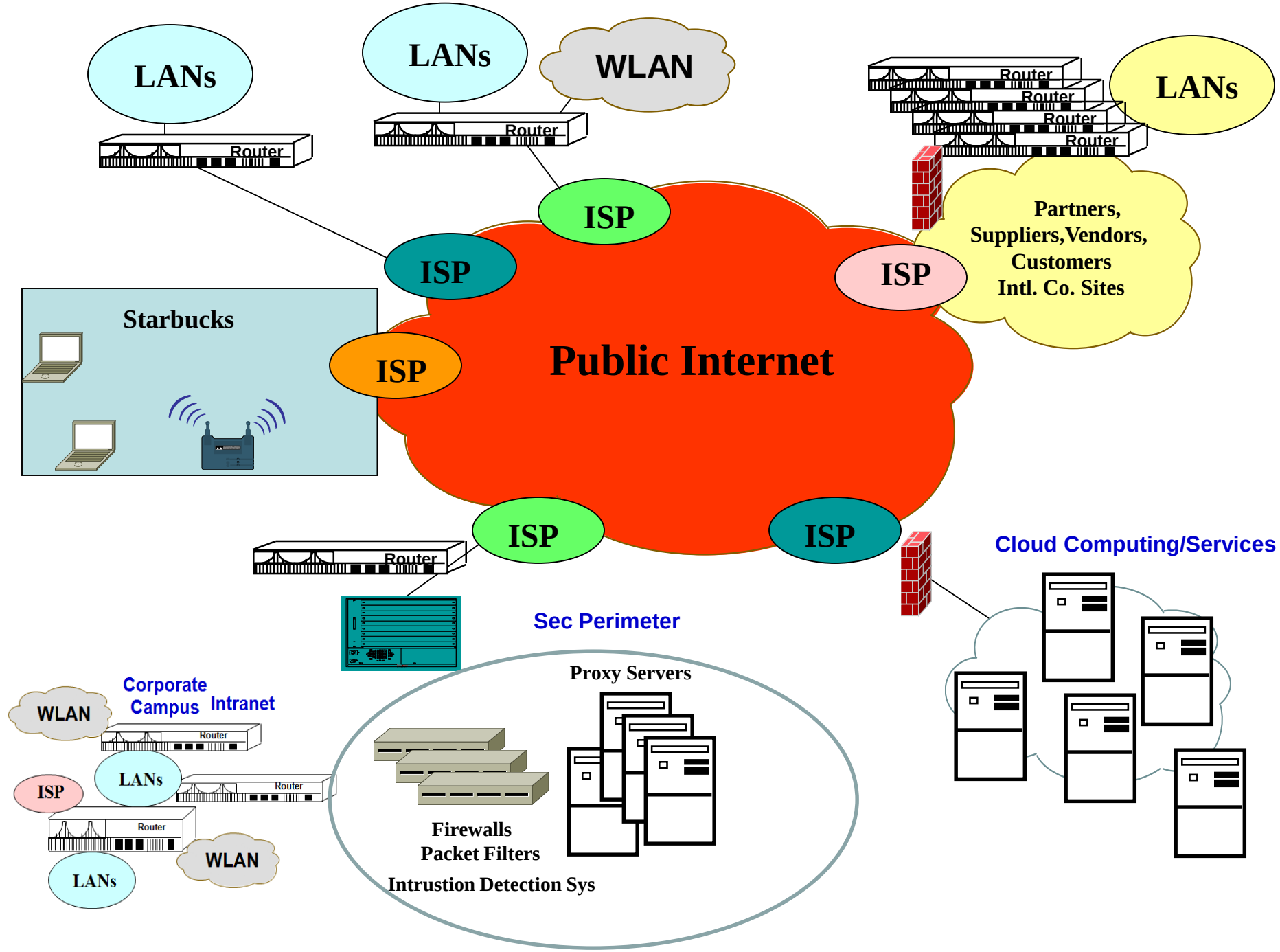

Security Perimeters/DMZ's – circa 2013
Remote Access SOHO
Cable/DSL
Starbucks
802.11 WLAN
ISP
Public Internet
ISP
ISP
ISP
Partner/Supplier/Customer
Router
LAN Switch
Router
Router
Router
LAN Switch
Proxy Server
VPN Server
(terminate client VPNs)
Authentication Server
(WPA/WPA2)
802.1X
FTP/TFTP Server
DHCP Server (External)
DNS Server (External)
Directory Server (Trusts)
NTP (time)
Email G/W
10/100/1000 Ethernet
Perimeter Core
Firewalls
Packet Filters
Intrusion Detection Sys
Malware Detection Sys
LAN Switch
LAN Switch
packet filter
packet filter
LAN Switch
LAN Switch
Router
Router Terminating
LAN to LAN VPN Tunnels
Router
Router
802.11 WLAN users
WPA
Intranet
Internal Co. Users
LAN Switch
Onsite Partners
WEP

Key Takeaway

The primary components and strategies of cyber security/IA are network centric based.

They attempt to inspect, monitor, filter/block traffic on network based mechanisms;

- **internet protocol (IP) address**
- **IP TCP/UDP port**
- **network access control lists (ACLs)**


LANs
Router
LANs
WLAN
Router
Router
Router
Router
Router
LANs
ISP
ISP
ISP
ISP
ISP
ISP
Partners,
Suppliers,Vendors,
Customers
Intl. Co. Sites
Starbucks
Public Internet
Router
Cloud Computing/Services
Sec Perimeter
Proxy Servers
Corporate
Campus Intranet
WLAN
Router
LANs
Router
ISP
Router
WLAN
LANs
Firewalls
Packet Filters
Intrustion Detection Sys