ThaiAdmin

Basic Knowledge for Advance Network Troubleshooting #1

By Warin Loasakul (Fordot)

ThaiAdmin

Agenda

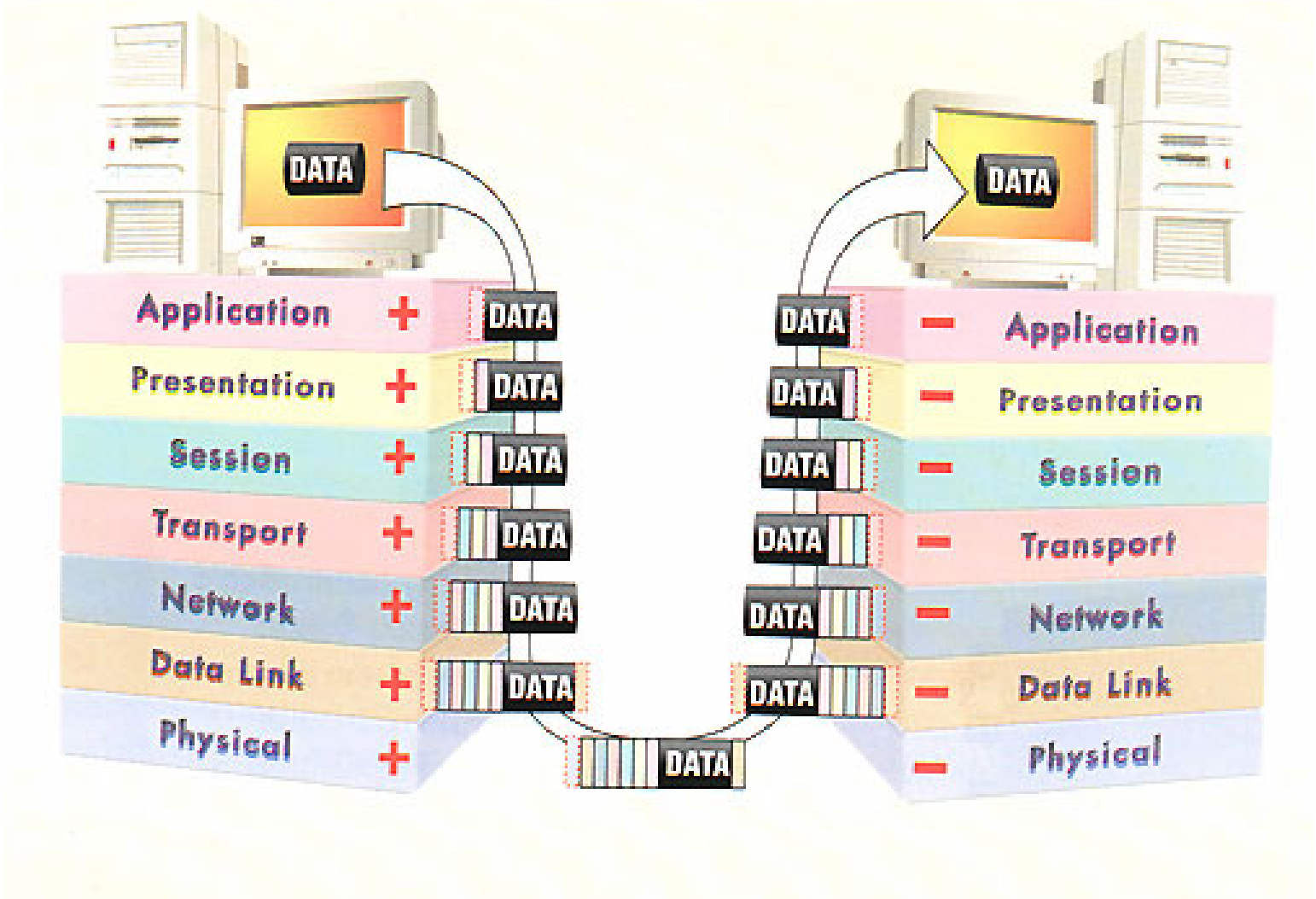
1. OSI 7 Layer & Beyond the 7th layer
2. Ethereal: Basic usage introduction
3. Protocol Detail

ThaiAdmin

OSI 7 Layer

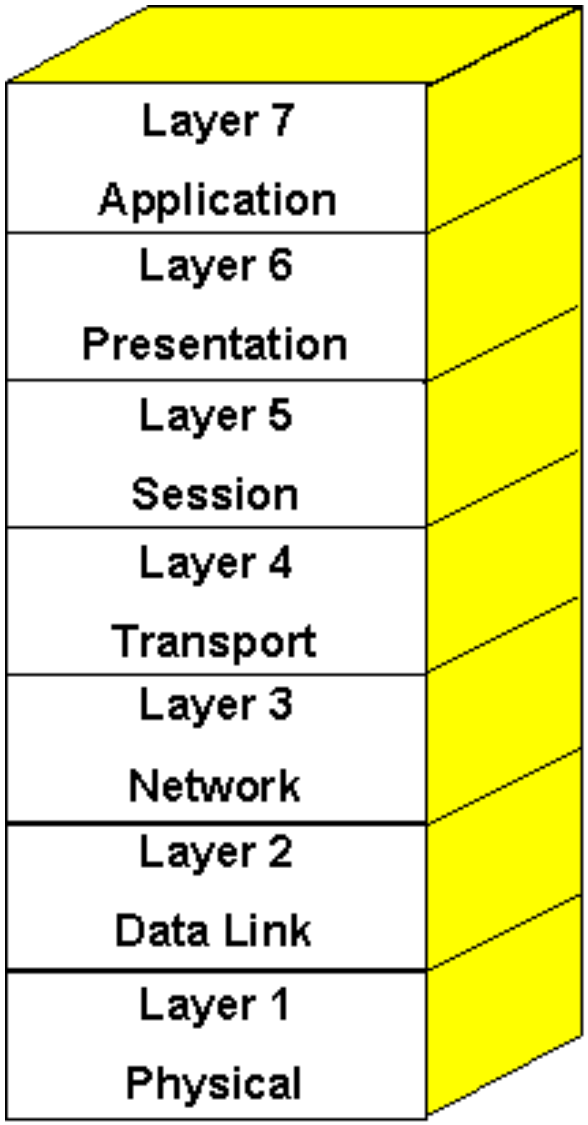
ThaiAdmin

Data Flow and Header



ThaiAdmin

Meaning



Applications and application interfaces for OSI networks. Provides access to lower layer functions and services.

Negotiates syntactic representations and performs data transformations, e.g. compression and code conversion.

Coordinates connection and interaction between applications, establishes dialogue, manages and synchronizes direction of data flow.

Ensures end-to-end data transfer and integrity across the network. Assembles packets for routing by Layer 3.

Routes and relays data units across a network of nodes. Manages flow control and call establishment procedures.

Transfers data units from one network node to another over transmission circuit. Ensures data integrity between nodes.

Delimits and encodes the bits onto the physical medium. Defines electrical, mechanical and procedural formats.

ThaiAdmin

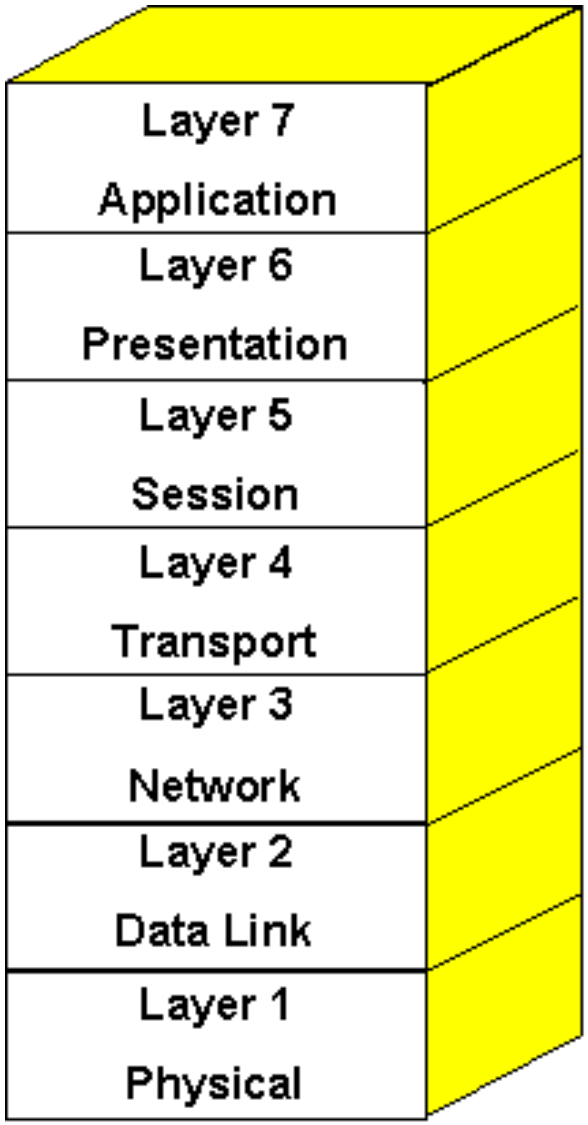
Layering
(Beyond the 7th layer)

DoD Stack (1970)

Process Layer	Telnet, FTP, e-mail, etc
Host to Host Layer	TCP, UDP
Internet Layer	IP, ICMP, IGMP
Network Access Layer	Device driver and interface card

ThaiAdmin

OSI Model (1978)



Applications and application interfaces for OSI networks. Provides access to lower layer functions and services.

Negotiates syntactic representations and performs data transformations, e.g. compression and code conversion.

Coordinates connection and interaction between applications, establishes dialogue, manages and synchronizes direction of data flow.

Ensures end-to-end data transfer and integrity across the network. Assembles packets for routing by Layer 3.

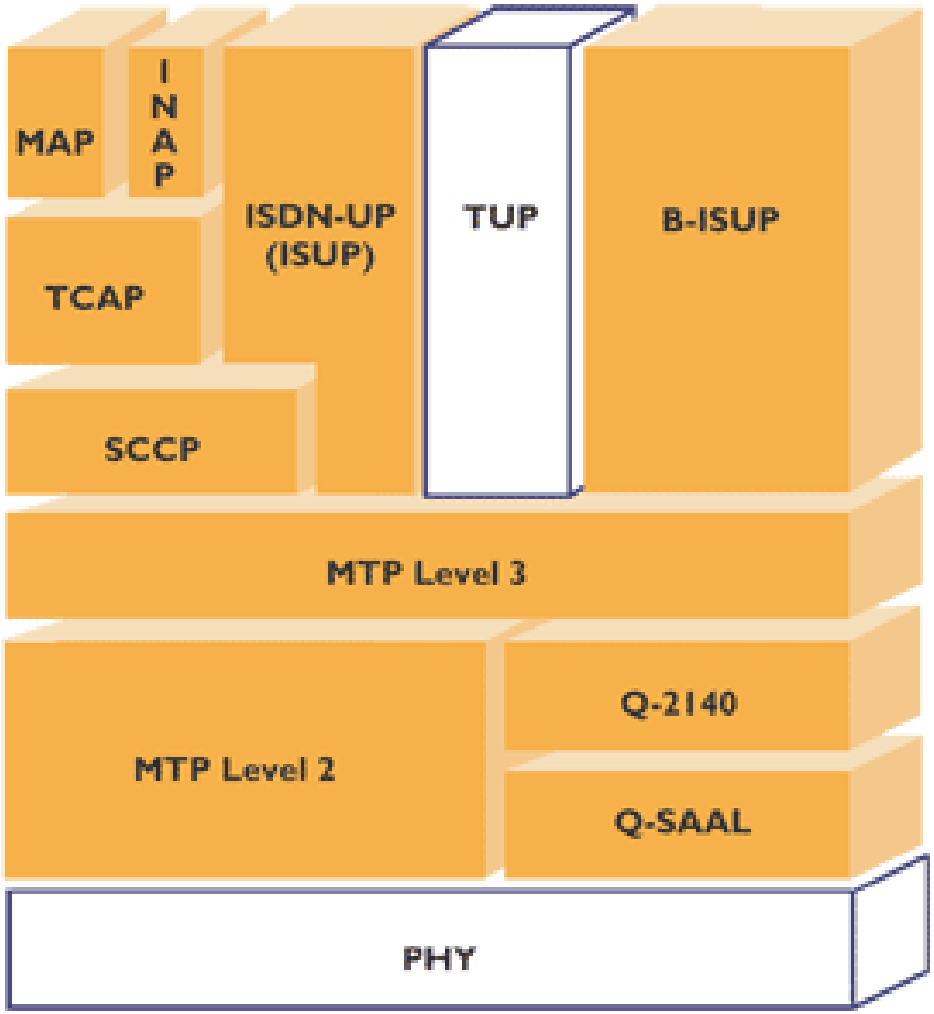
Routes and relays data units across a network of nodes. Manages flow control and call establishment procedures.

Transfers data units from one network node to another over transmission circuit. Ensures data integrity between nodes.

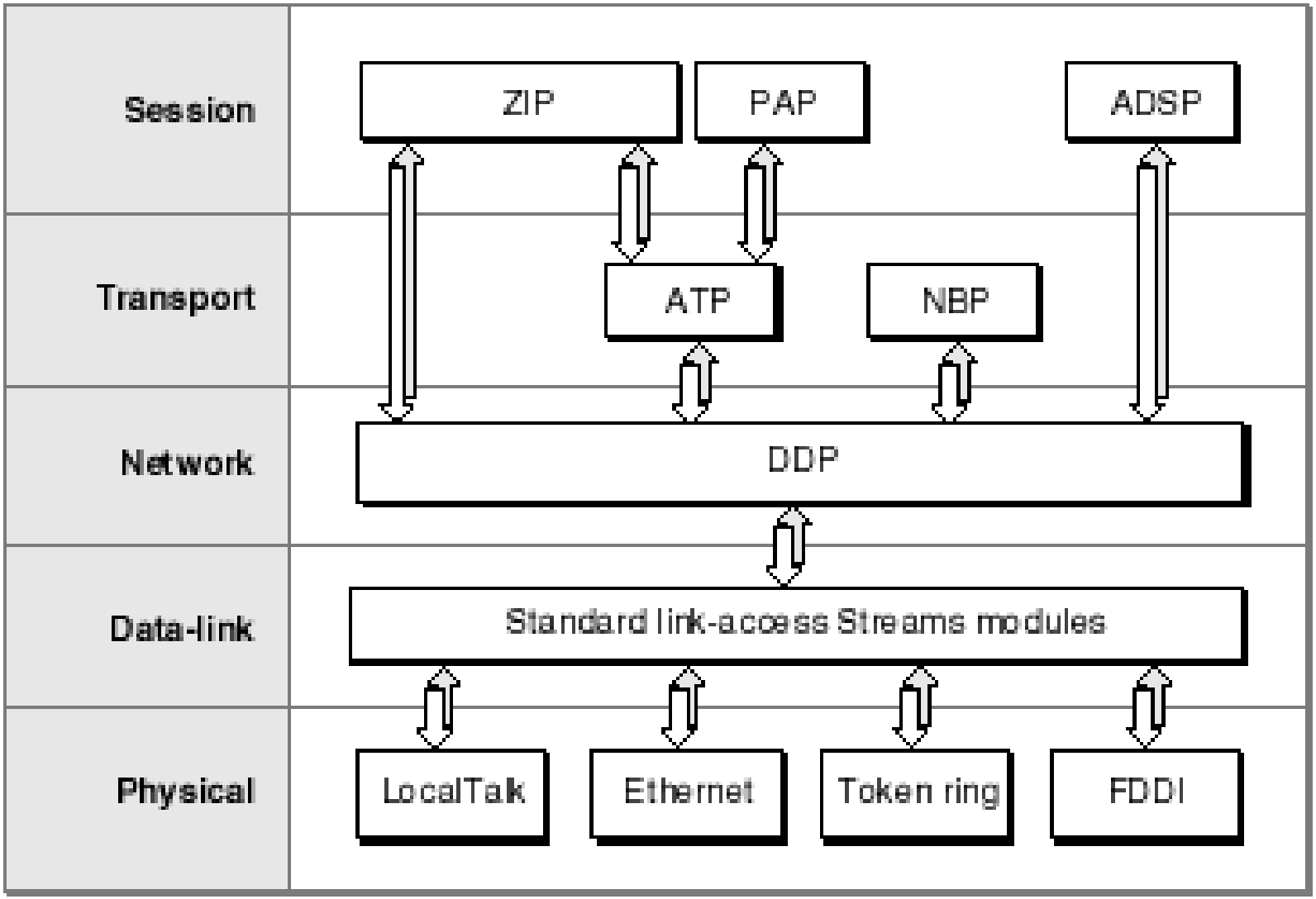
Delimits and encodes the bits onto the physical medium. Defines electrical, mechanical and procedural formats.

ThaiAdmin

SS7 Stack (1981)

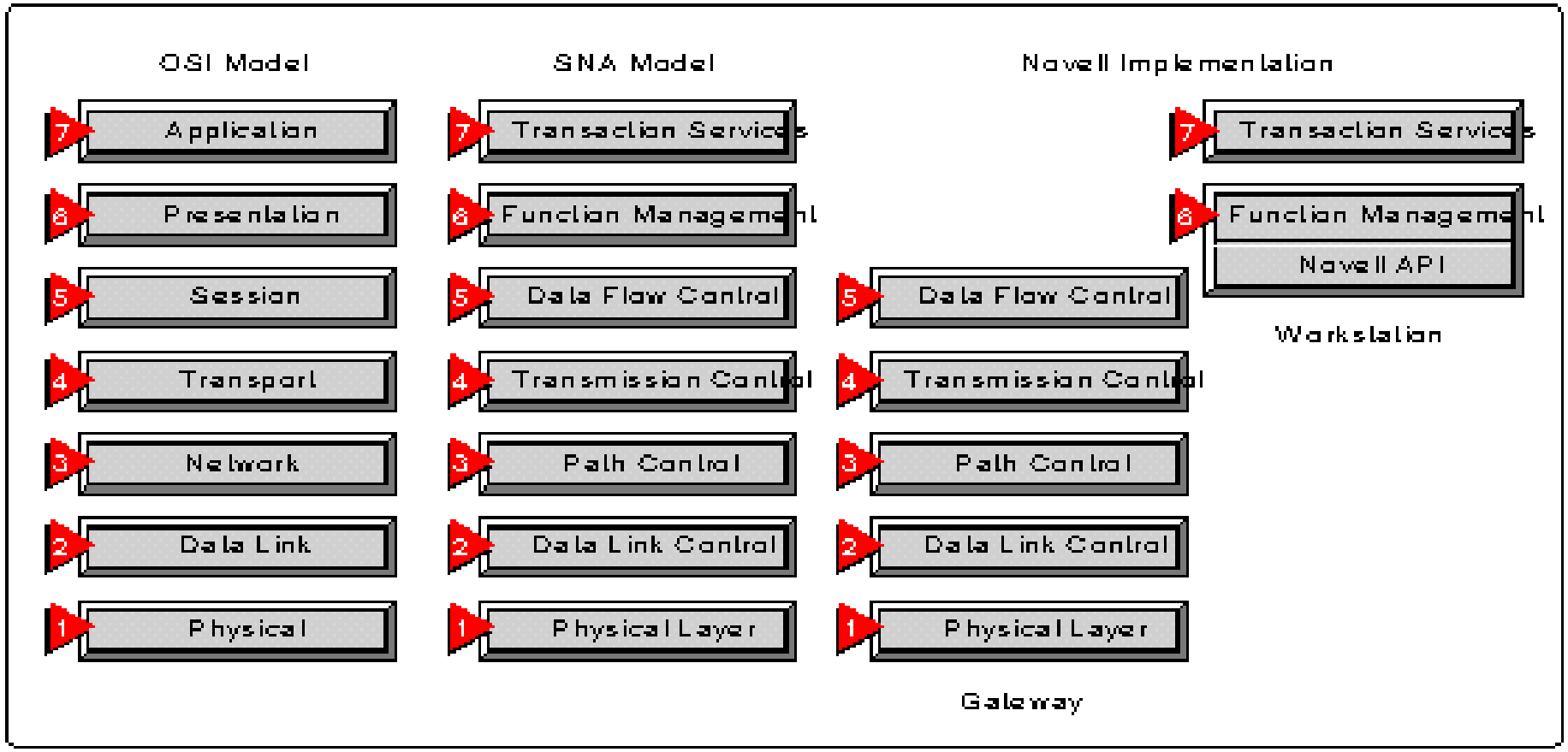


Apple Talk Stack (1984)



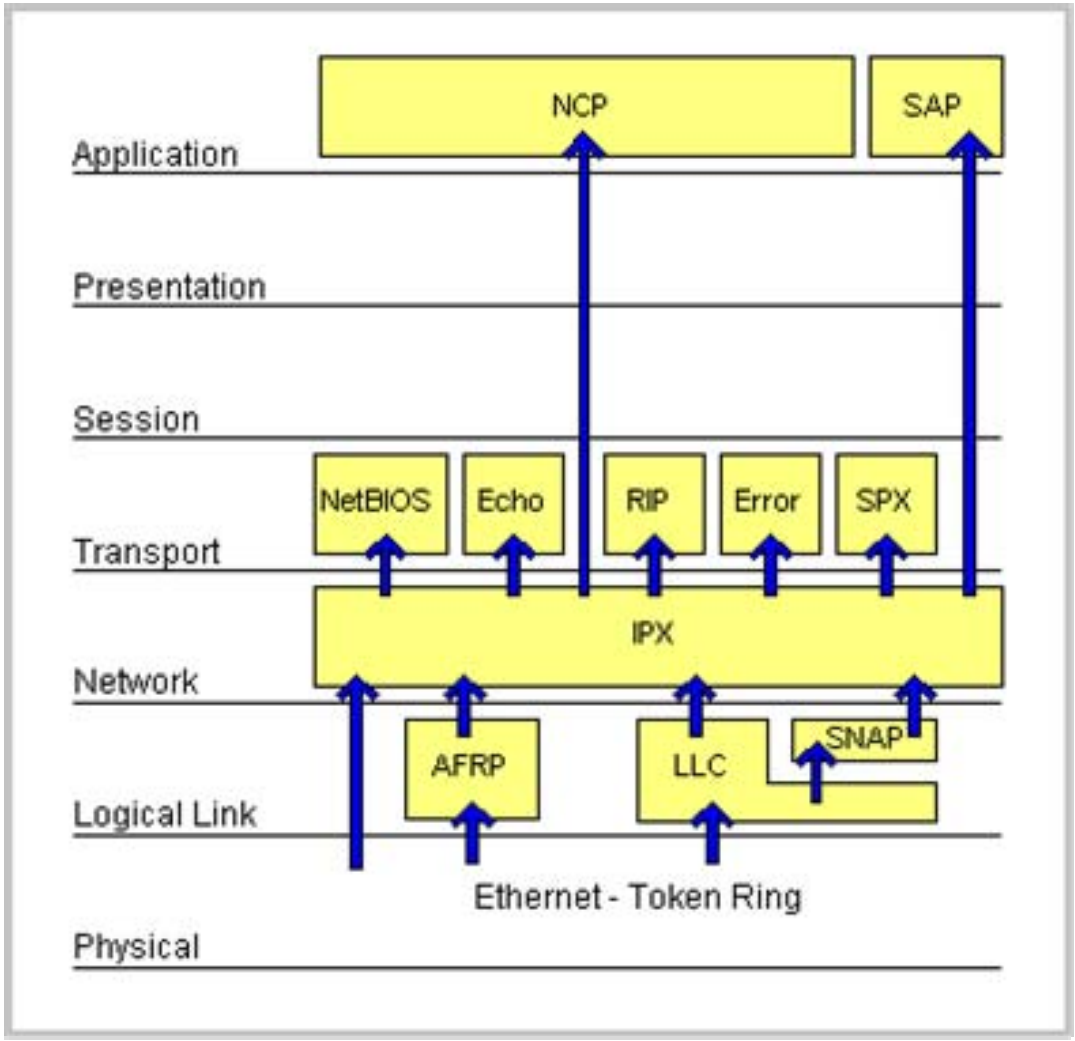
ThaiAdmin

SNA Stack (1974)



Novel Protocol Suite

Novell Protocol Suite



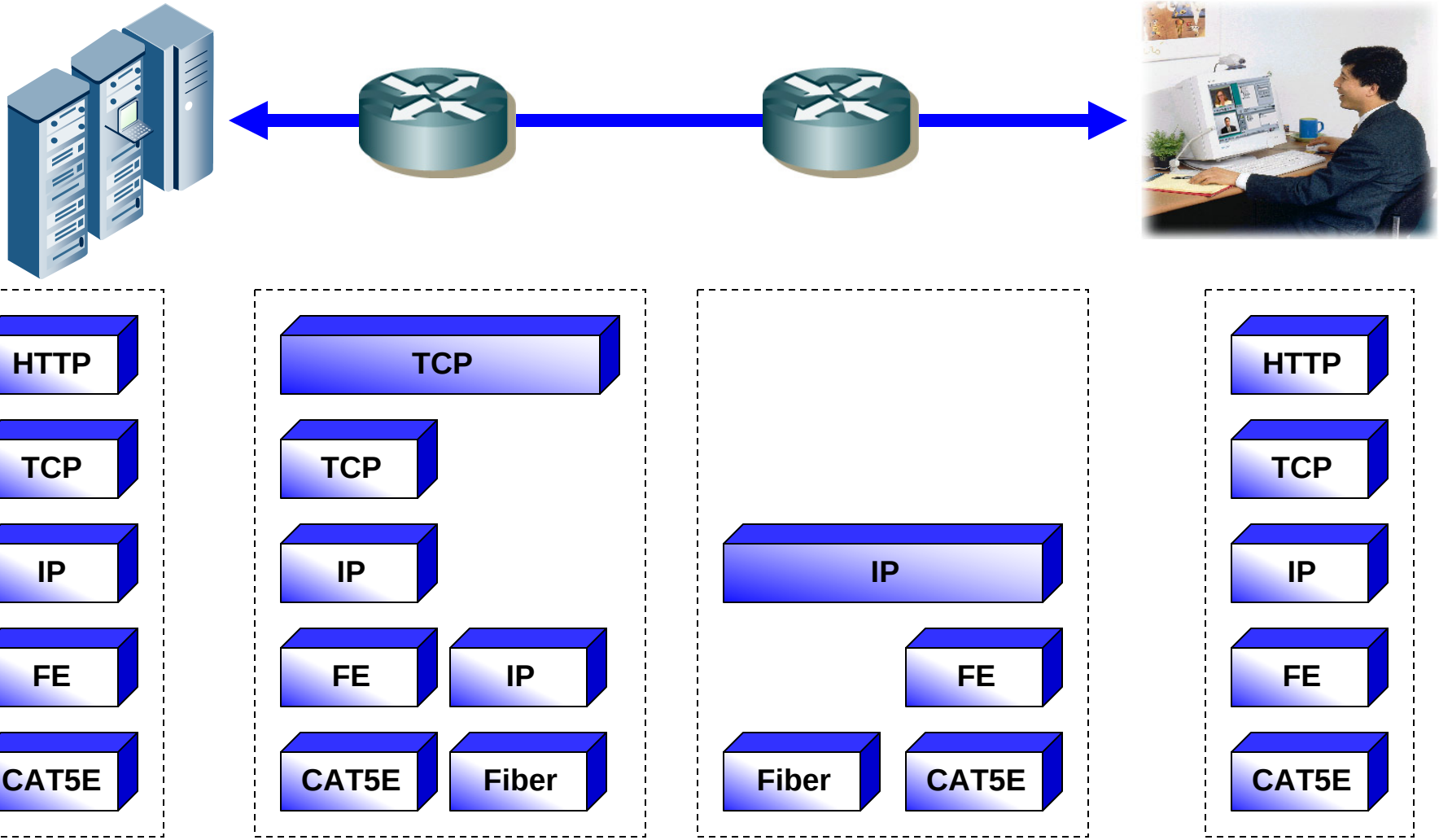
ThaiAdmin

Layer	Misc. Examples	TCP/IP (DoD) (1970)	SS7 (1981)	AppleTalk (1984)	OSI suite (1978)	IPX suite (1987)	SNA (1974)	UMTS (1998)
7 - Application	HL7, Modbus	HTTP, SMTP, SNMP, FTP, Telnet, NFS, NTP	ISUP, INAP, MAP, TUP, TCAP	AFP, PAP	FTAM, X.400, X.500, DAP		APPC	
6 - Presentation	TDI, ASCII, EBCDIC, MIDI, MPEG	XDR, SSL, TLS		AFP, PAP				
5 - Session	Named Pipes, NetBIOS, SIP, SAP, SDP	Session establishment for TCP		ASP, ADSP, ZIP		NWLink	DLC?	
4 - Transport	NetBEUI	TCP, UDP, RTP, SCTP		ATP, NBP, AEP, RTMP	TP0, TP1, TP2, TP3, TP4	SPX, RIP		
3 - Network	NetBEUI, Q.931	IP, ICMP, IPsec, ARP, RIP, OSPF, BGP	MTP-3, SCCP	DDP	X.25 (PLP), CLNP	IPX		RRC (Radio Resource Control)
2 - Data Link	Ethernet, Token Ring, FDDI, PPP, HDLC, Q.921, Frame Relay, ATM, Fibre Channel		MTP-2	LocalTalk, TokenTalk, EtherTalk, Apple Remote Access, PPP	X.25 (LAPB), Token Bus	802.3 framing, Ethernet II framing	SDLC	MAC (Media Access Control)
1 - Physical	RS-232, V.35, V.34, Q.911, T1, E1, 10BASE-T, 100BASE-TX, ISDN, SONET, DSL		MTP-1	Localtalk on shielded, Localtalk on unshielded (PhoneNet)	X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703)		Twinax	PHY (Physical Layer)

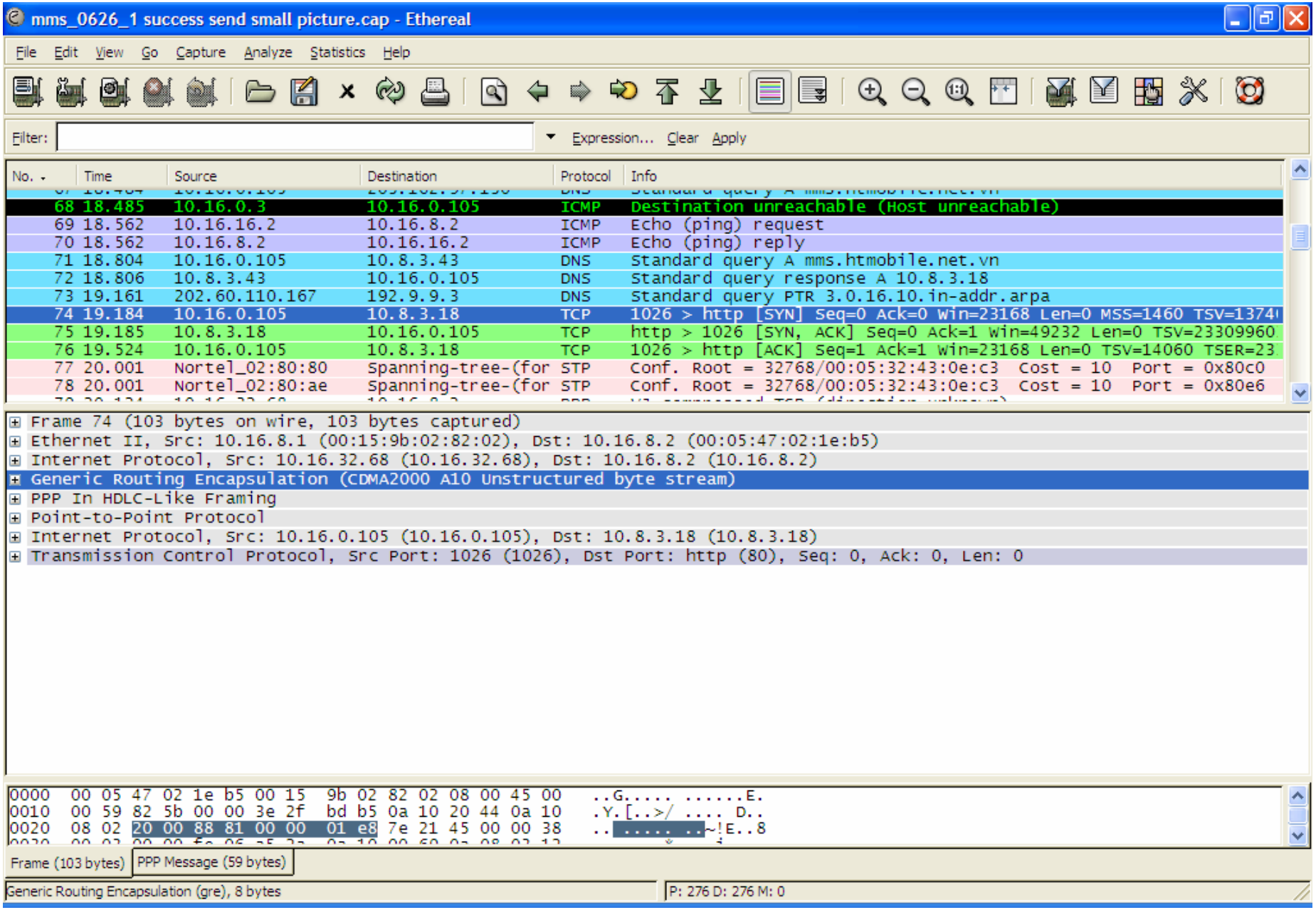
Group Discussion

ThaiAdmin

Discussion 1: Something wrong? Or not?

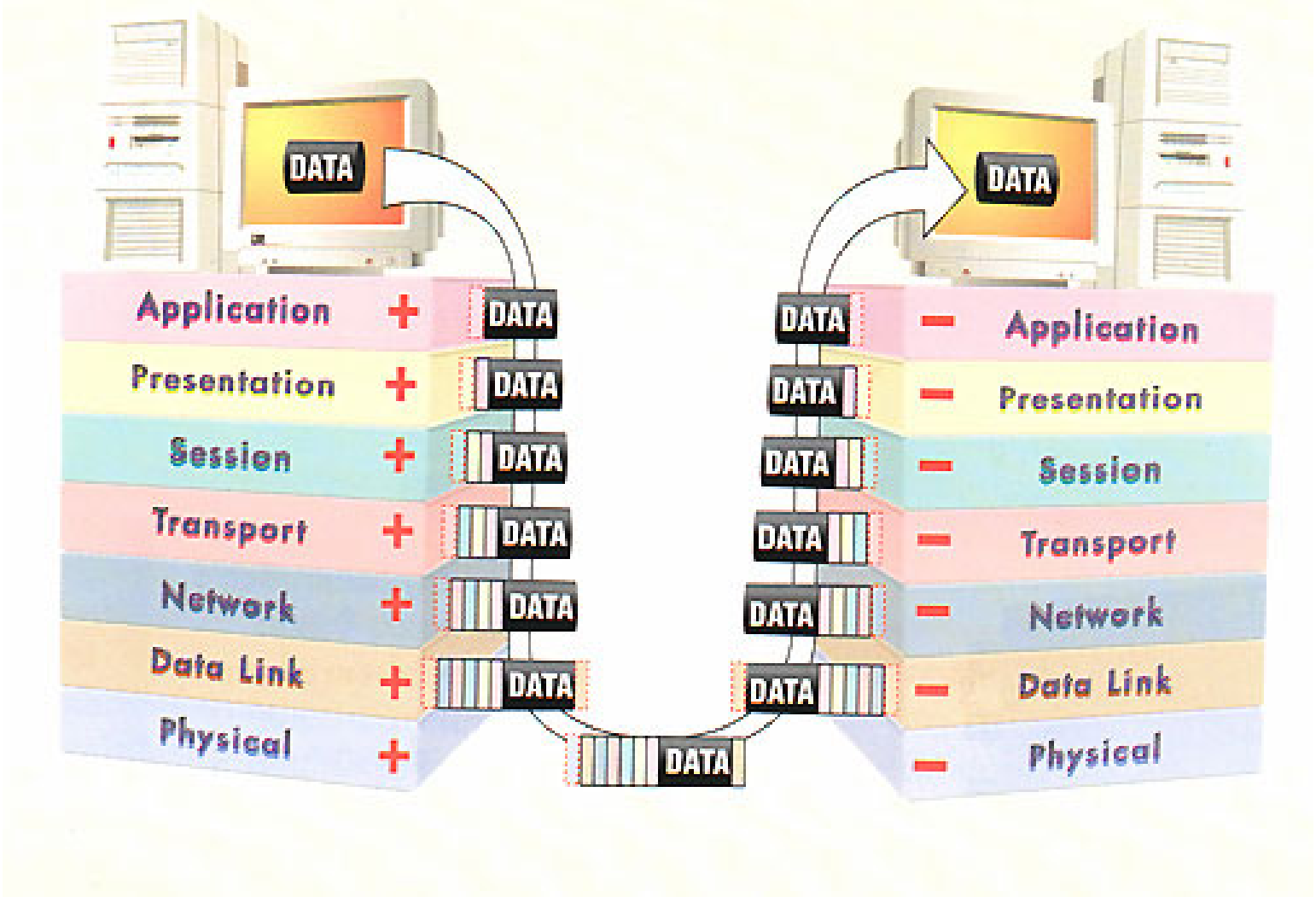


ThaiAdmin


mms_0626_1 success send small picture.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
68 18.485 10.16.0.3 10.16.0.105 ICMP Destination unreachable (Host unreachable)
69 18.562 10.16.16.2 10.16.8.2 ICMP Echo (ping) request
70 18.562 10.16.8.2 10.16.16.2 ICMP Echo (ping) reply
71 18.804 10.16.0.105 10.8.3.43 DNS Standard query A mms.htmobile.net.vn
72 18.806 10.8.3.43 10.16.0.105 DNS Standard query response A 10.8.3.18
73 19.161 202.60.110.167 192.9.9.3 DNS Standard query PTR 3.0.16.10.in-addr.arpa
74 19.184 10.16.0.105 10.8.3.18 TCP 1026 > http [SYN] Seq=0 Ack=0 Win=23168 Len=0 MSS=1460 TSV=1374
75 19.185 10.8.3.18 10.16.0.105 TCP http > 1026 [SYN, ACK] Seq=0 Ack=1 Win=49232 Len=0 TSV=23309960
76 19.524 10.16.0.105 10.8.3.18 TCP 1026 > http [ACK] Seq=1 Ack=1 Win=23168 Len=0 TSV=14060 TSER=23
77 20.001 Nortel_02:80:80 Spanning-tree-(for STP Conf. Root = 32768/00:05:32:43:0e:c3 Cost = 10 Port = 0x80c0
78 20.001 Nortel_02:80:ae Spanning-tree-(for STP Conf. Root = 32768/00:05:32:43:0e:c3 Cost = 10 Port = 0x80e6
Frame 74 (103 bytes on wire, 103 bytes captured)
Ethernet II, Src: 10.16.8.1 (00:15:9b:02:82:02), Dst: 10.16.8.2 (00:05:47:02:1e:b5)
Internet Protocol, Src: 10.16.32.68 (10.16.32.68), Dst: 10.16.8.2 (10.16.8.2)
Generic Routing Encapsulation (CDMA2000 A10 Unstructured byte stream)
PPP In HDLC-Like Framing
Point-to-Point Protocol
Internet Protocol, Src: 10.16.0.105 (10.16.0.105), Dst: 10.8.3.18 (10.8.3.18)
Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: http (80), Seq: 0, Ack: 0, Len: 0
0000 00 05 47 02 1e b5 00 15 9b 02 82 02 08 00 45 00
0010 00 59 82 5b 00 00 3e 2f bd b5 0a 10 20 44 0a 10
0020 08 02 20 00 88 81 00 00 01 e8 7e 21 45 00 00 38
Frame (103 bytes) PPP Message (59 bytes)
Generic Routing Encapsulation (gre), 8 bytes
P: 276 D: 276 M: 0

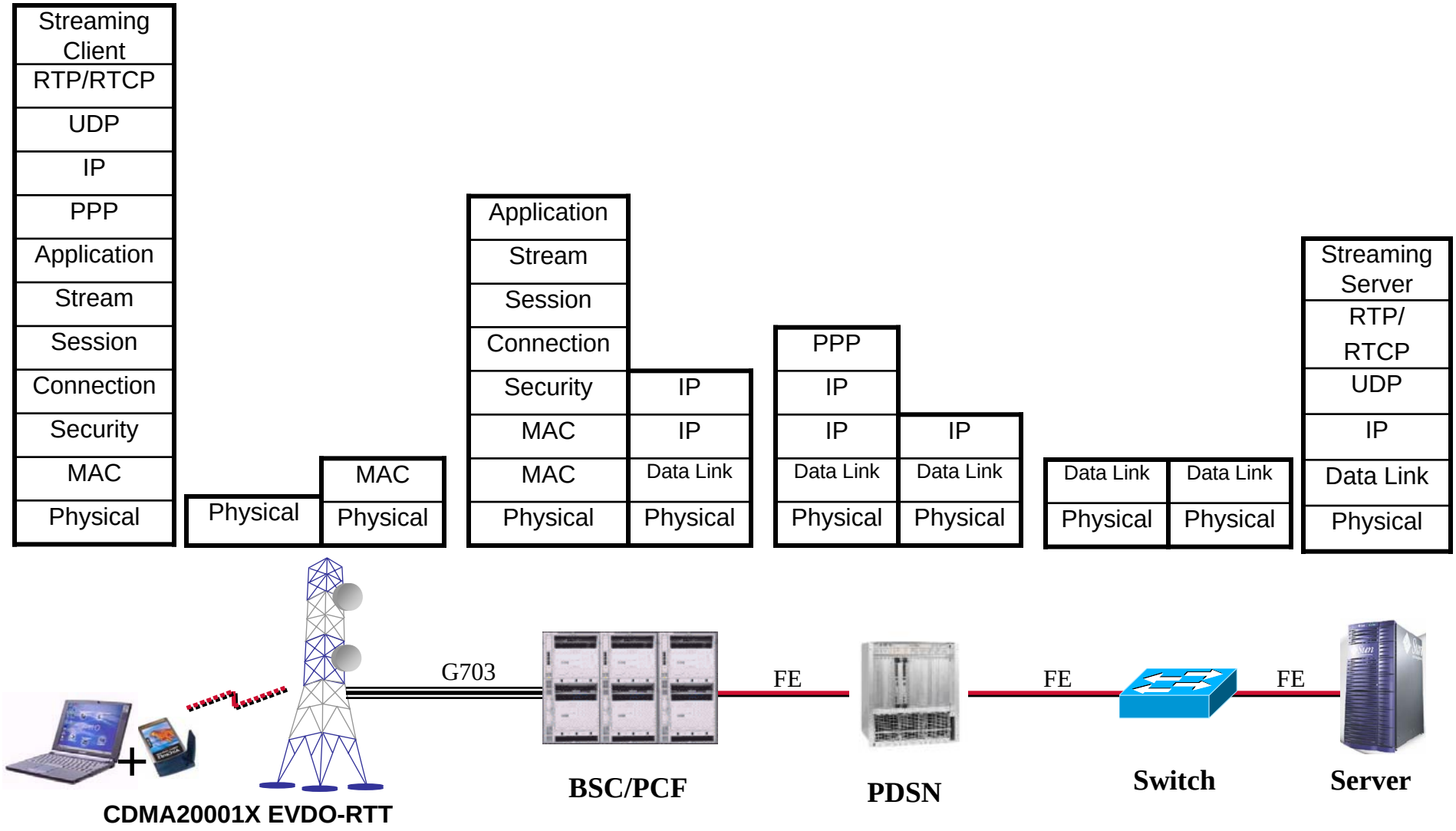
ThaiAdmin

Is this picture still can be trust?
What you learn from University is Correct?



ThaiAdmin

Discussion 2:
Something wrong? Or not?

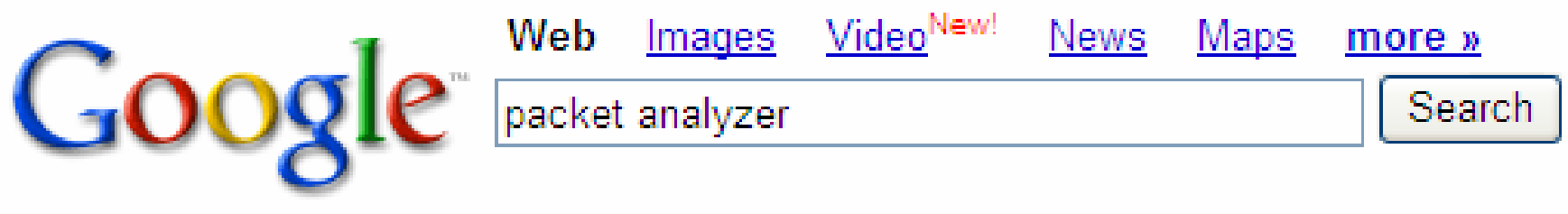


ThaiAdmin

Network Analyzer Tools

Most Popular

- Ethereal Network Analyzer
- Sniffer Pro
- Snoop Analyzer Standard
- Network Stumbler Wireless Packet Sniffer
- IP Sniffer
- etc



What is Ethereal

- Ethereal is a network packet analyzer
- A network packet analyzer will try to capture network packet
- And display captured data
- Ethereal is Open Source
- Available for UNIX and Windows.
- http://www.ethereal.com/ 

ThaiAdmin

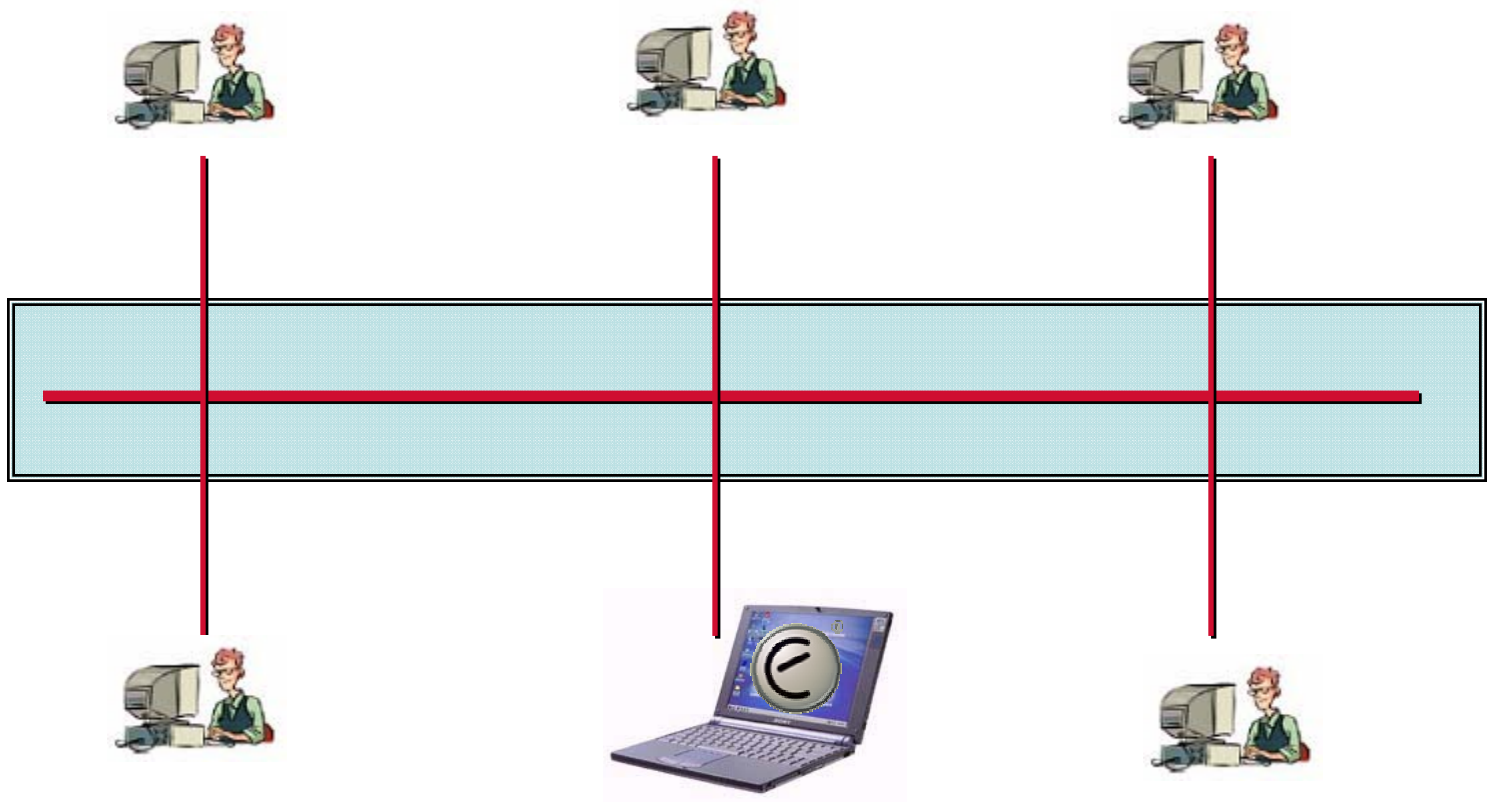
Introduction to Ethereal

- How to setup network for packet capturing
- How to capture message
- How to capture with filtering
- How to display message
- How to display with filtering

ThaiAdmin

How to setup network for packet capturing

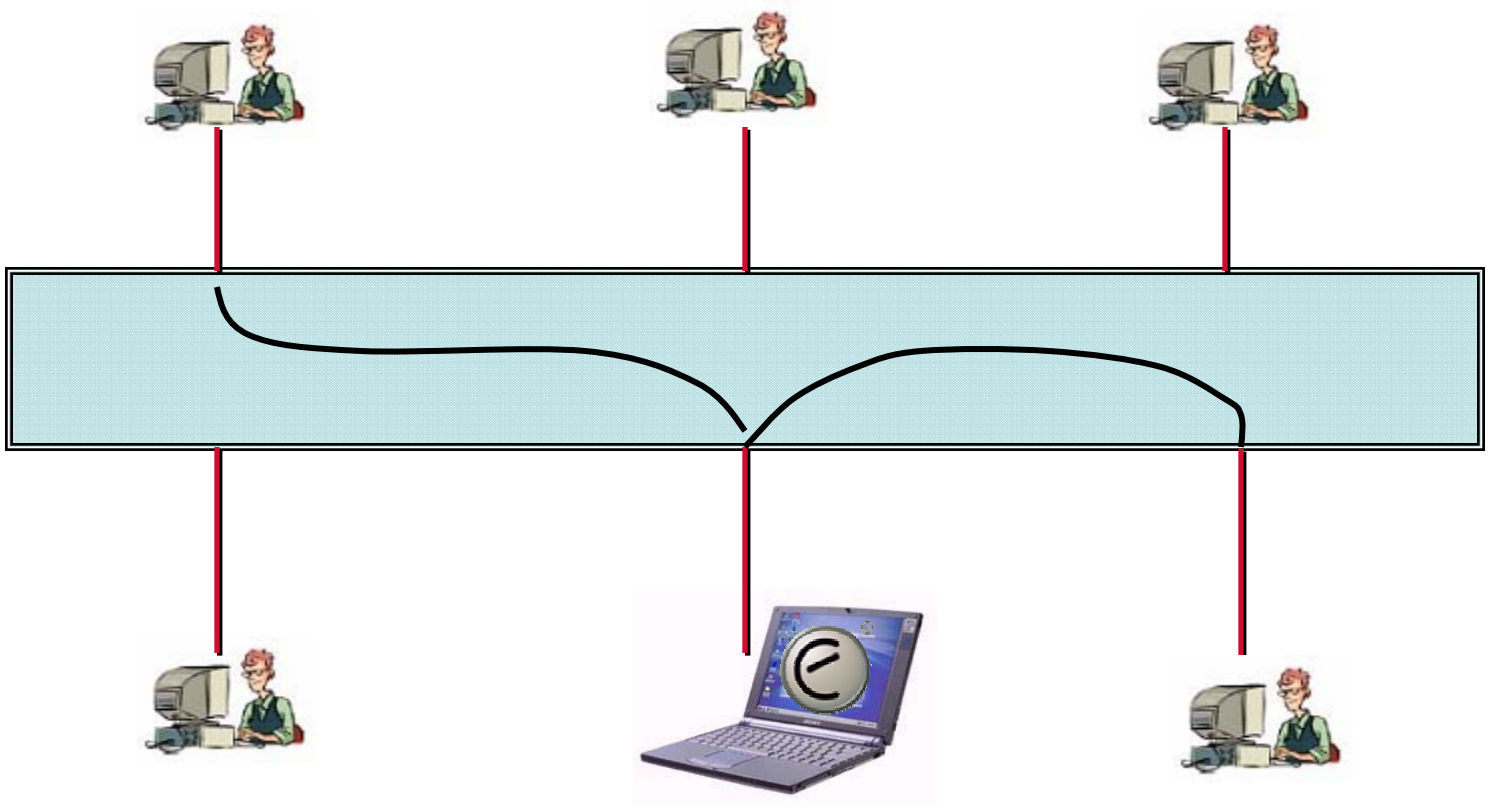
- Share Media Hub



ThaiAdmin

How to setup network for packet capturing

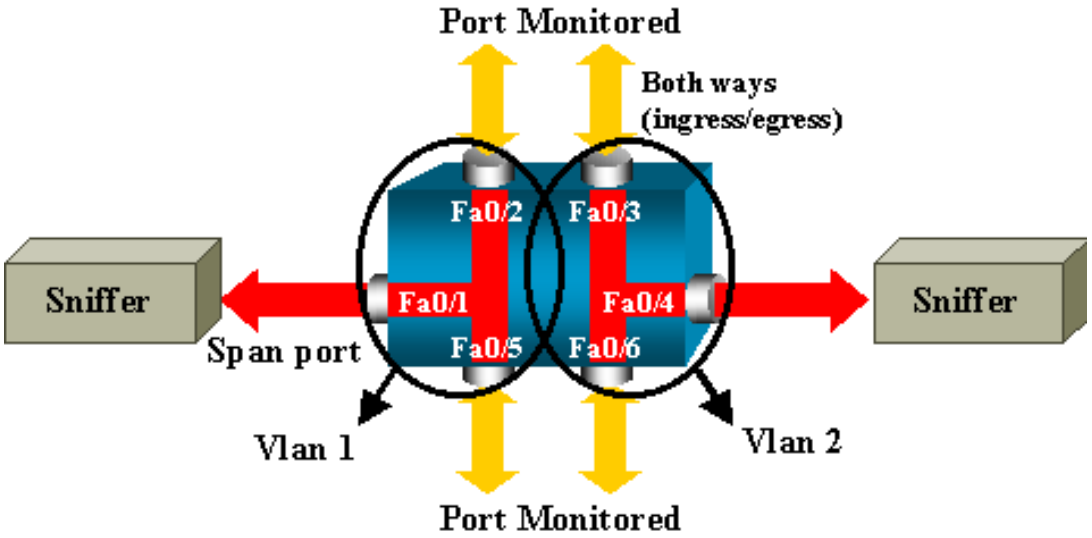
- LAN Switching



Have to configure Mirror port in LAN Switch before capture packet

ThaiAdmin

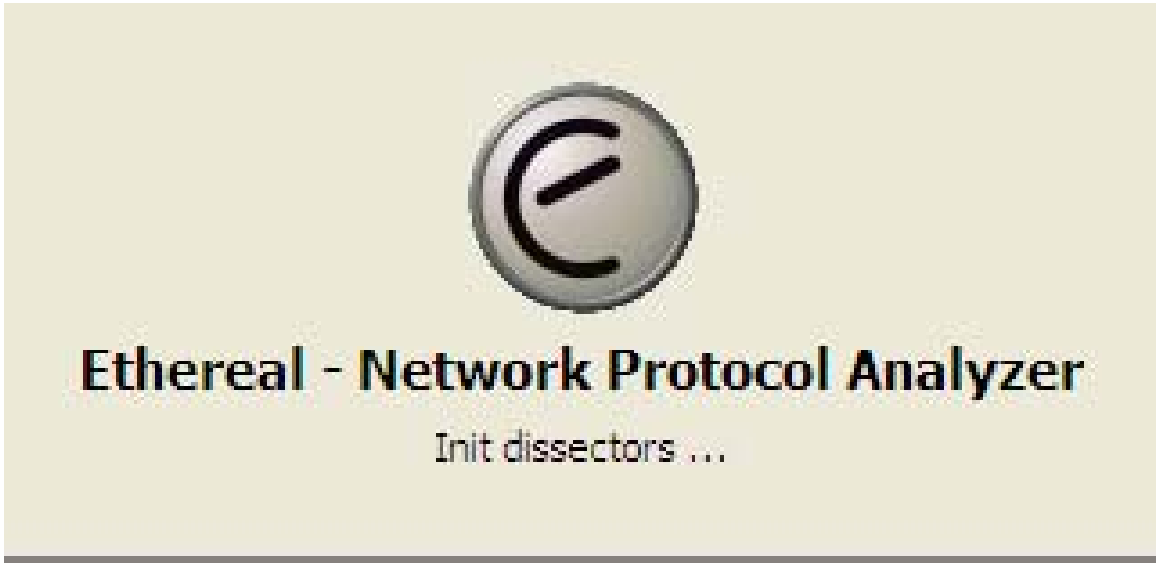
Cisco span port command




```
!
 interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/5
port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
port monitor FastEthernet0/3
port monitor FastEthernet0/6
switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 2
!
interface VLAN1
ip address 10.200.8.136 255.255.252.0
no ip directed-broadcast
no ip route-cache
```

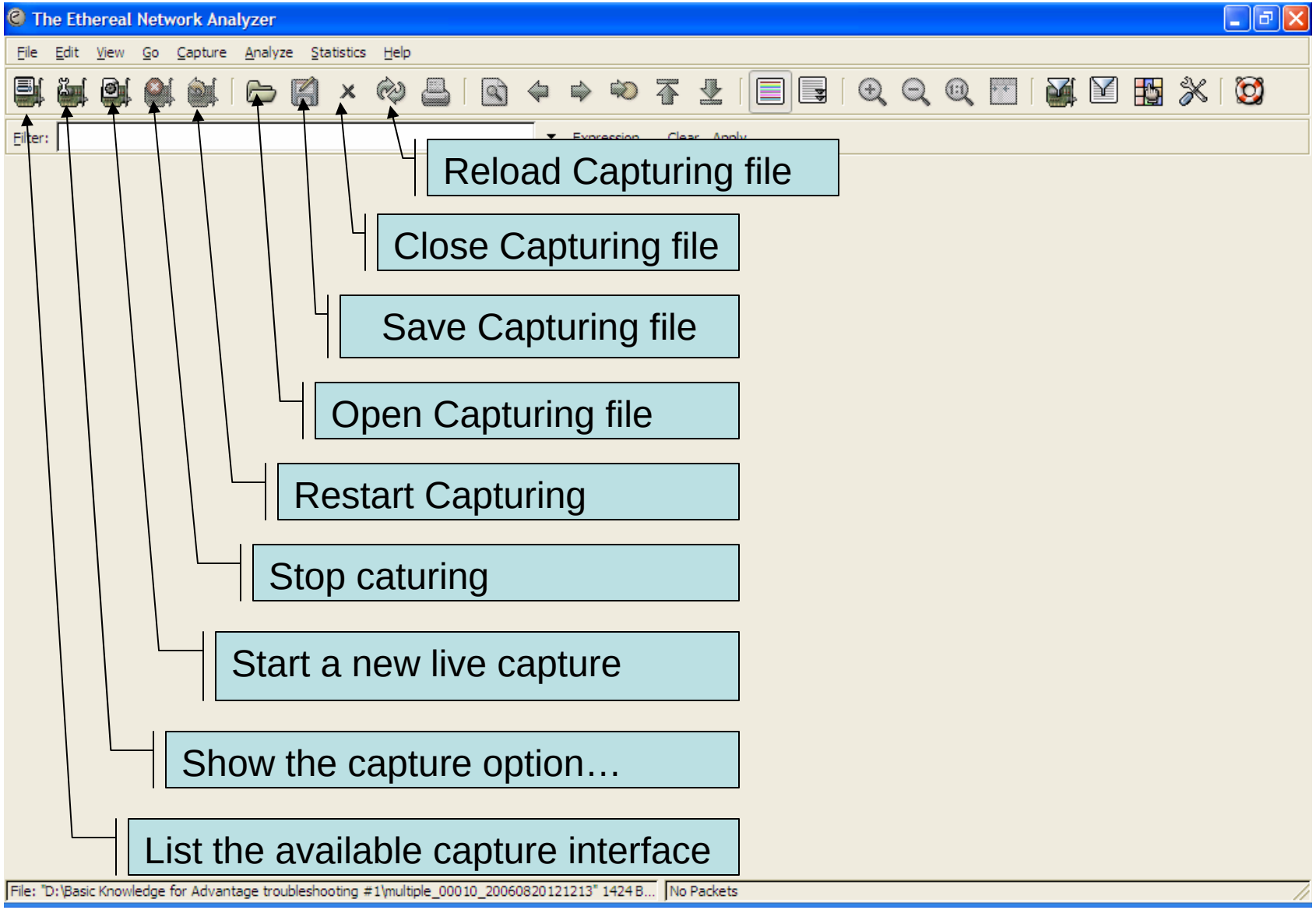
ThaiAdmin

Start Ethereal



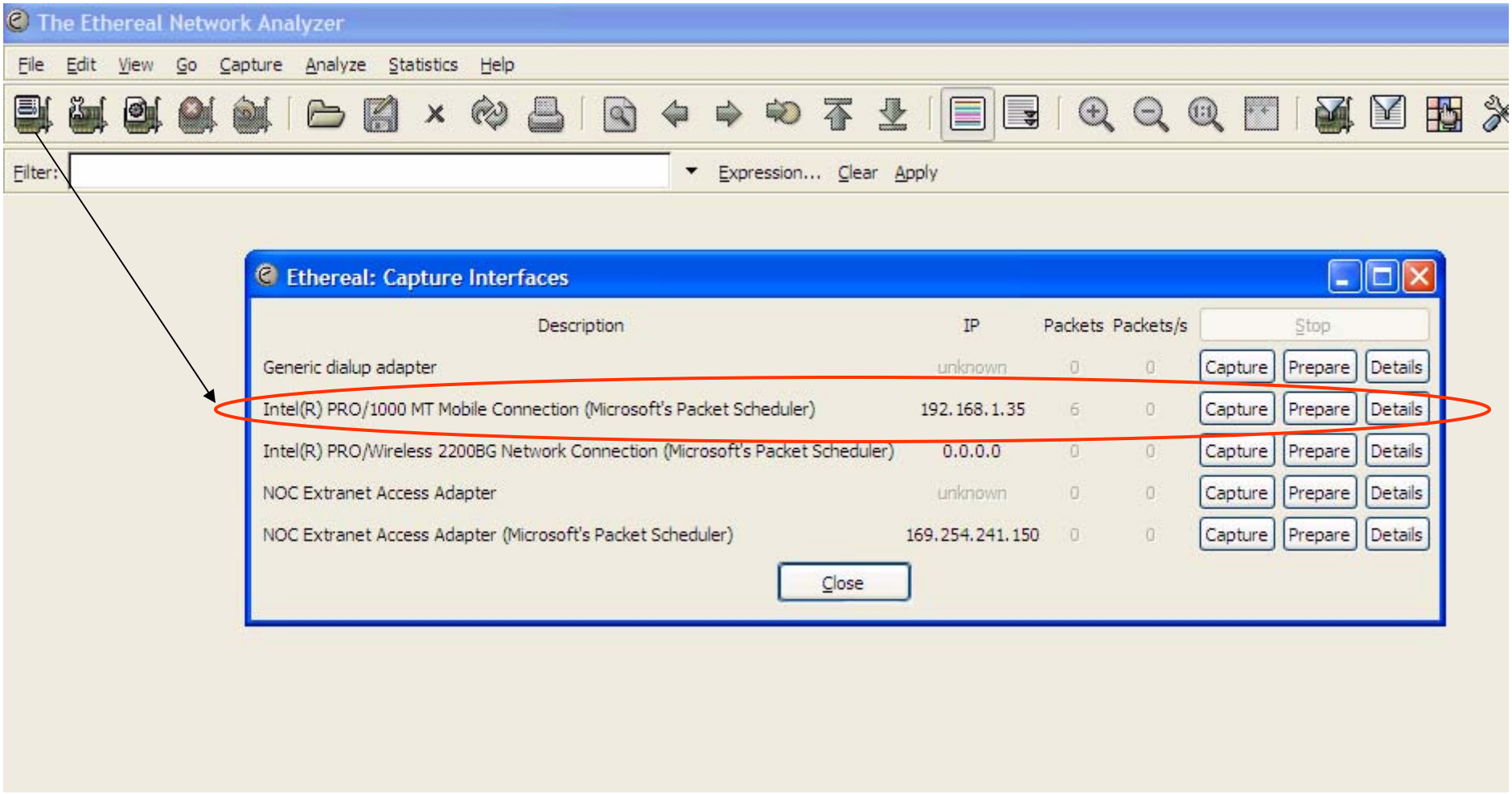
ThaiAdmin

Capturing Live Network Data



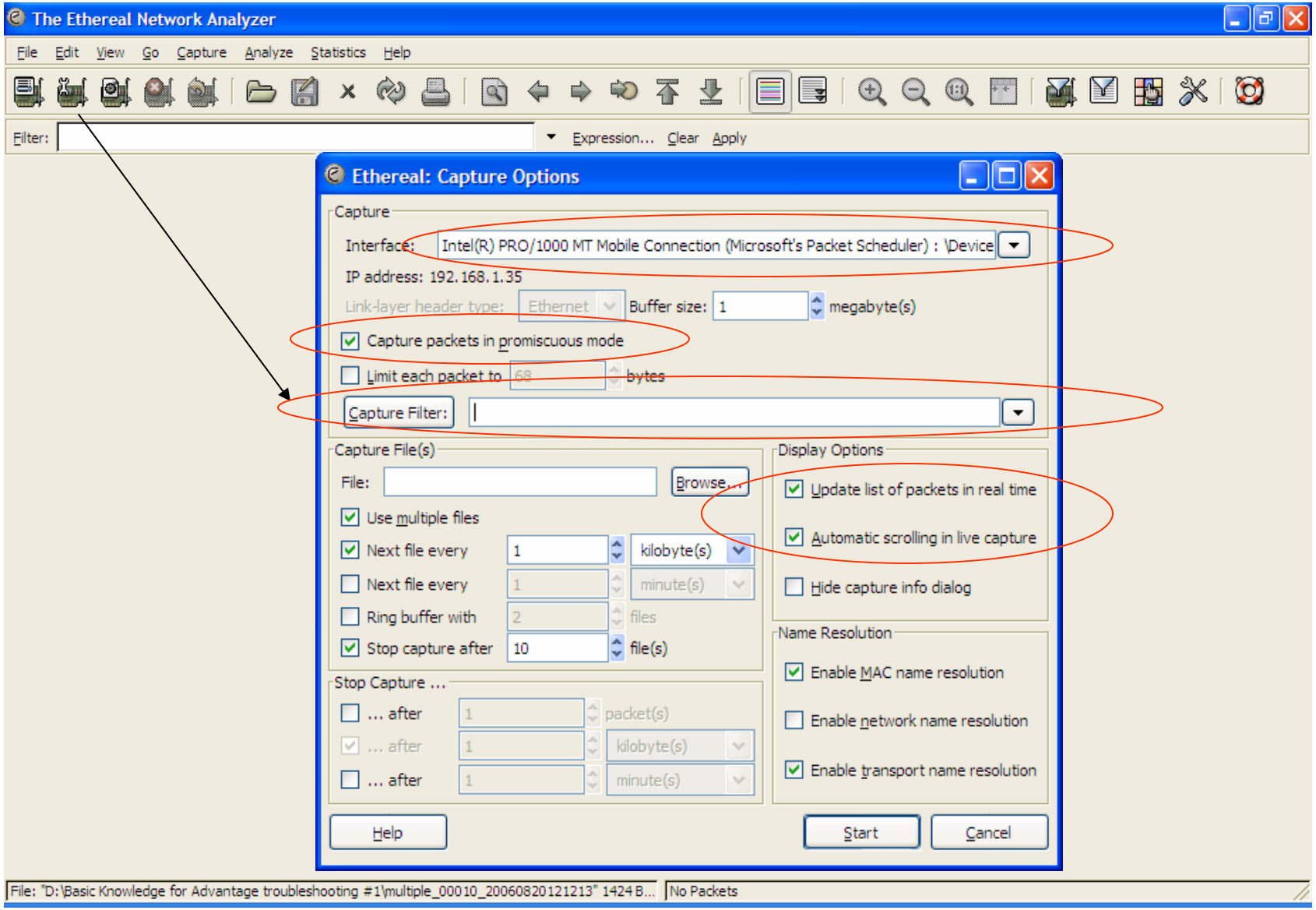
ThaiAdmin

List the Available Capture Interface



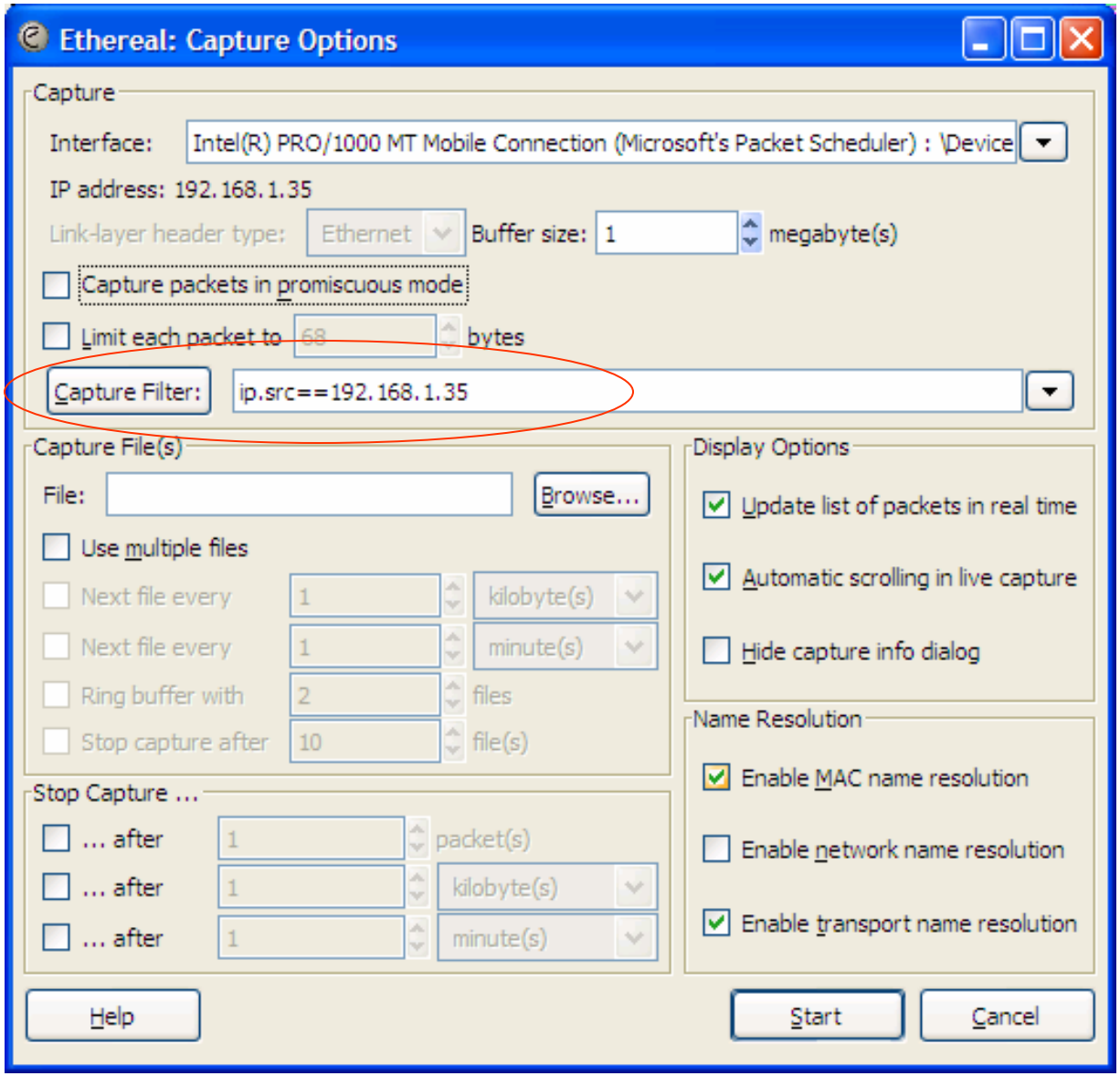
ThaiAdmin

Show the Capture Option



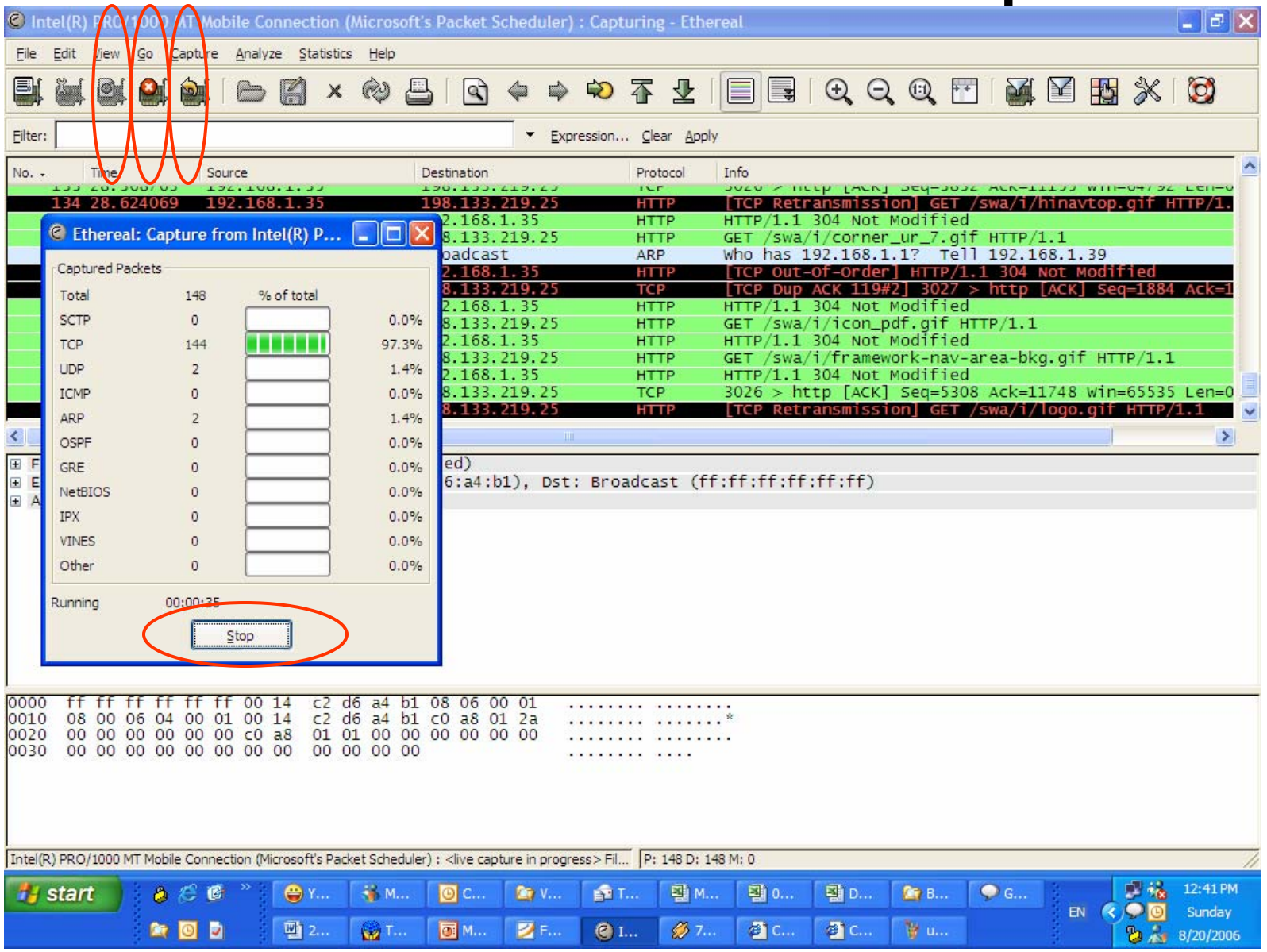
ThaiAdmin

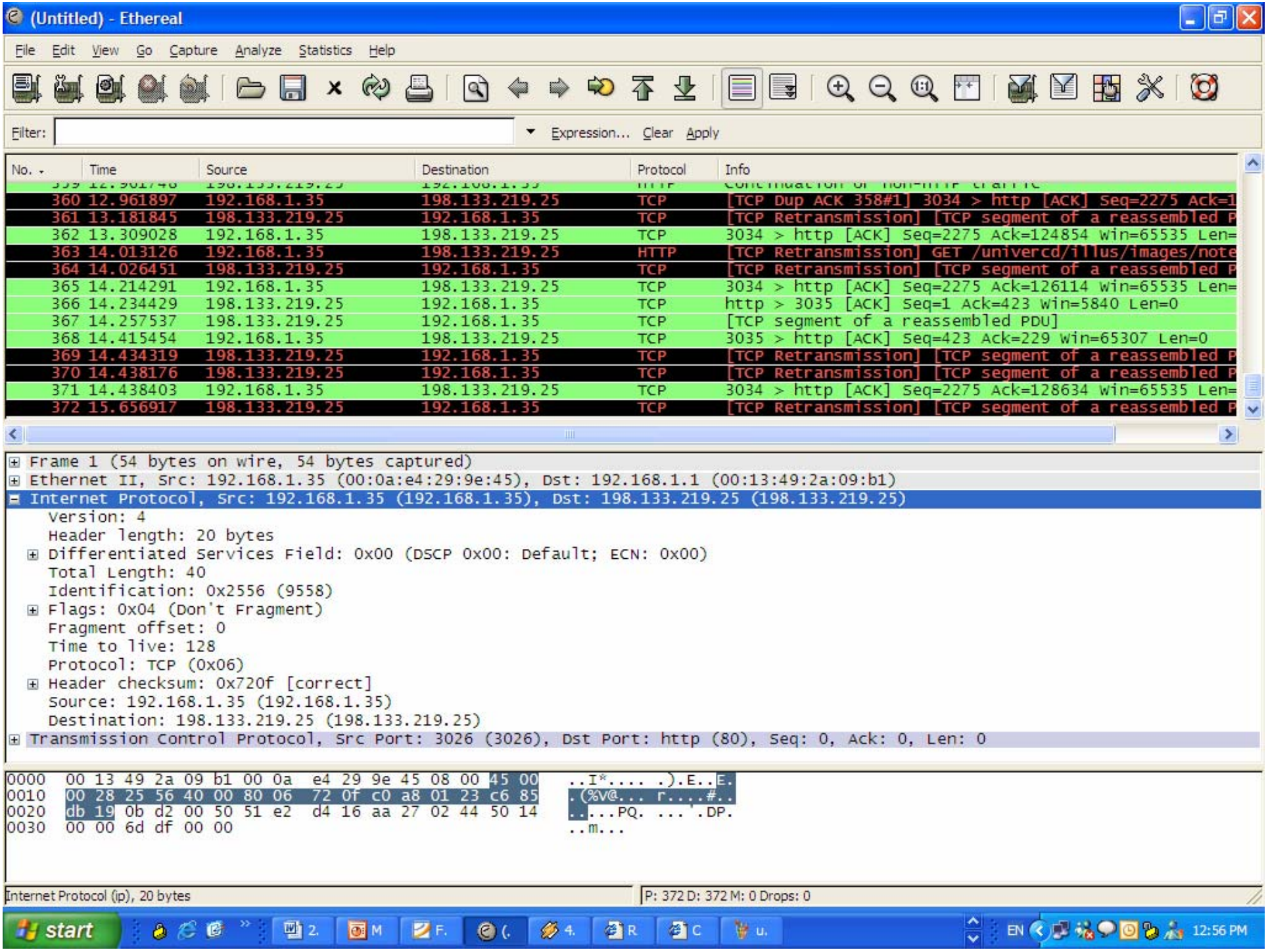
Capture Filter

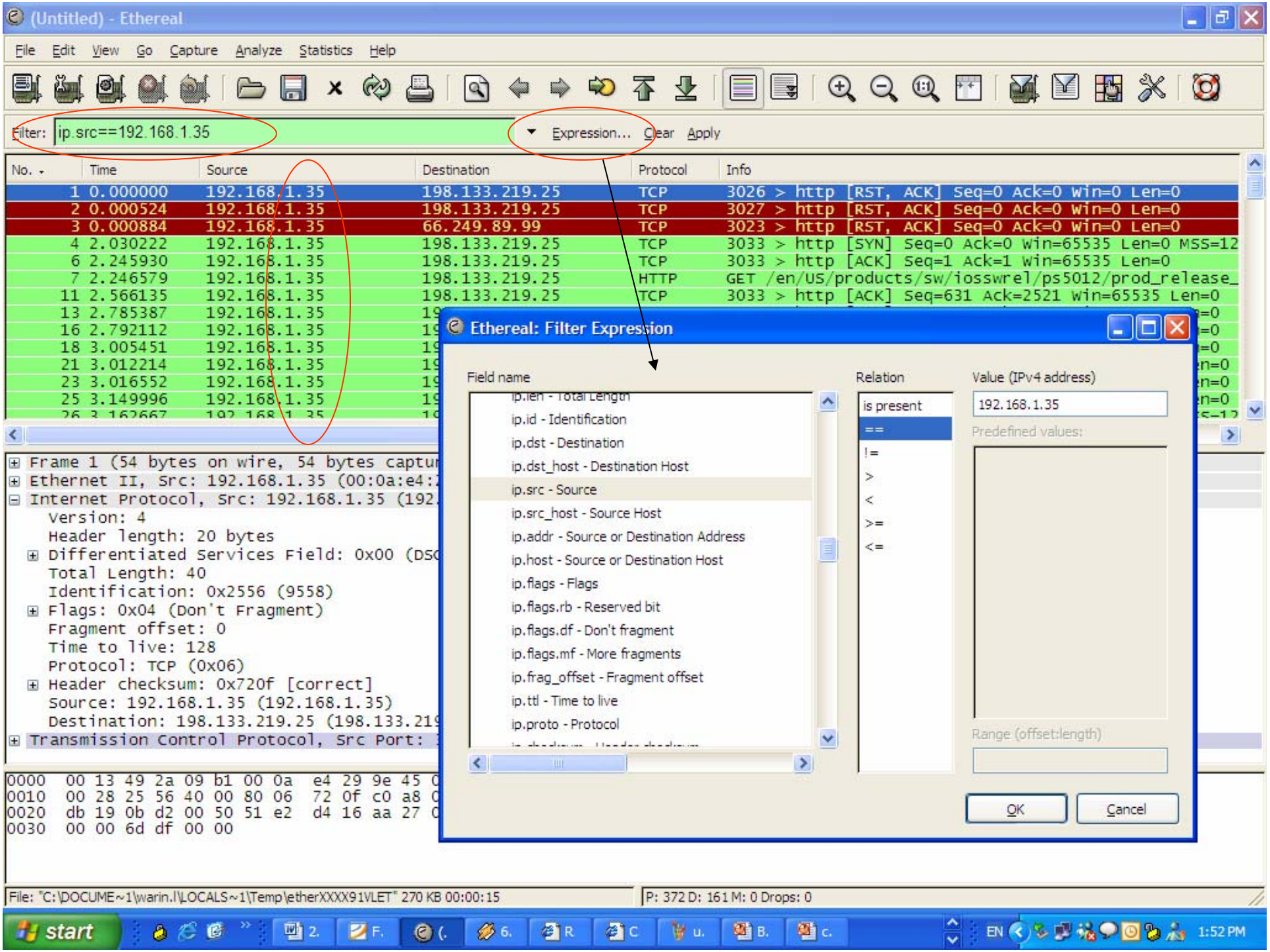


ThaiAdmin

Start a New Live Capture




(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
360 12.961897 192.168.1.35 198.133.219.25 TCP [TCP Dup ACK 358#1] 3034 > http [ACK] Seq=2275 Ack=1
361 13.181845 198.133.219.25 192.168.1.35 TCP [TCP Retransmission] [TCP segment of a reassembled P
362 13.309028 192.168.1.35 198.133.219.25 TCP 3034 > http [ACK] Seq=2275 Ack=124854 Win=65535 Len=
363 14.013126 192.168.1.35 198.133.219.25 HTTP [TCP Retransmission] GET /univercd/illus/images/note
364 14.026451 198.133.219.25 192.168.1.35 TCP [TCP Retransmission] [TCP segment of a reassembled P
365 14.214291 192.168.1.35 198.133.219.25 TCP 3034 > http [ACK] Seq=2275 Ack=126114 Win=65535 Len=
366 14.234429 198.133.219.25 192.168.1.35 TCP http > 3035 [ACK] Seq=1 Ack=423 Win=5840 Len=0
367 14.257537 198.133.219.25 192.168.1.35 TCP [TCP segment of a reassembled PDU]
368 14.415454 192.168.1.35 198.133.219.25 TCP 3035 > http [ACK] Seq=423 Ack=229 Win=65307 Len=0
369 14.434319 198.133.219.25 192.168.1.35 TCP [TCP Retransmission] [TCP segment of a reassembled P
370 14.438176 198.133.219.25 192.168.1.35 TCP [TCP Retransmission] [TCP segment of a reassembled P
371 14.438403 192.168.1.35 198.133.219.25 TCP 3034 > http [ACK] Seq=2275 Ack=128634 Win=65535 Len=
372 15.656917 198.133.219.25 192.168.1.35 TCP [TCP Retransmission] [TCP segment of a reassembled P
Frame 1 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 192.168.1.35 (00:0a:e4:29:9e:45), Dst: 192.168.1.1 (00:13:49:2a:09:b1)
Internet Protocol, Src: 192.168.1.35 (192.168.1.35), Dst: 198.133.219.25 (198.133.219.25)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 40
Identification: 0x2556 (9558)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x720f [correct]
Source: 192.168.1.35 (192.168.1.35)
Destination: 198.133.219.25 (198.133.219.25)
Transmission Control Protocol, Src Port: 3026 (3026), Dst Port: http (80), Seq: 0, Ack: 0, Len: 0
0000 00 13 49 2a 09 b1 00 0a e4 29 9e 45 08 00 45 00 ..I*.... .).E..E.
0010 00 28 25 56 40 00 80 06 72 0f c0 a8 01 23 c6 85 .(%V@... r....#..
0020 db 19 0b d2 00 50 51 e2 d4 16 aa 27 02 44 50 14 .....PQ. ...'.DP.
0030 00 00 6d df 00 00 ..m...
Internet Protocol (ip), 20 bytes
P: 372 D: 372 M: 0 Drops: 0
start
12:56 PM


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.src==192.168.1.35
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.1.35 198.133.219.25 TCP 3026 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
2 0.000524 192.168.1.35 198.133.219.25 TCP 3027 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
3 0.000884 192.168.1.35 66.249.89.99 TCP 3023 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
4 2.030222 192.168.1.35 198.133.219.25 TCP 3033 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=12
6 2.245930 192.168.1.35 198.133.219.25 TCP 3033 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7 2.246579 192.168.1.35 198.133.219.25 HTTP GET /en/US/products/sw/iosswrel/ps5012/prod_release_
11 2.566135 192.168.1.35 198.133.219.25 TCP 3033 > http [ACK] Seq=631 Ack=2521 Win=65535 Len=0
13 2.785387 192.168.1.35
16 2.792112 192.168.1.35
18 3.005451 192.168.1.35
21 3.012214 192.168.1.35
23 3.016552 192.168.1.35
25 3.149996 192.168.1.35
Frame 1 (54 bytes on wire, 54 bytes captur
Ethernet II, Src: 192.168.1.35 (00:0a:e4:
Internet Protocol, Src: 192.168.1.35 (192.
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSC
Total Length: 40
Identification: 0x2556 (9558)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x720f [correct]
Source: 192.168.1.35 (192.168.1.35)
Destination: 198.133.219.25 (198.133.219
Transmission Control Protocol, Src Port:
0000 00 13 49 2a 09 b1 00 0a e4 29 9e 45
0010 00 28 25 56 40 00 80 06 72 0f c0 a8
0020 db 19 0b d2 00 50 51 e2 d4 16 aa 27
0030 00 00 6d df 00 00
Ethereal: Filter Expression
Field name
ip.len - Total Length
ip.id - Identification
ip.dst - Destination
ip.dst_host - Destination Host
ip.src - Source
ip.src_host - Source Host
ip.addr - Source or Destination Address
ip.host - Source or Destination Host
ip.flags - Flags
ip.flags.rb - Reserved bit
ip.flags.df - Don't fragment
ip.flags.mf - More fragments
ip.frag_offset - Fragment offset
ip.ttl - Time to live
ip.proto - Protocol
Relation
is present
==
!=
>
<
>=
<=
Value (IPv4 address)
192.168.1.35
Predefined values:
Range (offset:length)
OK
Cancel
File: "C:\DOCUME~1\warin.I\LOCALS~1\Temp\etherXXXX91VLET" 270 KB 00:00:15
P: 372 D: 161 M: 0 Drops: 0
start
1:52 PM

Detail Protocol: BOOTP/DHCP

BOOTP

- Provides a means for downloading:
  - Static IP Address
  - Subnet mask
  - Default Router address
  - Boot server address and Boot file name
  - Option parameters
- Communicate on UDP Ports 67 (Server) and 68 (Client)

What is DHCP?

- An update version of BOOTP called the Dynamic Host Configuration Protocol
- A safe, reliable, and simple TCP/IP network configuration protocol
  - Conserves IP address by leasing them instead of assigning them permanently
  - Dynamically allocates reusable network address
  - Automatically provides minimal requirements of IP address, subnet mask, and default gateway

IP Address Assignment

- Automatic Allocation (static maps)
  - DHCP is preconfigured with MAC-IP address mapping
  - Devices always receive the same assigned address
  - Address are not shared
- Dynamic Allocation
  - Address are shared
  - Address is assigned for a specified period of time

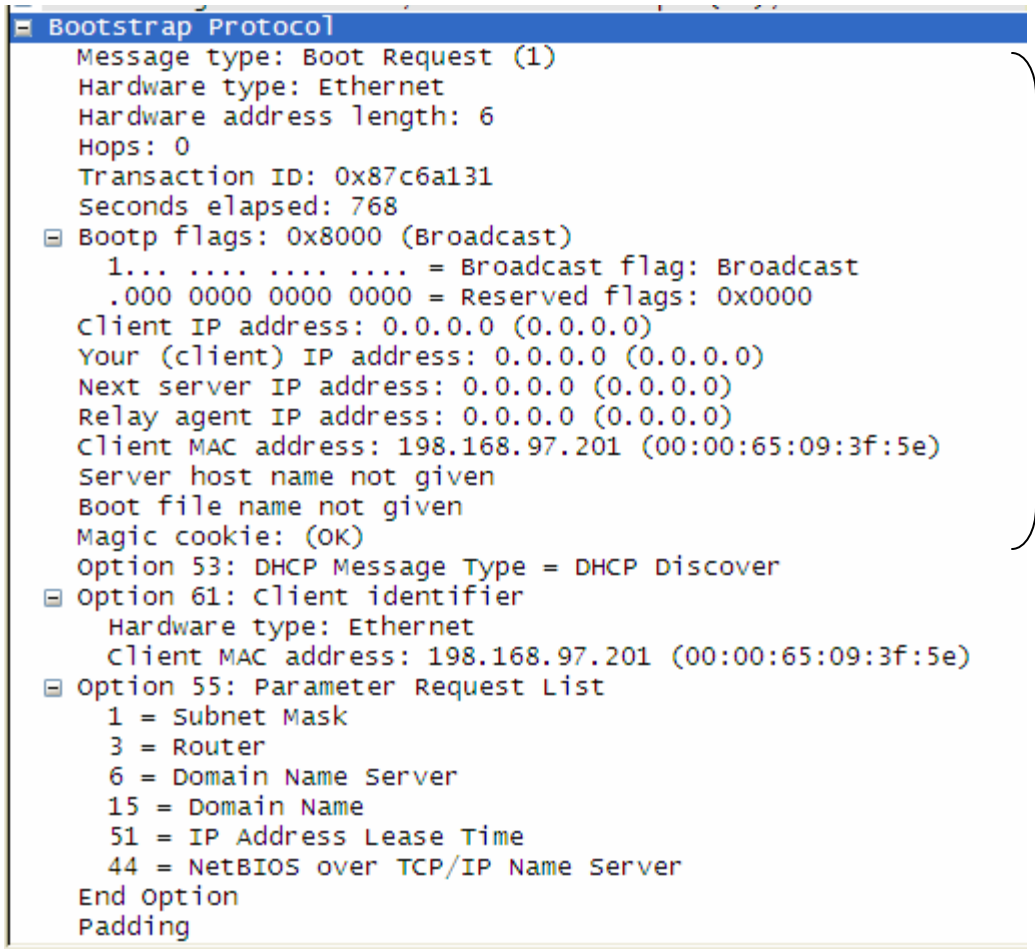
Dynamic Allocation Configuration

- Address ranges or “Scopes” are reserved on DHCP server for dynamic allocation
  - IP address is leased to DHCP client for a specified amount of time
  - DHCP Client must request lease renewal after a predefined period of time:
    - Renewal timer = 50% of lease time
    - Rebinding timer = 87.5% of lease time
    - Lease timer = 100% of lease time

ThaiAdmin

BOOTP/DHCP Headers

- Initial frames broadcast to DLC FFFFFFFFFFFF and IP 255.255.255.255
- Client uses UDP port 68, Sever uses port 67



Popular BOOTP/DHC Parameters

- Client IP configuration parameters
  - Subnet mask and broadcast address
  - Client Host name (may be different than domain name)
  - Internet Domain name
  - Default Ip Time-to-Live
  - Default Maximum transmission Unit (frame size)
  - Static Routers
- Client TCP parameters
  - TCP default TTL
  - TCP Keep-Alive Interval
  - Send TCP Keep-Alive Garbage Octet
- Lists of IP addresses for client to use
  - Domain Name Servers
  - Default Router

ThaiAdmin

DHCP Messages

- Discover: Finding DHCP server
- Offer: Server offer to Client
- Request: Client Request to Server
- Ack: Server > Client
- Nack: Server refuse client request
- Decline: Client > Server
- Release: Client > Server
- Inform: Client inform Server its parameter

ThaiAdmin

D.O.R.A Address Initialization

DHCP Client **DHCP Server**

Discover

Broadcast to all, Indicates hardware address type,
May offer an IP address and lease time

Offer

All servers unicast or broadcast to all, Offer an
Available IP address and timing information

Request

Broadcast to all, Indicates the chosen server
Address and preferred IP address

Ack

Chosen server commits the binding and broadcast to
All, The Ack includes the IP address and other
Configuration information. The remaining servers free
The address.

ThaiAdmin

DHCP Release and Renewal

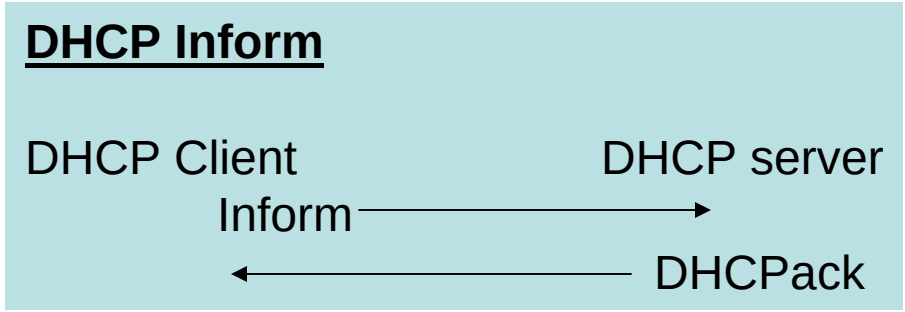
Address release

Address Renewal

Address Renewal Refusal

ThaiAdmin

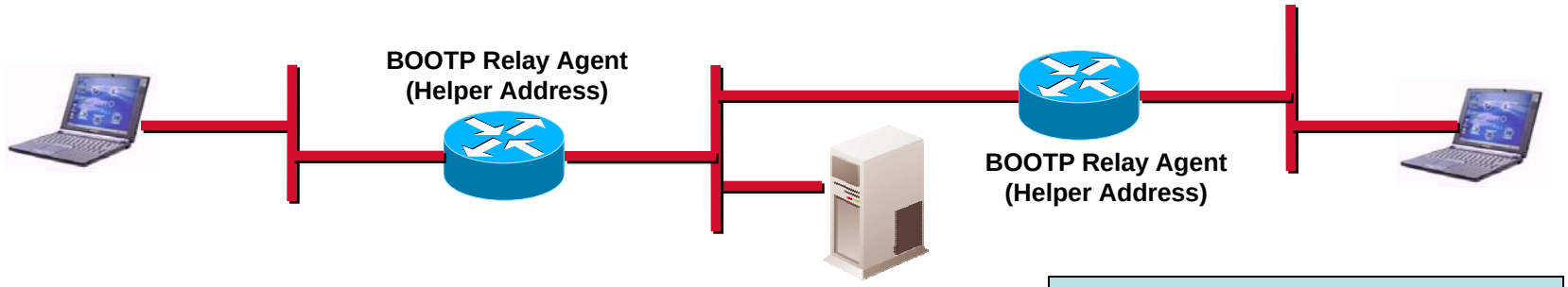
DHCP Inform

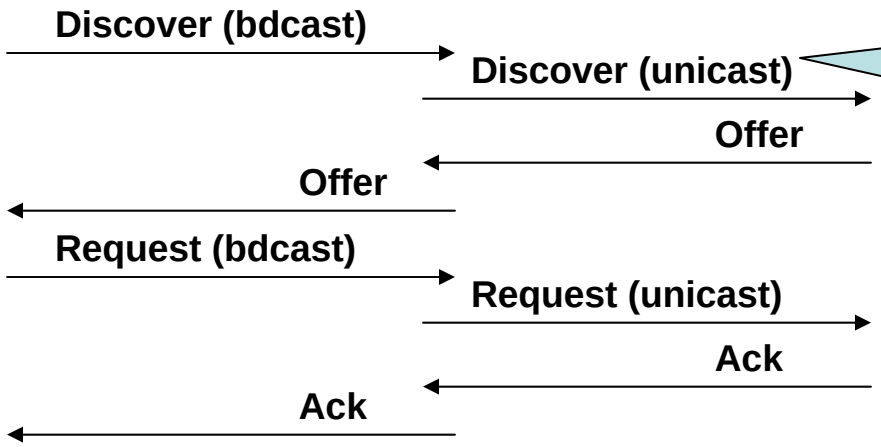


- Client has an externally configured network address
- DHCP Inform message allows the client to request local configuration information
- Server responds with DHCPack containing appropriate parameters
- Server does not check the address against the least table

BOOTP Relay

- DHCP server cannot communicate with clients on the other side of a router
  - A BOOTP Relay Agent must be enabled on the router and it must be configured to forward the messages





The server learns the subnet from the router's IP address so the correct address can be returned

DHCP Troubleshooting

- DHCP server thinks an address is expired
  - A client continues to use an address from cache that has now been leased to another client by the server
- Overlapping scopes with mulitple DHCP servers
  - The servers do not communicate to inform each other of their range of address
- The DHCP server ran out of address
- Duplicate IP address still occur with DHCP
  - Nothing stops a user from configuring a static OP address
  - Since Windows NT Sp2 allows the server to Ping an address to see if it is in use before it assigns it to a new host
- Use the **Advanced tab > IP** > **UDP** > **BOOTP** to filter in only BOOTP and DHCP frames

ThaiAdmin

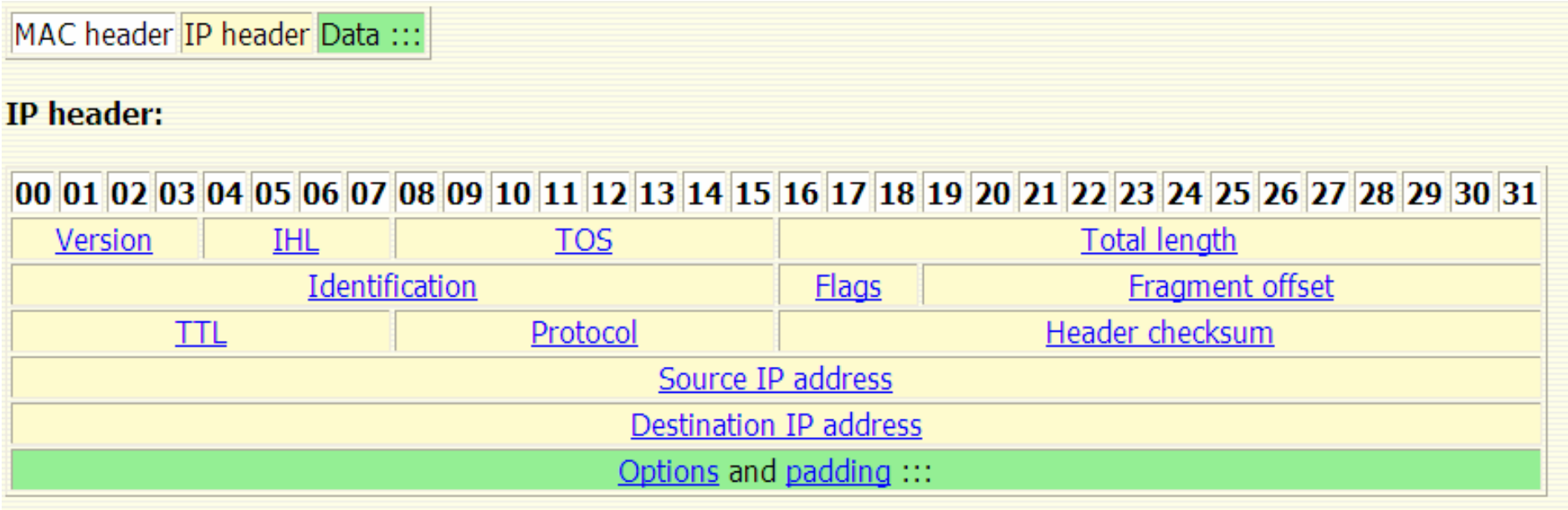
Demo-LAB

- DHCP Demo
- DHCP Troubleshooting
- DHCP Relay

Detail Protocol: IP v4

ThaiAdmin

IP Header



ThaiAdmin

IP Header (Cont.)

Version. 4 bits.
Specifies the format of the IP packet header.

Version	Description
0	Reserved.
1 2 3	
4	IP, Internet Protocol.
5	ST, ST Datagram Mode.
6	SIP, Simple Internet Protocol. SIPP, Simple Internet Protocol Plus. IPv6, Internet Protocol.
7	TP/IX, The Next Internet.
8	PIP, The P Internet Protocol.
9	TUBA
10 - 14	
15	reserved.

ThaiAdmin

IP Header (Cont.)

IHL, Internet Header Length. 4 bits.
Specifies the length of the IP packet header in 32 bit words. The minimum value for a valid header is 5.

TOS, Type of Service. 8 bits.
Specifies the parameters for the type of service requested. The parameters may be utilized by networks to define the handling of the datagram during transport. The M bit was added to this field in RFC 1349.

00	01	02	03	04	05	06	07
Precedence			D	T	R	M	0

Precedence. 3 bits.

Value	Description
0	Routine.
1	Priority.
2	Immediate.
3	Flash.
4	Flash override.
5	CRITIC/ECP.
6	Internetwork control.
7	Network control.

D. 1 bit.
Minimize delay.

Value	Description
0	Normal delay.
1	Low delay.

T. 1 bit.
Maximize throughput.

Value	Description
0	Normal throughput.
1	High throughput.

R. 1 bit.
Maximize reliability.

Value	Description
0	Normal reliability.
1	High reliability.

M. 1 bit.
Minimize monetary cost.

Value	Description
0	Normal monetary cost.
1	Minimize monetary cost.

ThaiAdmin

IP Header (Cont.)

Total length. 16 bits.
Contains the length of the datagram.

Identification. 16 bits.
Used to identify the fragments of one datagram from those of another. The originating protocol module of an internet datagram sets the identification field to a value that must be unique for that source-destination pair and protocol for the time the datagram will be active in the internet system. The originating protocol module of a complete datagram clears the *MF* bit to zero and the *Fragment Offset* field to zero.

ThaiAdmin

IP Header (Cont.)

Flags. 3 bits.

00	01	02
R	DF	MF

R, reserved. 1 bit.
Should be cleared to 0.

DF, Don't fragment. 1 bit.
Controls the fragmentation of the datagram.

Value	Description
0	Fragment if necessary.
1	Do not fragment.

MF, More fragments. 1 bit.
Indicates if the datagram contains additional fragments.

Value	Description
0	This is the last fragment.
1	More fragments follow this fragment.

ThaiAdmin

IP Header (Cont.)

Fragment Offset. 13 bits.
Used to direct the reassembly of a fragmented datagram.

TTL, Time to Live. 8 bits.
A timer field used to track the lifetime of the datagram. When the TTL field is decremented down to zero, the datagram is discarded.

Protocol. 8 bits.
This field specifies the next encapsulated protocol.

Value	Protocol
0	HOPOPT, IPv6 Hop-by-Hop Option.
1	ICMP, Internet Control Message Protocol.
2	IGAP, IGMP for user Authentication Protocol. IGMP, Internet Group Management Protocol. RGMP, Router-port Group Management Protocol.
3	GGP, Gateway to Gateway Protocol.
4	IP in IP encapsulation.

ThaiAdmin

IP Header (Cont.)

Header checksum. 16 bits.
A 16 bit one's complement checksum of the IP header and IP options.

Source IP address. 32 bits.
IP address of the sender.

Destination IP address. 32 bits.
IP address of the intended receiver.

Options. Variable length.

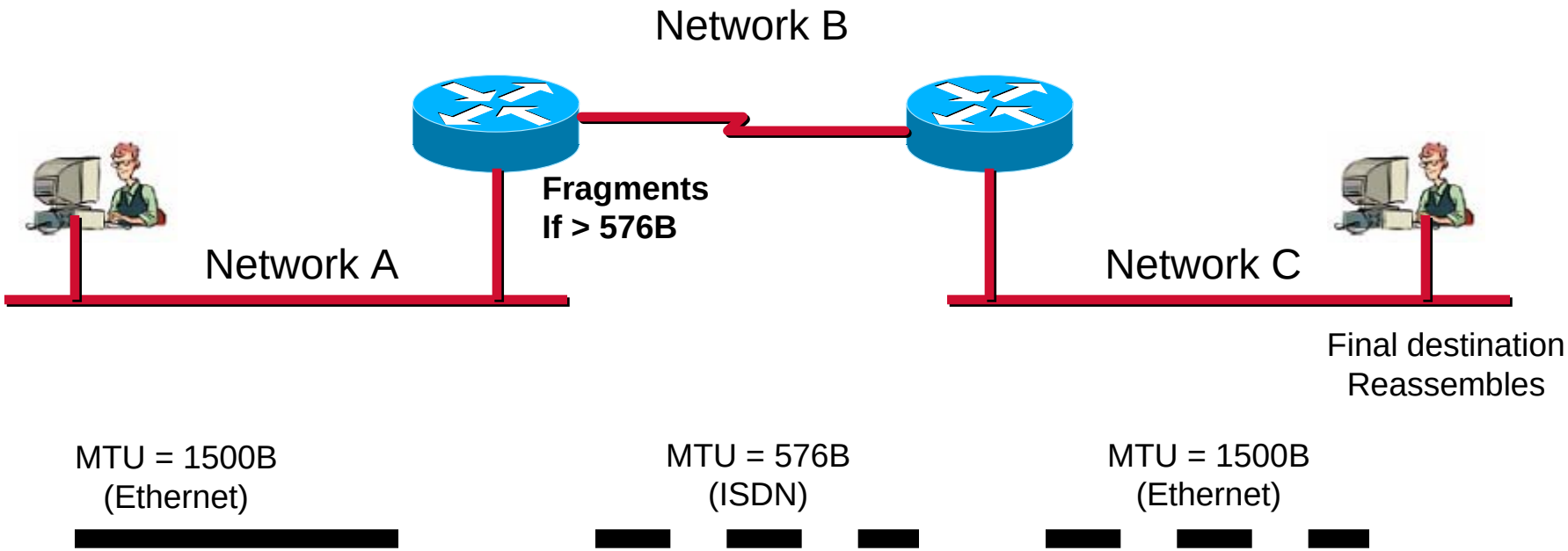
00	01	02	03	04	05	06	07
C	Class	Option					

Padding. Variable length.
Used as a filler to guarantee that the data starts on a 32 bit boundary.

MHTML Document

ThaiAdmin

IP Fragmentation and Reassembly



MTU = Maximum Transfer Unit

ThaiAdmin

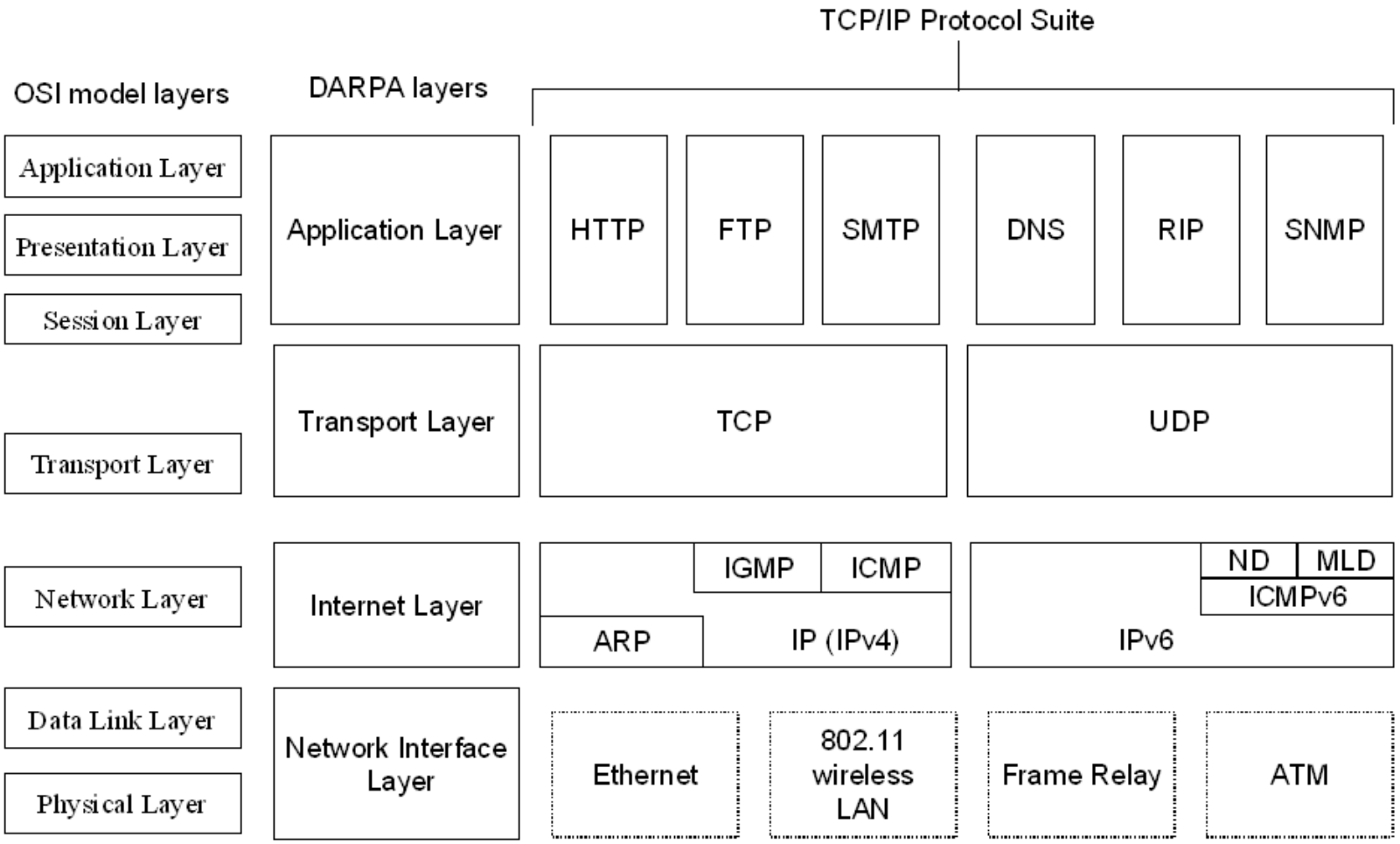
Demo-LAB

- IP Header Demo
- Missing Fragmentation

Detail Protocol: ARP

ThaiAdmin

ARP/RARP Layer



ThaiAdmin

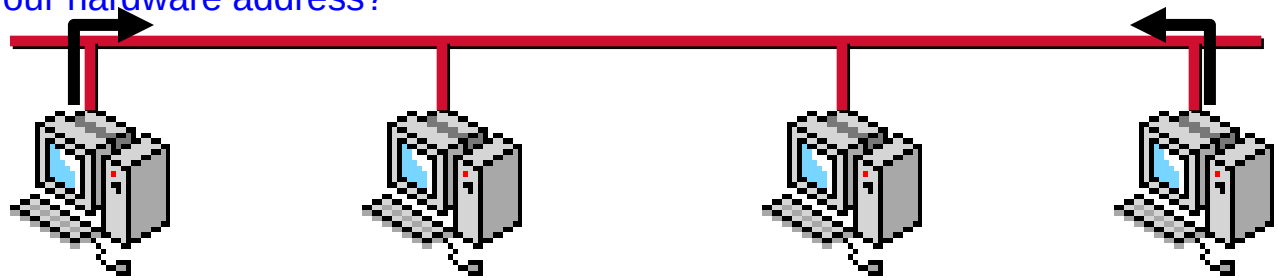
How ARP Works

- Each station maintains as Address Resolution Cache of recently acquired physical/internet address

Station A checks its ARP cache to see if it has Station B's hardware address. If it isn't in caches, it uses its address mask to determine if Station B is on its subnet. If yes, it uses ARP to get it.

Broadcast:
Station B, where are you?
I know your IP address;
What is your hardware address?

Point to Point:
My hardware address is xxxxxx



Station A
192.68.37.48

Address cached

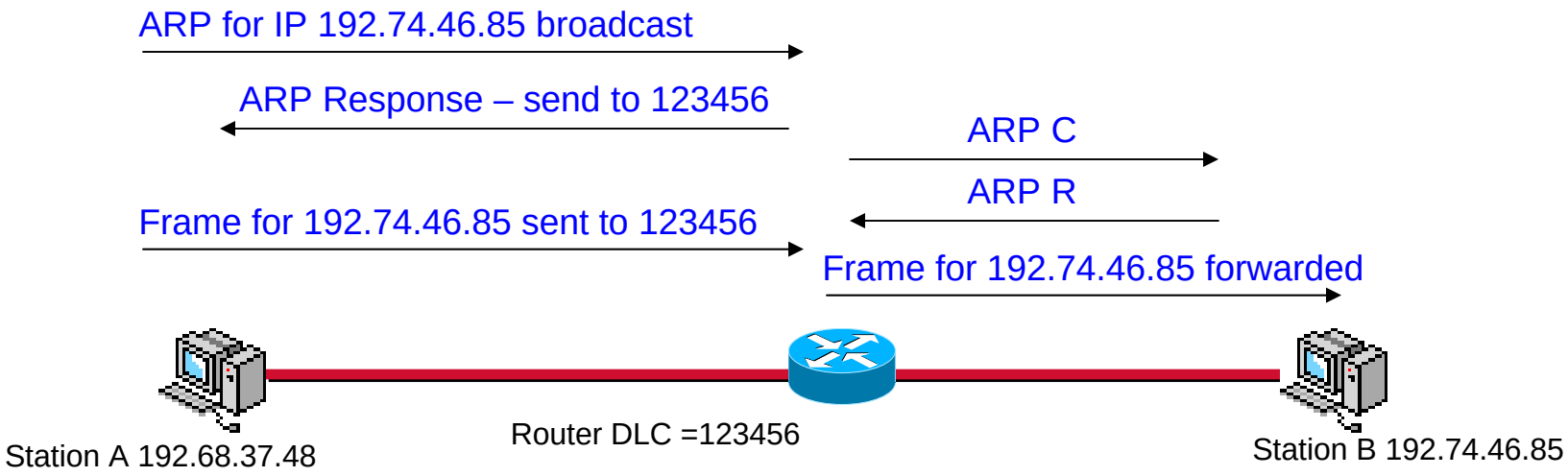
Station B
192.68.37.136

ARP and Network Devices

- ARP frames are broadcast
- Hubs, switches and bridges forward ARP frames so everyone on the subnet hears them
  - If the device is active, it responds directly to the source
- Routers do not forward ARP frames

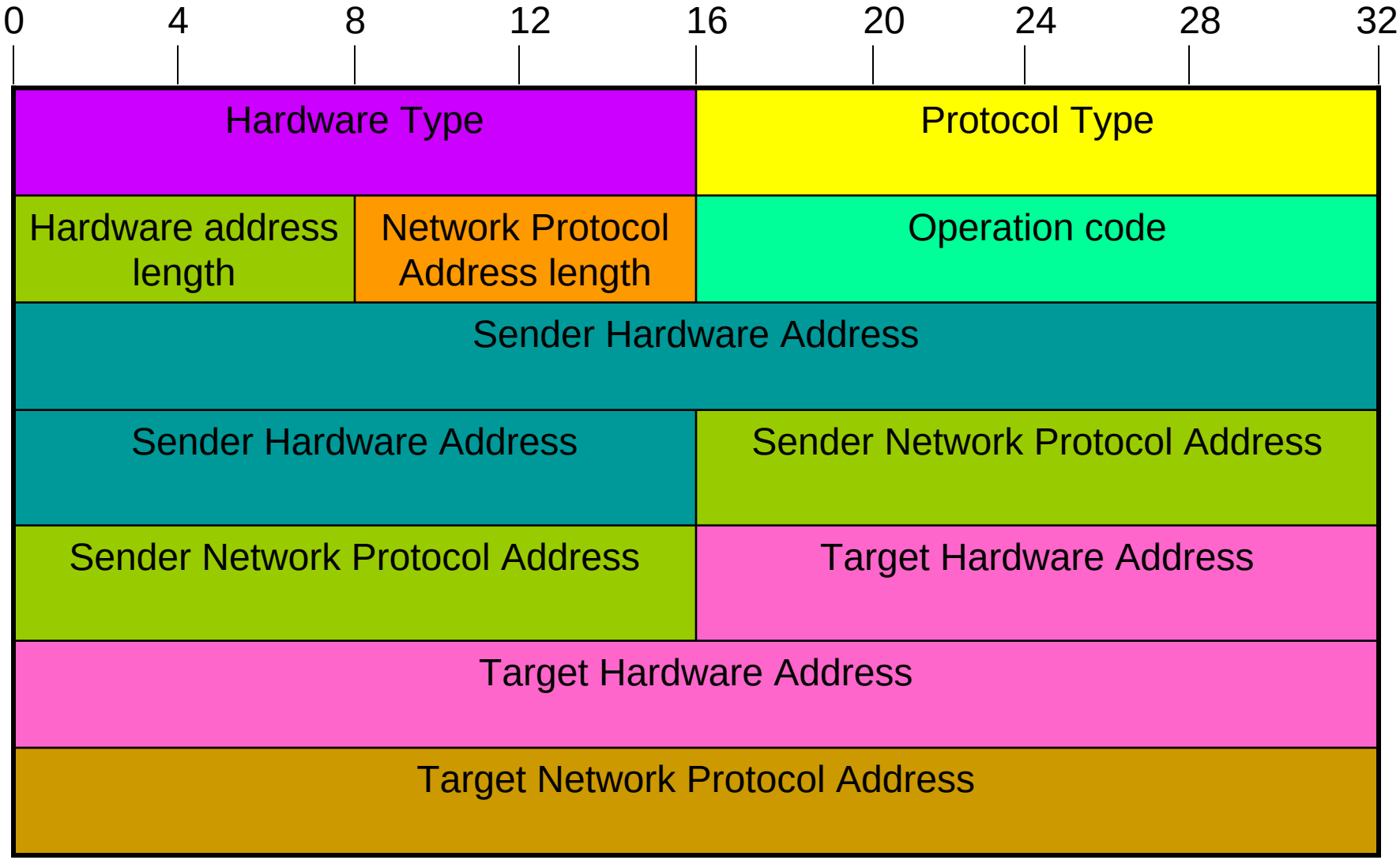
Proxy ARP

- Station A needs to communicate to Station B but does not have a default gateway (or use it's own IP address for the gateway). How can it learn an appropriate DLC address? **Proxy ARP!**
- Station A needs a DLC address to map to the known IP address for B. A ARPs on its own segment and the router responds with its DLC address (knowing that the destination network is accessible via its other port)
- When A sends its request to B, it will then use B's IP address and the router's DLC address. The router will then route the packet to B



ThaiAdmin

ARP/RARP Frame Format



ARP Field Descriptions

- Hardware Type (2 bytes). 1=ethernet.
- Protocol Type(2 bytes). 0800H (hex) = IP address.
- Hardware Address Length(1 byte). 6
- Network Protocol Address Length (1 byte). 4
- Operation Code. 1 = ARP request, 2=ARP reply, 3=RARP request, 4=RARP reply.
- The sender's ethernet address (6 bytes)
- The sender's IP address (4 bytes)
- The recipient's ethernet address (6 bytes)
- The recipient's IP address (4 bytes)

Other ARPs

- Reverse ARP
  - Locates the IP address for a hardware address
  - Used for diskless workstations
- Inverse ARP
  - A device sends an ARP after obtaining an address through DHCP
  - Used Mainly in Frame Relay and ATM
- Gratuitous ARP – two types
  - A device sends an ARP after obtaining an address through DHCP to check it's unique
    - Prevents conflicts with hard-coded devices
  - A device sends an ARP broadcast for its own address to update others on the network
    - Receivers update their ARP cache
- UnARP
  - ARP response frame with zeros in the hardware address fields
  - Receivers remove entry from cache

ARP troubleshooting Tips

- Filter on ARP protocol
- Look for ARP command with no replies
  - Many upper layer protocols ARP to get the address first
  - Upper layer problems may be due to ARP failures
  - Ensure proxy ARP is enabled on the router
  - Check for signs of default gateway configuration problems
- Filter on individual address to check intervals of ARPs to find aging table and gratuitous ARP problems
  - This is important on routers
- Look for ARP sweeps
  - A series of ARPs with incrementing IP address indicates an automated test program is running or a hacker is trying to break in
  - Confirm the source is authorized

ThaiAdmin

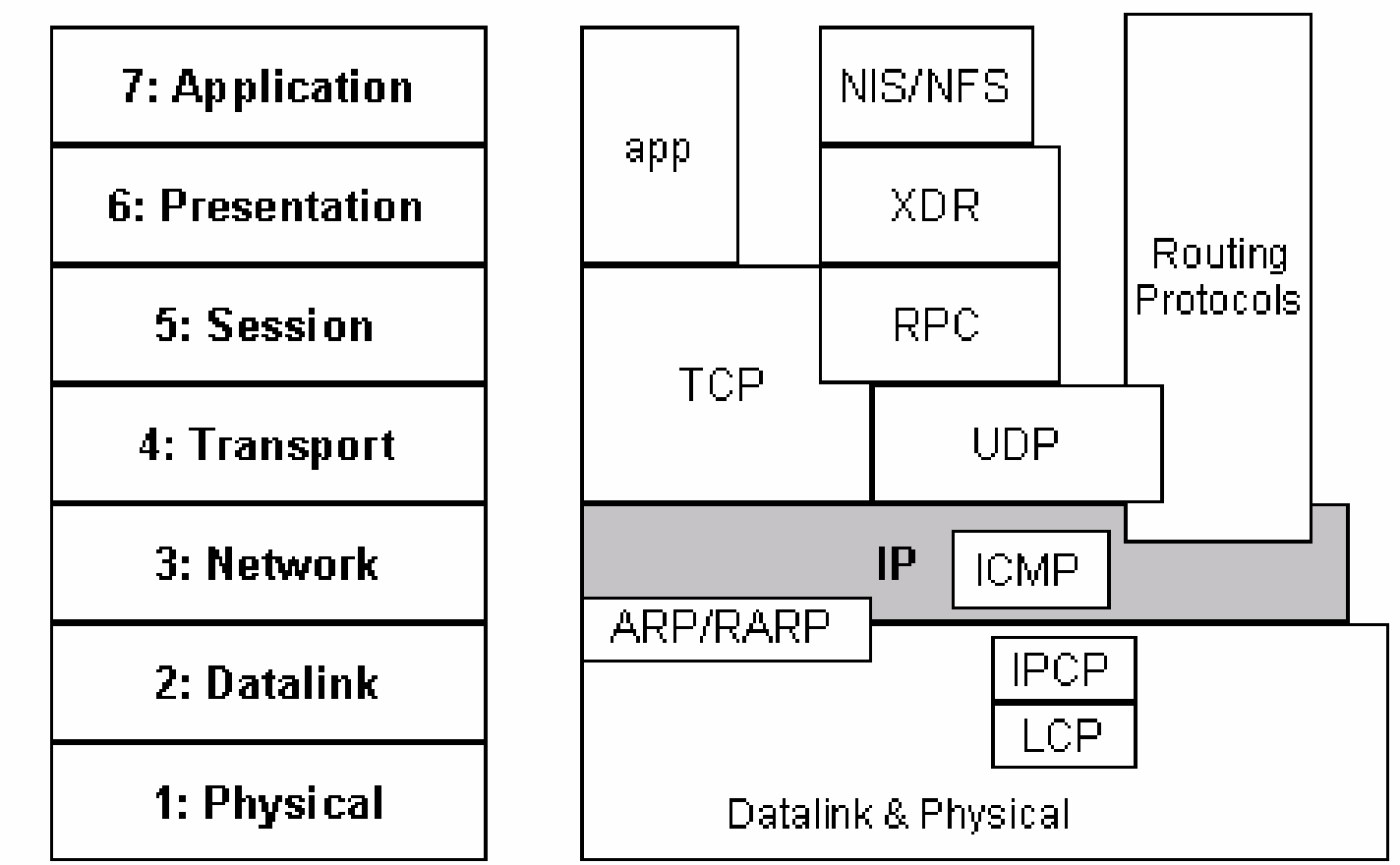
Demo-LAB

- Complete & Fail ARP
- Reverse ARP
- Gratuitous ARP

Detail Protocol: ICMP

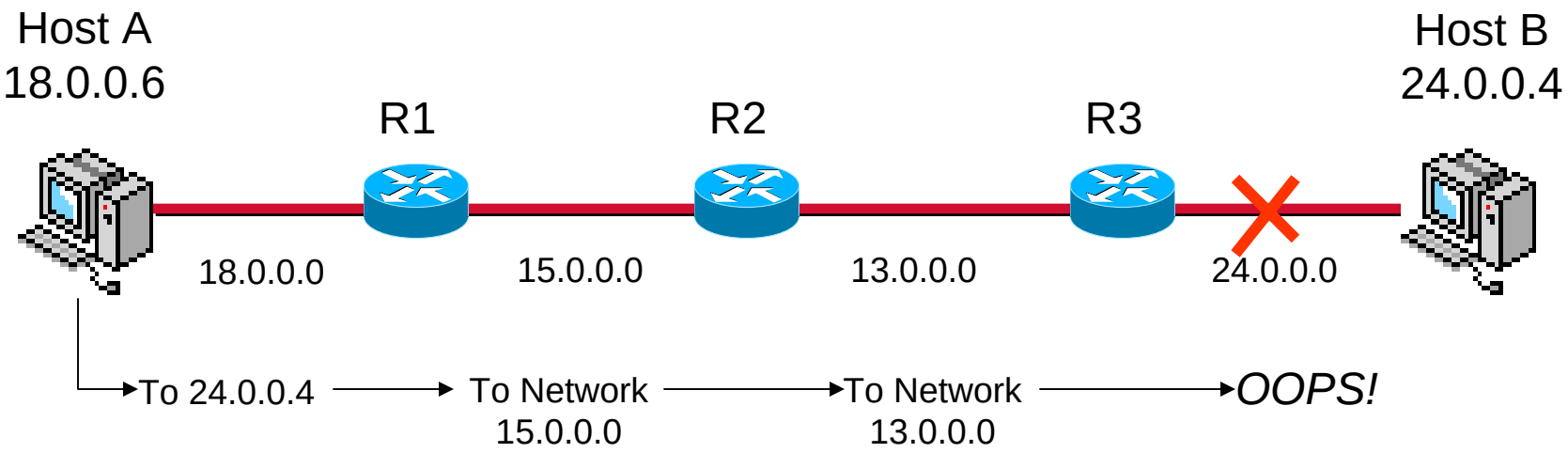
ThaiAdmin

ICMP Layer



ThaiAdmin

Reporting Trouble with IP Routing



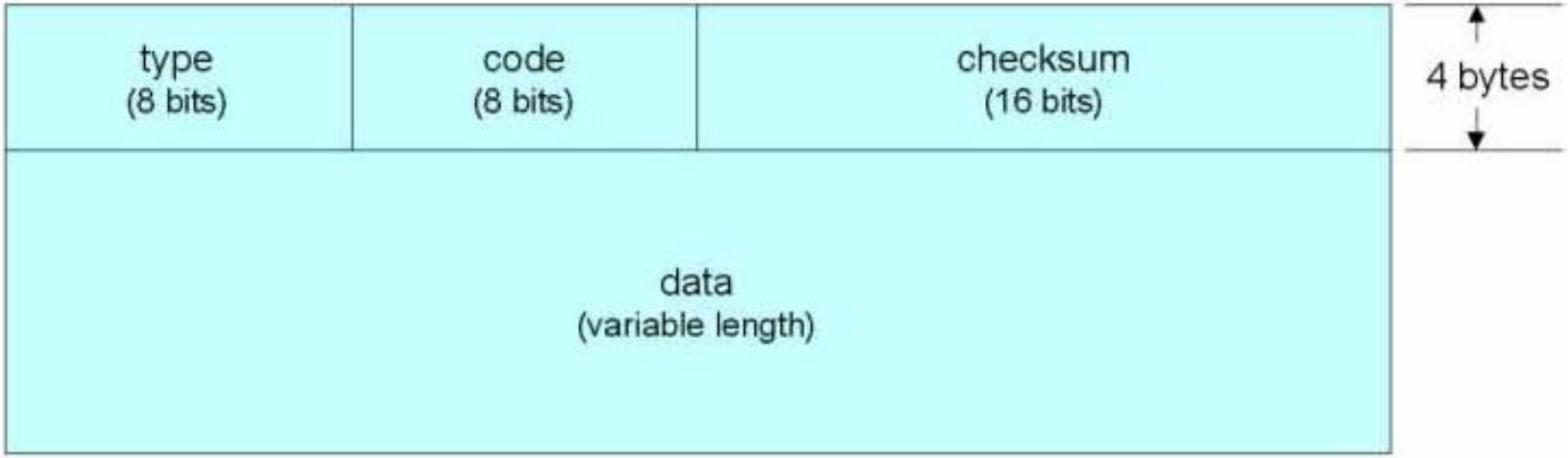
Q: How can you tell Host A the bad news?

A: ICMP!

ICMP net unreachable

ThaiAdmin

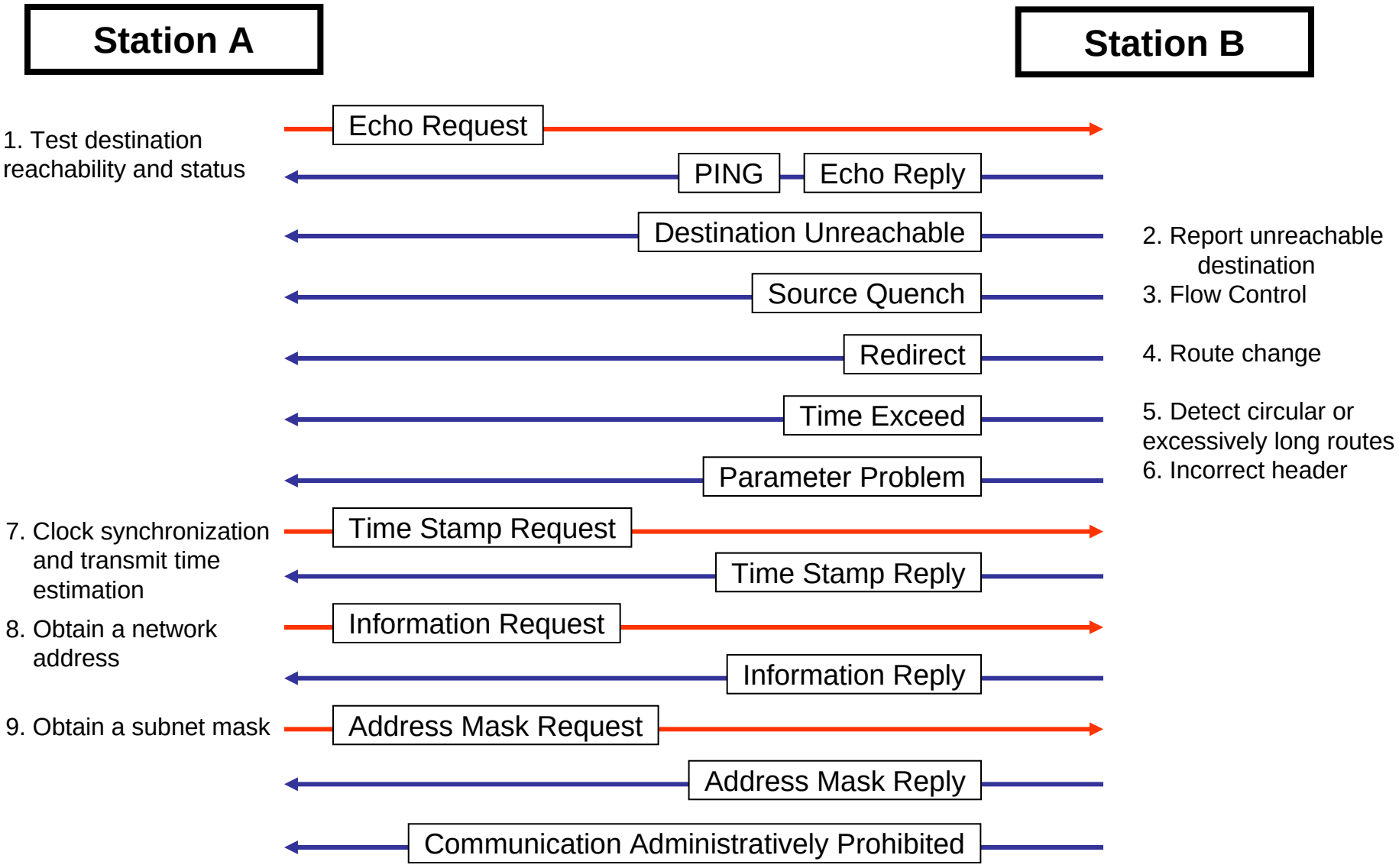
ICMP Message Format



ICMP message types			
type	description	type	description
0	echo reply	11	time exceeded
3	destination unreachable	12	parameter problem
4	source quench	13	timestamp request
5	redirect	14	timestamp reply
8	echo request	17	address mask request
9	router advertisement	18	address mask reply
10	router solicitation		

ThaiAdmin

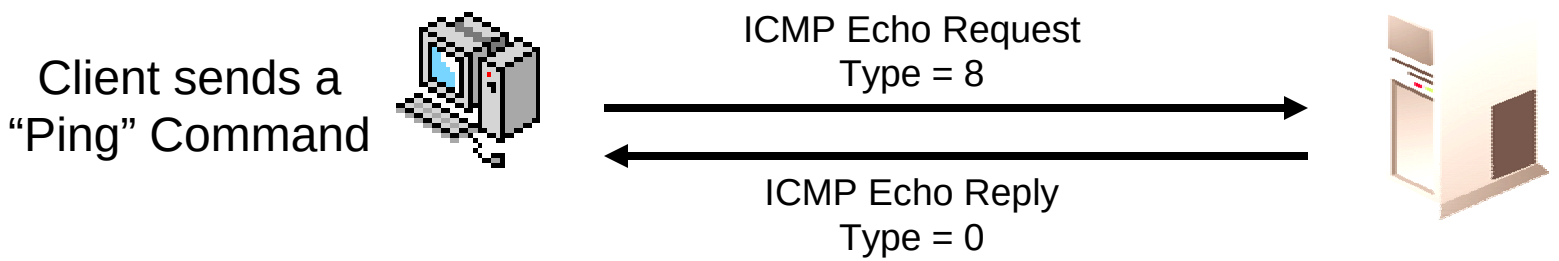
ICMP Message



ThaiAdmin

Echo Request/Reply Message

Field Size (Bits)	Field Name	Field Description
8	Type	**Echo Request = “8”, Echo Reply = “0”**
8	Code	“0”
16	Checksum	16-Bits One’s Complement of the Oned’s Complement sum of the ICMP message
16	Identifier	Used by client to match request to replies
16	Sequence Number	Used by client to match request to replies
Variable	Optional Data	Data to be returned to the client. An Echo Reply must return the same data as was received in the request



Destination Unreachable Message

Field Size (Bits)	Field Name	Field Description
8	Type	3
8	Code	0 = Net unreachable 1 = Host unreachable 2 = Protocol unreachable 3 = Port unreachable 4 = Fragmentation needed and “Don’t Fragment “Bit set 5 = Source Route Failed 6 = Destination network unknown 7 = destination host unknown 8 = source host not isolated 9 = Communication with destination network administratively prohibited 10 = same but host prohibited 11 = network unreachable for type of service 12 = Host unreachable for type of service
16	Checksum	16-Bits One’s Complement of the Oned’s Complement sum of the ICMP message
32	Unused	unused
Variable	IP Header + first 64 bits of Datagram	Used by the host to match the message to the appropriate process

ThaiAdmin

Destination Unreachable Message

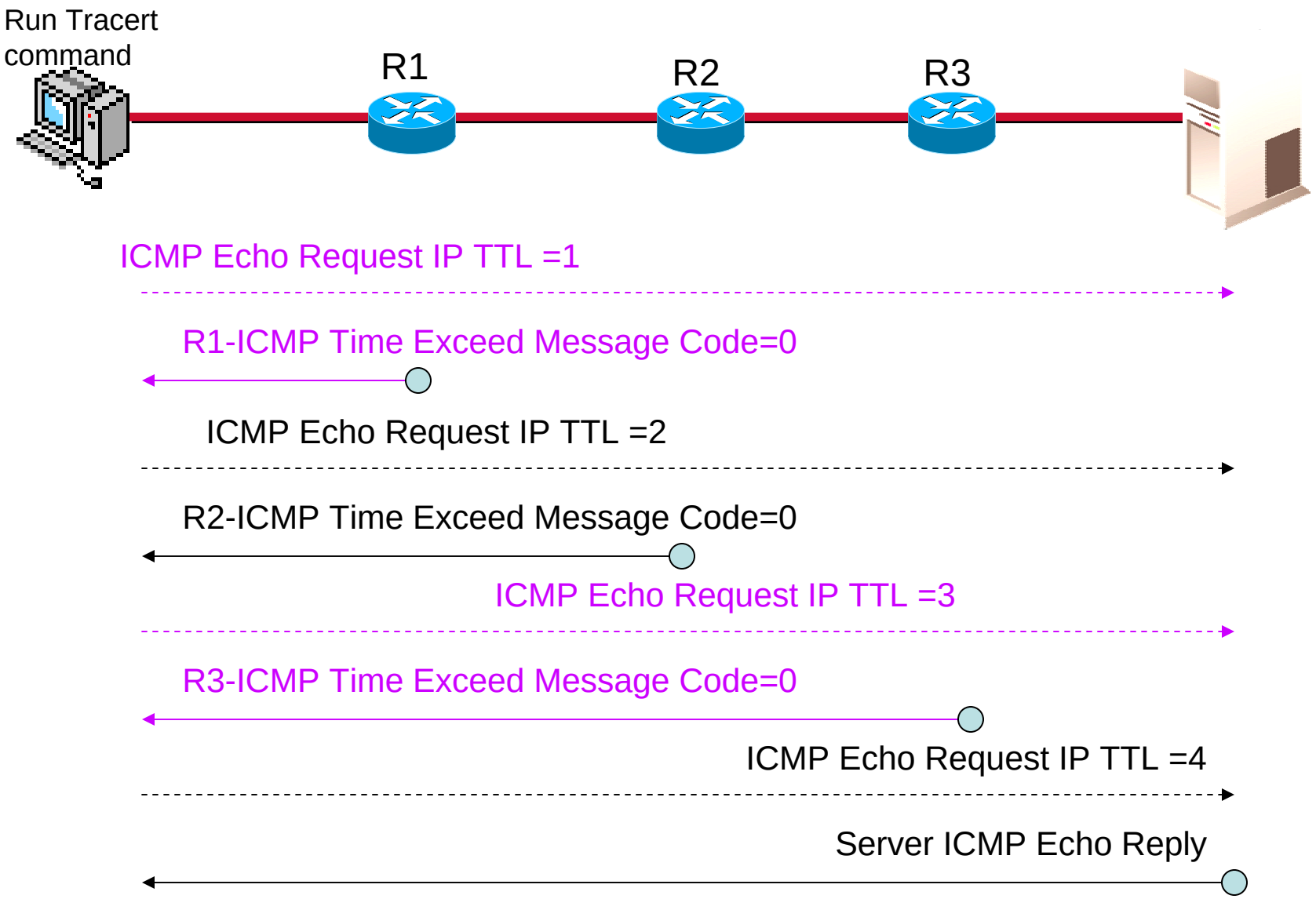
	Massage	Device	Layer
1.	Destination Network Unreachable	Router	Network
2.	Destination host Unreachable	Router	Network
3.	Protocol Unreachable	Host	Transport
4.	Port Unreachable	Host	Transport
5.	Fragment needed, don’t fragment bit set	Router	Network
6.	Source route failed	Router	Network
9.	Communication administratively prohibited	Router	Network

Time Exceeded Message

Field Size (Bits)	Field Name	Field Description
8	Type	11
8	**Code**	**0 = time to Live (TTL) Exceed in Transit** **1 = Fragment Reassembly Time Exceeded**
16	Checksum	16-Bits One's Complement of the Oned's Complement sum of the ICMP message
32	Unused	Not Used
Variable	IP Header + first 64 bits of Datagram	Used by the host to match the message to the appropriate process

ThaiAdmin

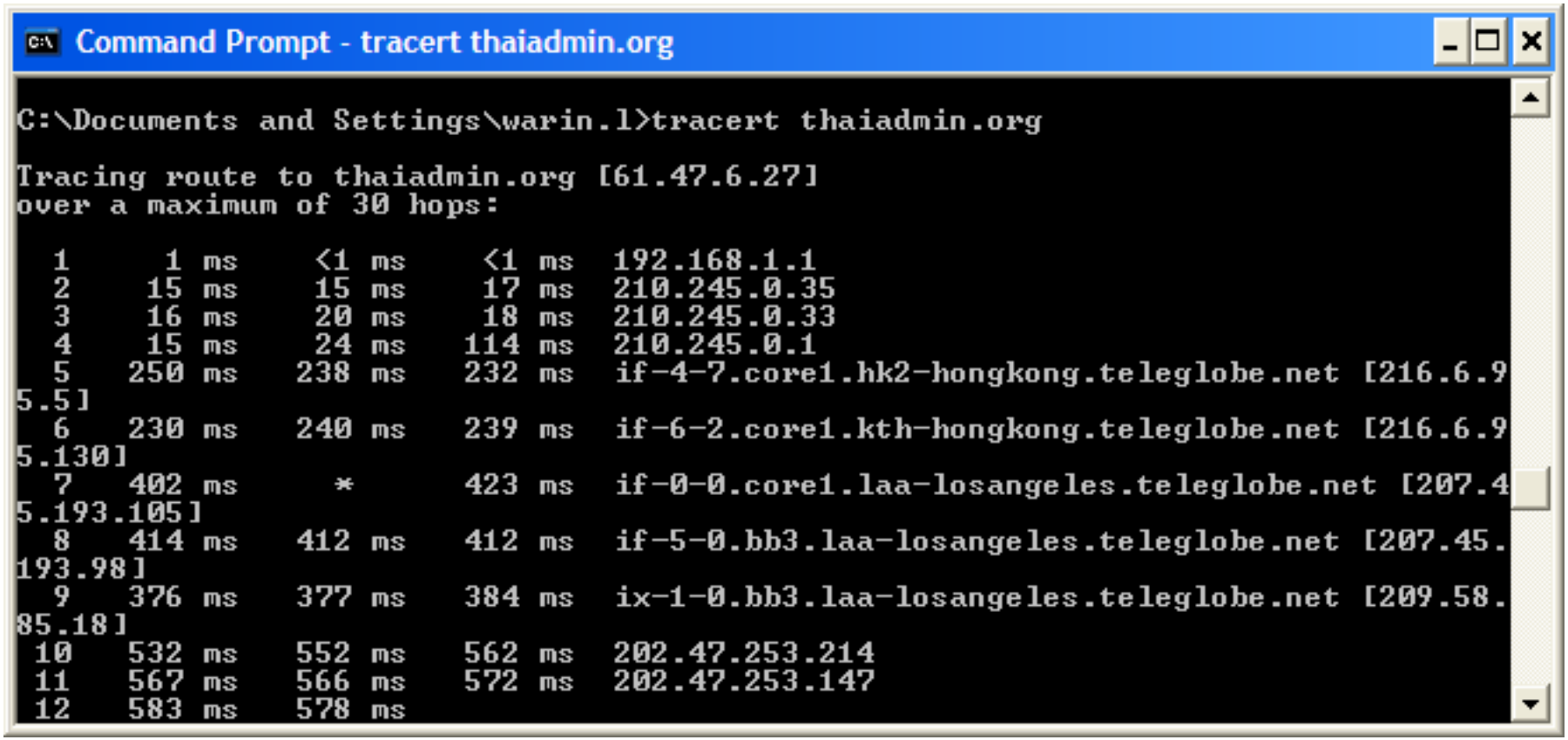
Time Exceeded Message



ThaiAdmin

Trace Route - Demo

- TRACERT

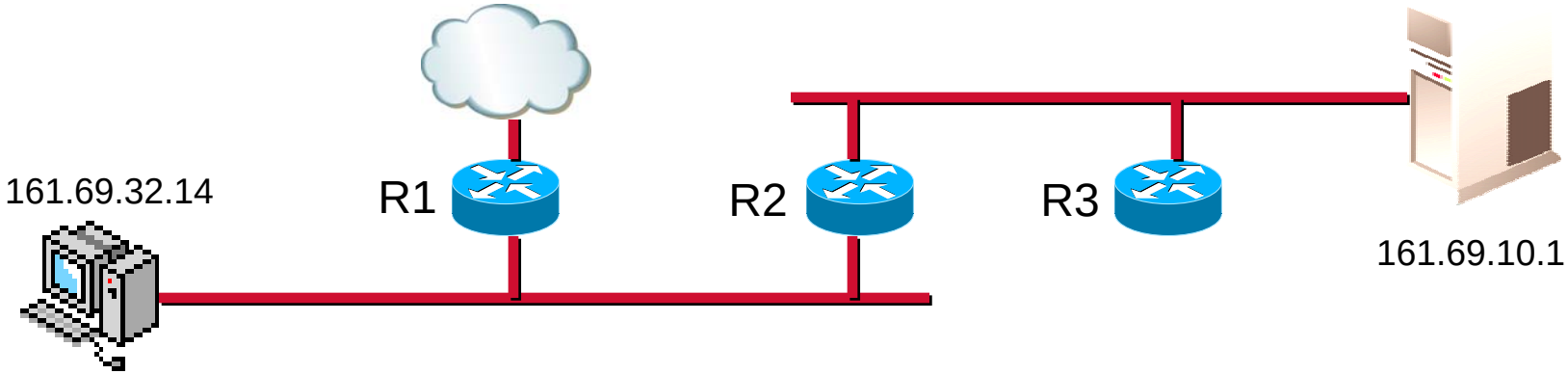


Redirect Message

Field Size (Bits)	Field Name	Field Description
8	Type	5
8	**Code**	**0 = Redirect Datagrams for the Network** **1 = Redirect Datagrams for the Host** **2 = Redirect Datagrams for the Type of service and the Network** **3 = Redirect Datagrams for the Type of service and the Host**
16	Checksum	16-Bits One's Complement of the Oned's Complement sum of the ICMP message
32	Gateway Internet Address	Address of the gateway to which traffic for the network specified on the internet destination network field of the original detagram should be sent
Variable	IP Header + first 64 bits of Datagram	Used by the host to match the message to the appropriate process

ThaiAdmin

Redirect Message



Client sends data to "Default" gateway

IP Packet, IP=161.69.10.1, DLC=R1-MAC

R1 – ICMP Redirect Message
Code=0, Gateway=R2

R1 sends redirect

R1 forwards the frame to R2

IP Packet, IP=161.69.10.1, DLC=R2-MAC

R2 forwards the frame to Server

IP Packet, IP=161.69.10.1, DLC=Server-MAC

Client updates table and sends data to R2

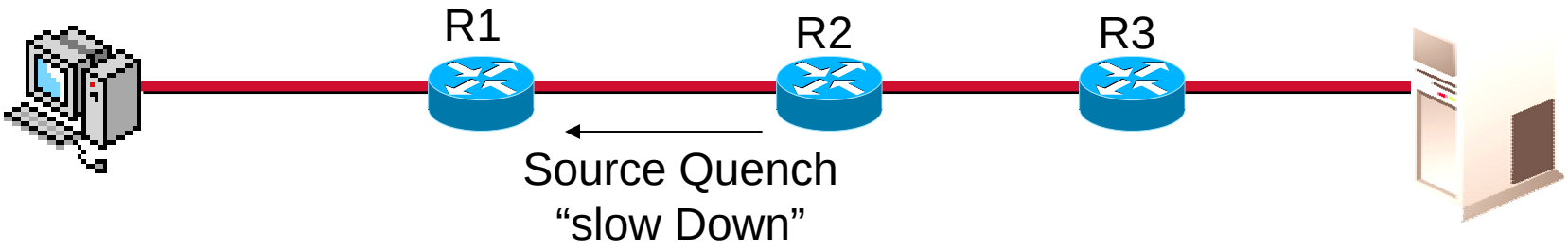
IP Packet, IP=161.69.10.1, DLC=R2-MAC

R2 forwards the frame to Server

IP Packet, IP=161.69.10.1, DLC=Server-MAC

Other ICMP Message

- 0 = Source Quench

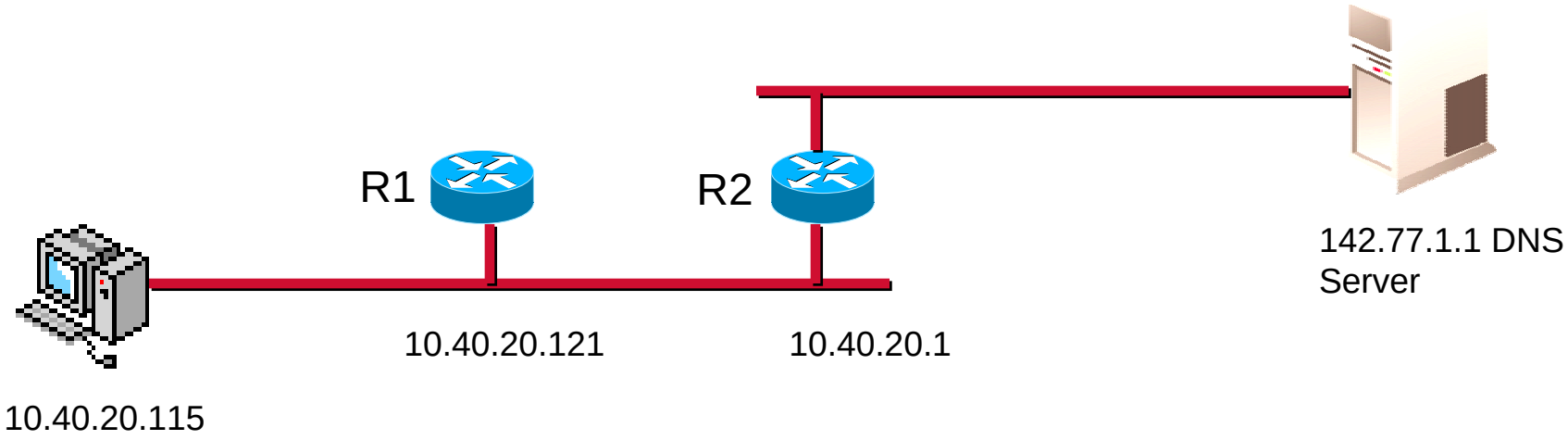


- Time stamps
  - 13 = Timestamp Request includes originating time
  - 14 = Timestamp Reply includes receive and transmit timer values
- Address masks
  - 17 = Address Mask request
  - 18 = Address mask Reply includes networks mask

ThaiAdmin

Demo Lab

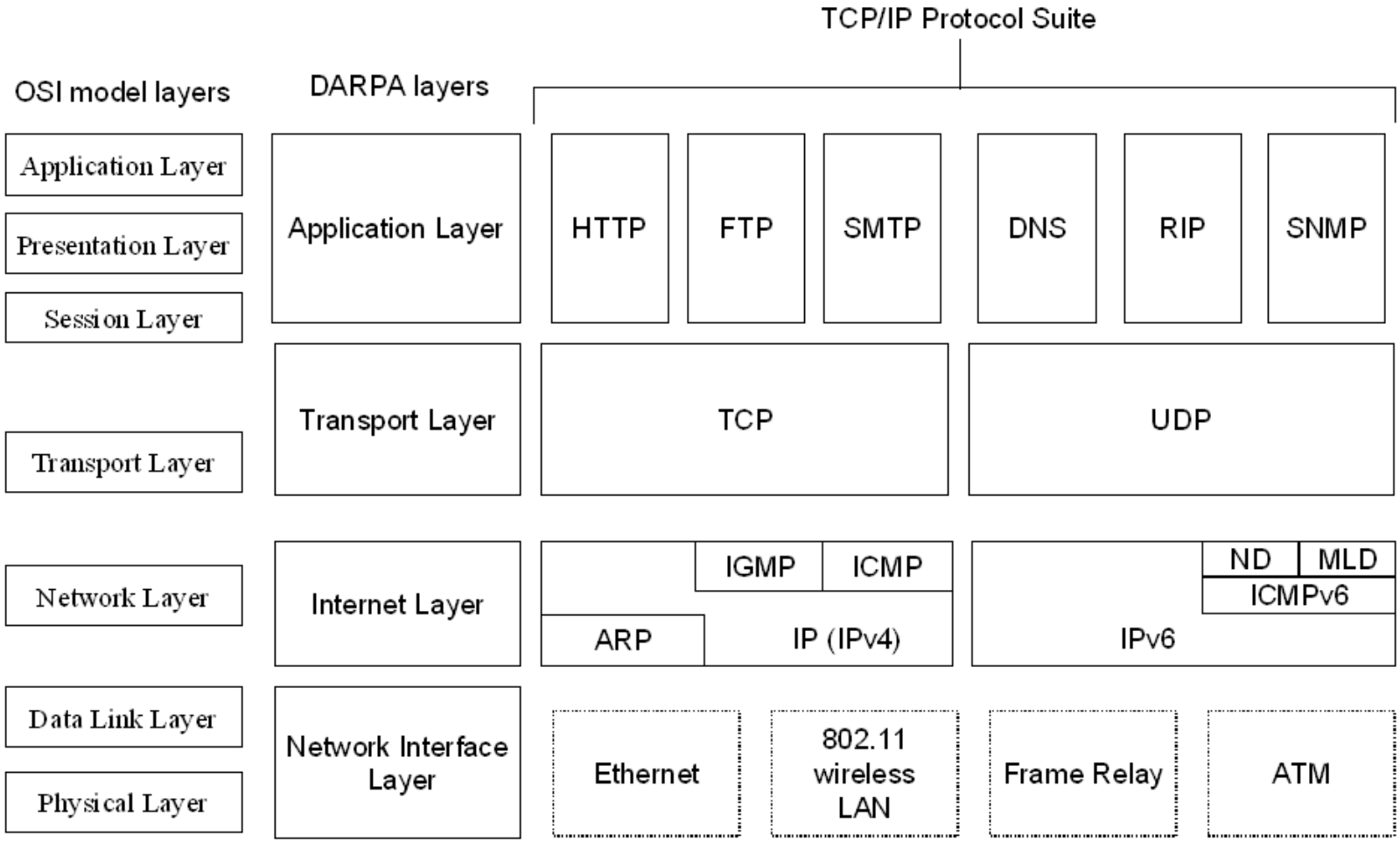
- ICMP Redirect



Detail Protocol: TCP

ThaiAdmin

Transmission Control Protocol (TCP)

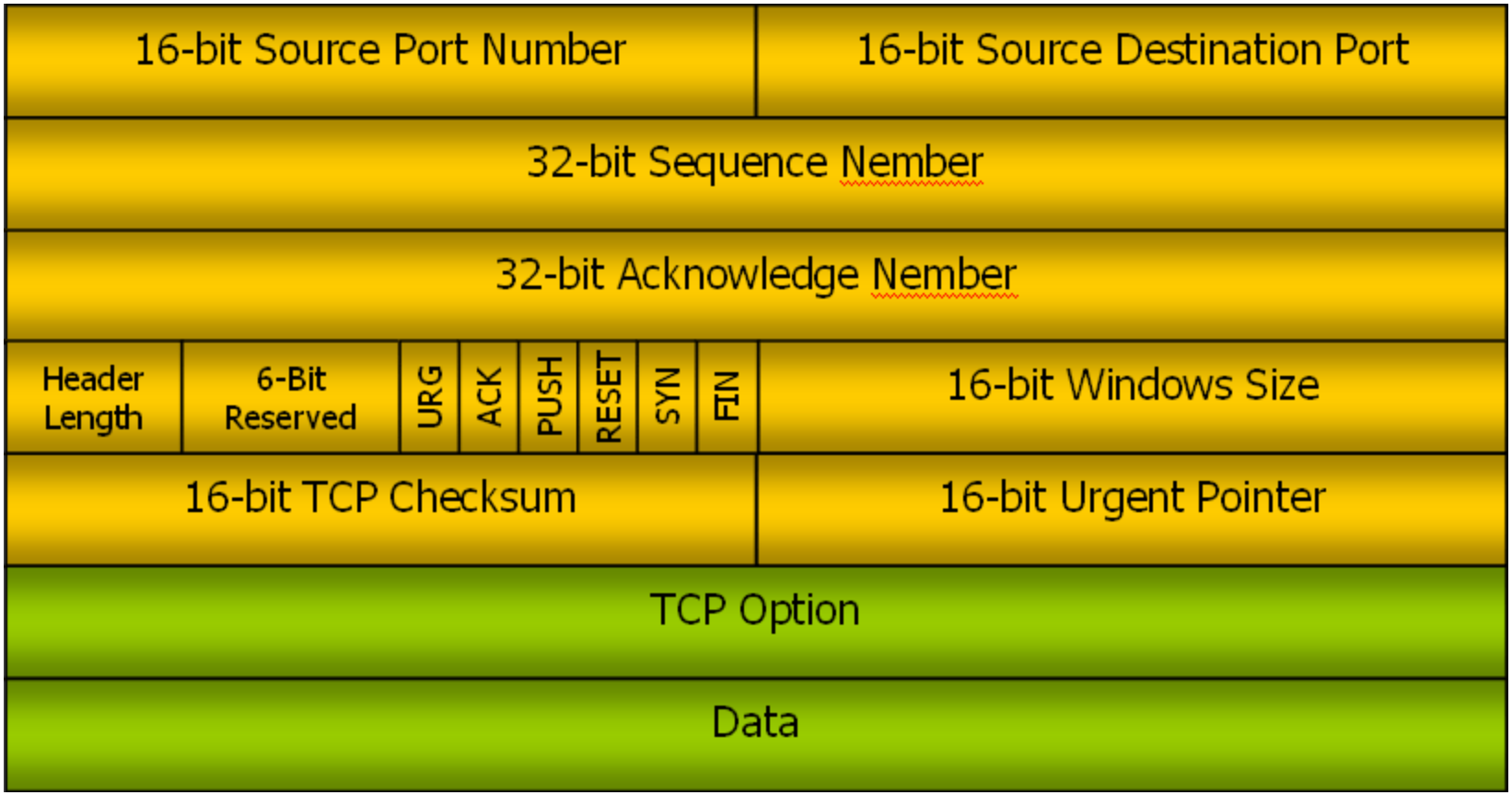


What Does TCP Do?

- Reliable Internetwork Packet Delivery
- Efficient Flow Control
- Multiplexing (Conversation and Connections)
- Error Control (Checksum)

ThaiAdmin

TCP Header



ThaiAdmin

TCP Fields

Bits	Name	Function
16	Source Port	An address identifying a process in the sending Host (ULP)
16	Destination Port	An address identifying a process in the destination host
32	SEQ Number	The number of the first octet of data in the segment being sent
32	ACK Number	The next sequence number the sender expects to receive
4	Data Offset	The number of 32 bit word in the TCP Header (5-15) The offset where the TCP data begins in the frame
6	Reserved	Reserved, must be 0

ThaiAdmin

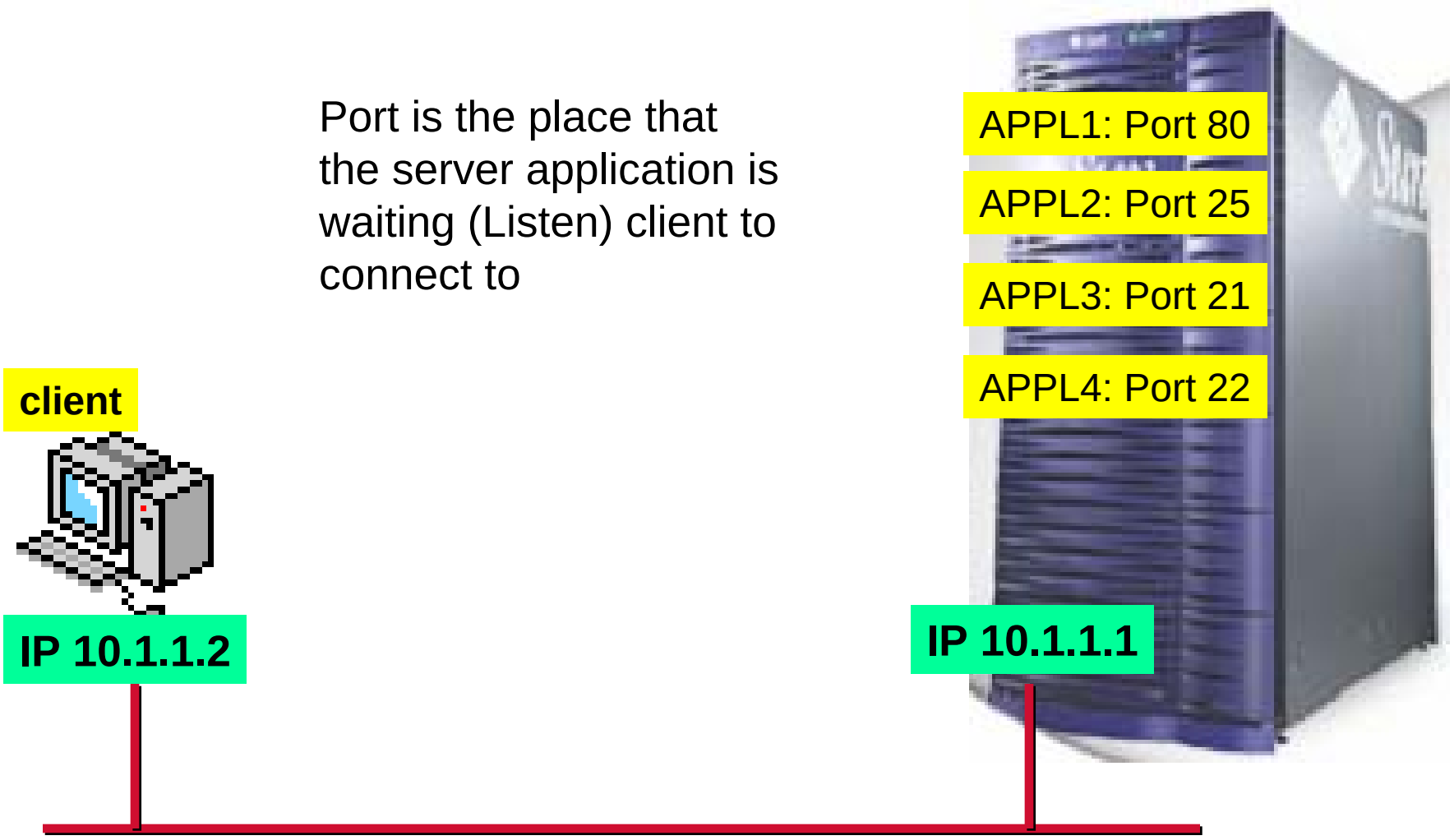
TCP Fields

	Bits	Name	Function
FLAGS	1	URG	Urgent Flag: There is information in the urgent field
	1	ACK	ACK Field is relevant: this is an acknowledgement frame
	1	PSH	Receiving TCP should immediately deliver segment to receiving ULP
	1	RST	Reset connection due to delayed duplicates, host crashes, etc
	1	SYN	Connection request
	1	FIN	Connection termination: sender won't transmit any more data
	16	Window	The number of bytes that the sender is willing to accept
	16	Checksum	16-Bits One's Complement of the One's Complement sum of all 16-bit words in the header, Pseudo header and text
	16	Urgent (Offset)	A position offset from the sequence number which points to the last byte of urgent data. Only interpreted when URG Flag set
	VAR	Options	Reserved for miscellaneous things, such as maximum segment size

ThaiAdmin

What is a Port?

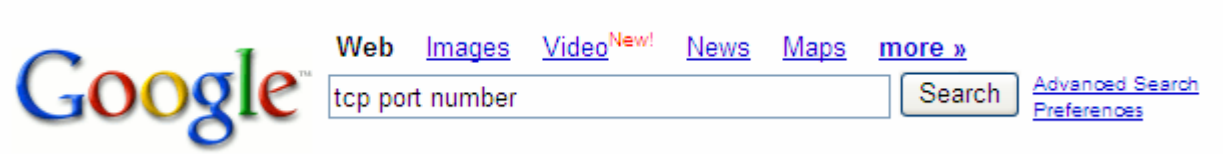
Port is the place that the server application is waiting (Listen) client to connect to



ThaiAdmin

Common UDP/TCP Port Number

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP



ThaiAdmin

Are Ports & Sockets the Same?

Port ≠ Sockets

- A **Port** is an address used by the Transport layer to talk to an application
- A **Socket** is the combination of the port number **and** IP address creating a unique address for an application in the network

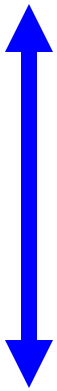
Source & Destination Port

- Most implementation:
  - Client will choose random port from internal pool as source port number
  - Destination has to be well known port number
- Example
  - User A send packet to Web server (port 80)
    - Step1: Client random choose source port from its internal pool (1024-65535). >> let get 54362 for example.
    - Step2: Client compose packet send to web server
      - Source IP: A's IP address
      - Source TCP port number is 54362
      - Destination IP: Web server's IP address
      - Destination TCP port number is 80 (well known port number)

What is a Connection?

Source Port Number

Source IP Address



Destination IP Address

Destination Port Number

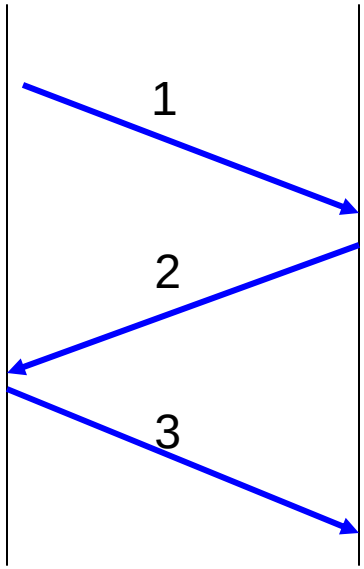
- Socket of one application is associated with the socket of another application process, creating a socket pair used to refer to the connection
- All data transfers are tracked through the socket pairing
- The socket paring is destroyed when a timeout expires after the connection is released

ThaiAdmin

Connection Establishment

The 3 Way Handshake

Send **SYN** (SEQ = X)
WIN = size
Max segment size = A



Receive SYN
Send **SYN** (SEQ=Y) / **ACK** (X+1)
Max segment Size = B

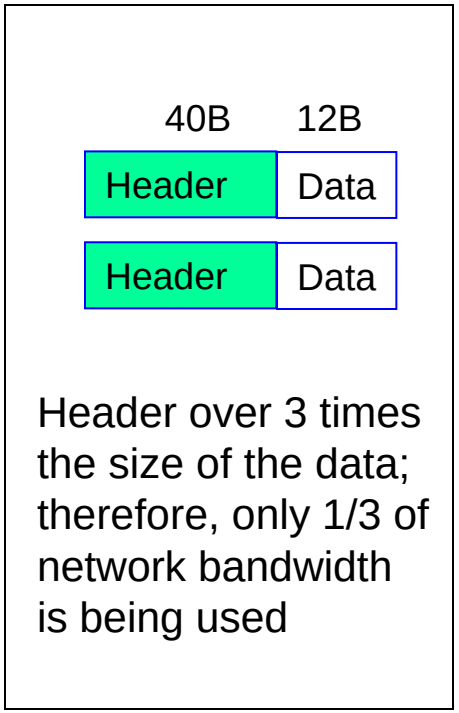
Receive SYN/ACK Segment
Send **ACK** (Y+1)

Receive **ACK** Segment

ThaiAdmin

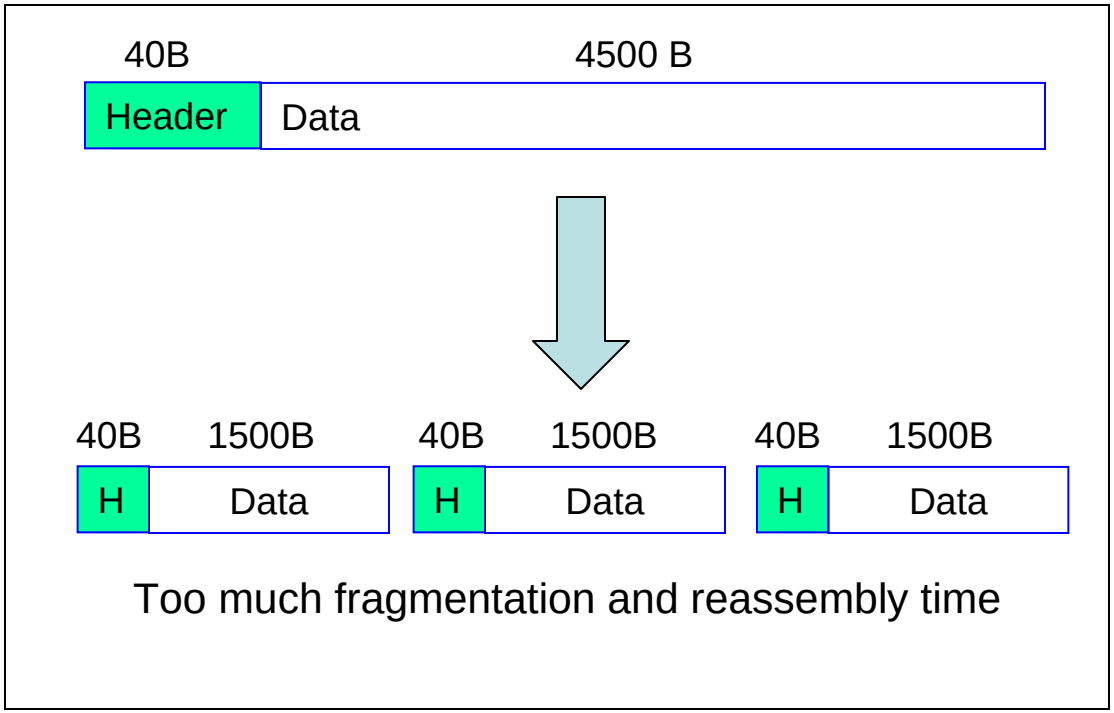
The Effect of Segment size on Performance

Small Segments



Header over 3 times the size of the data; therefore, only 1/3 of network bandwidth is being used

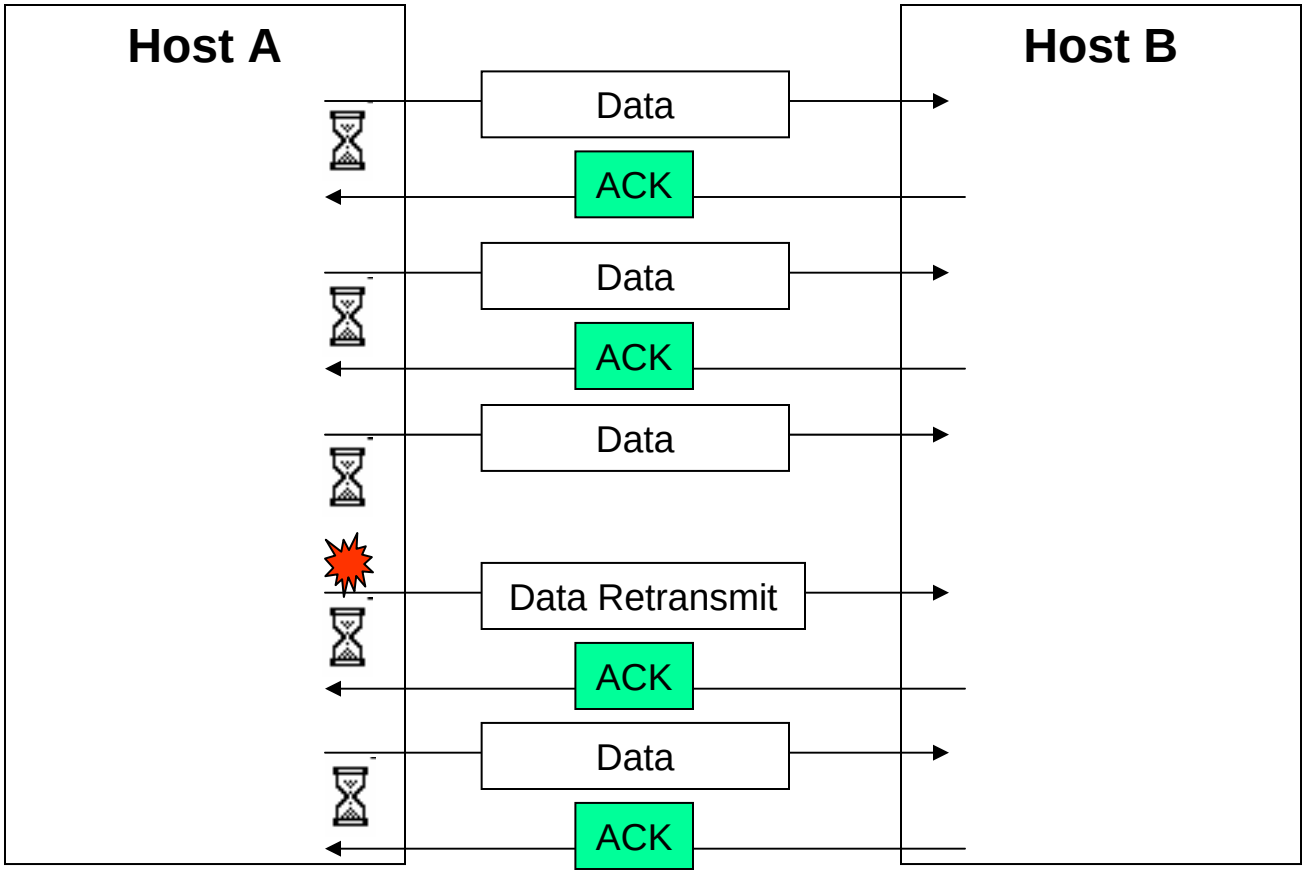
Large Segments



Too much fragmentation and reassembly time

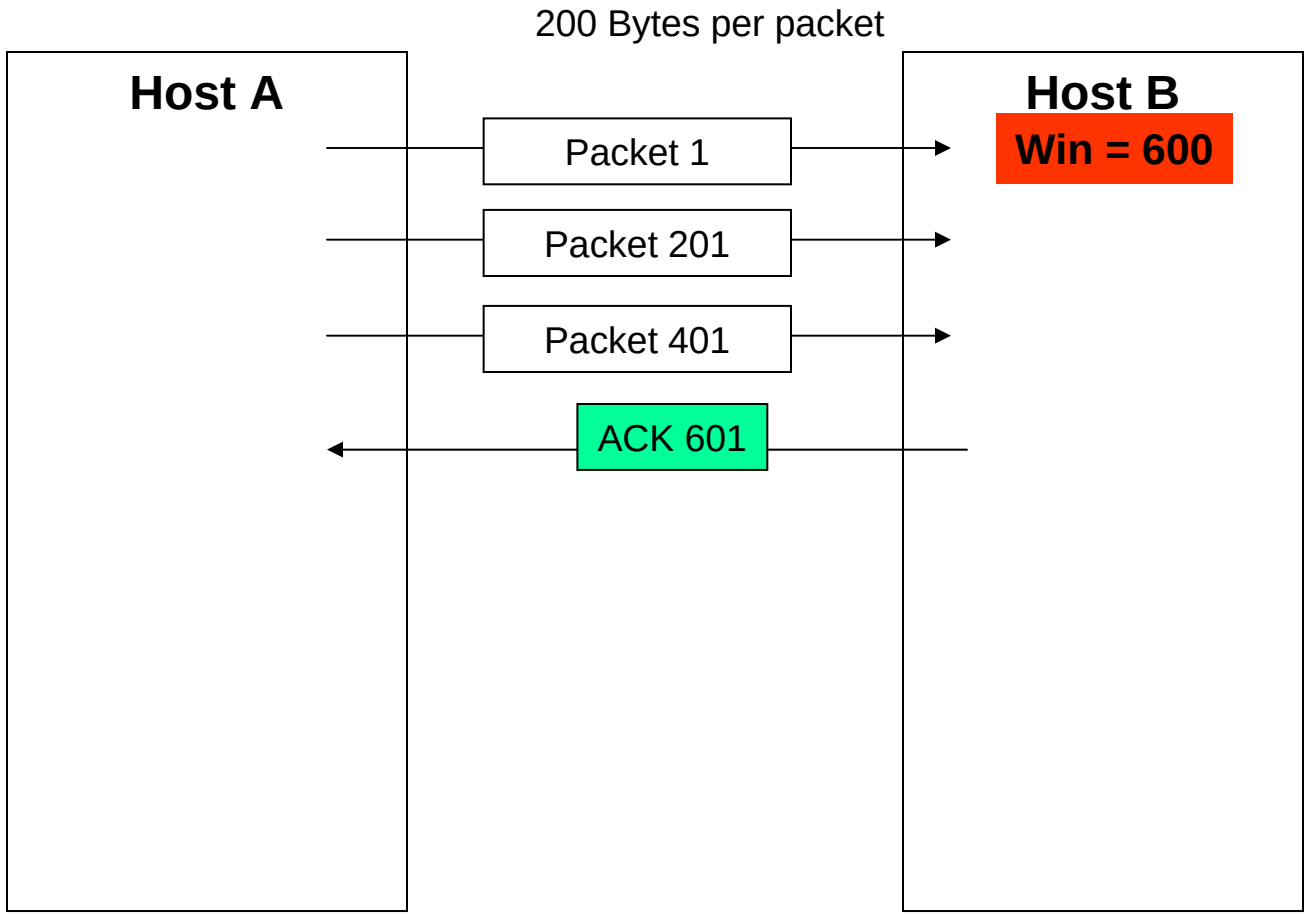
Reliable Delivery mechanisms

- Positive Acknowledge with Retransmission (PAR)



Reliable Delivery Mechanisms

- Sliding Window



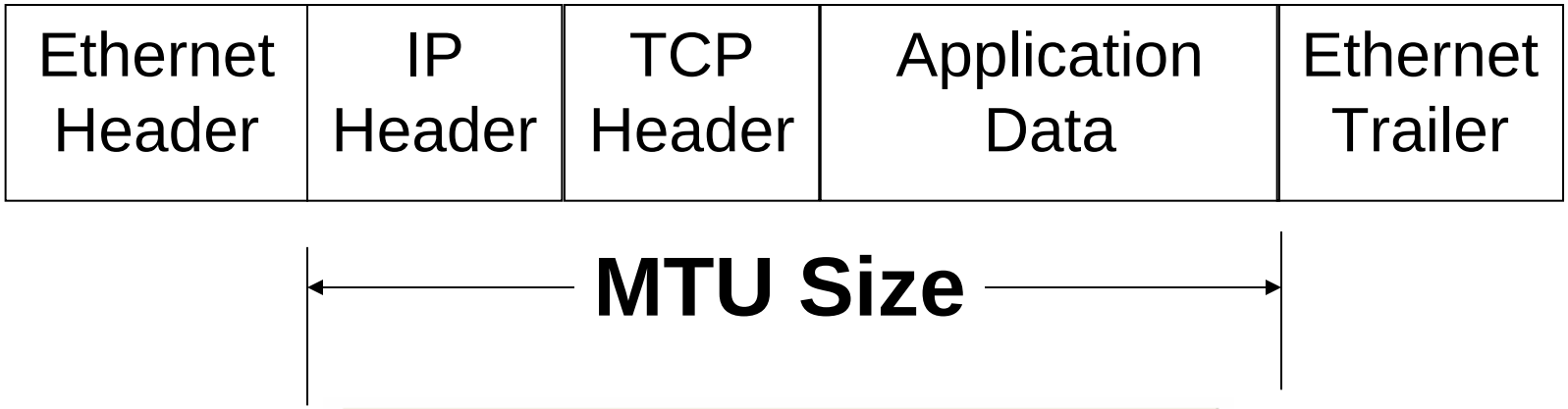
Efficient Flow Control
Sliding Window

- Simple PAR mechanisms waste bandwidth: Sender must receive ACK prior to sending more data
- Sliding window protocols allow multiple transmission without an ACK
- Sliding window provide flow control
- Each station has a send and receive window
  - The size of my send window is the size of your receive window
  - The window indicates the buffer space available for that application at that moment
  - Transmitted data is held in the buffer until the ACK is received
  - Only unacknowledged data is retransmitted

ThaiAdmin

MTU

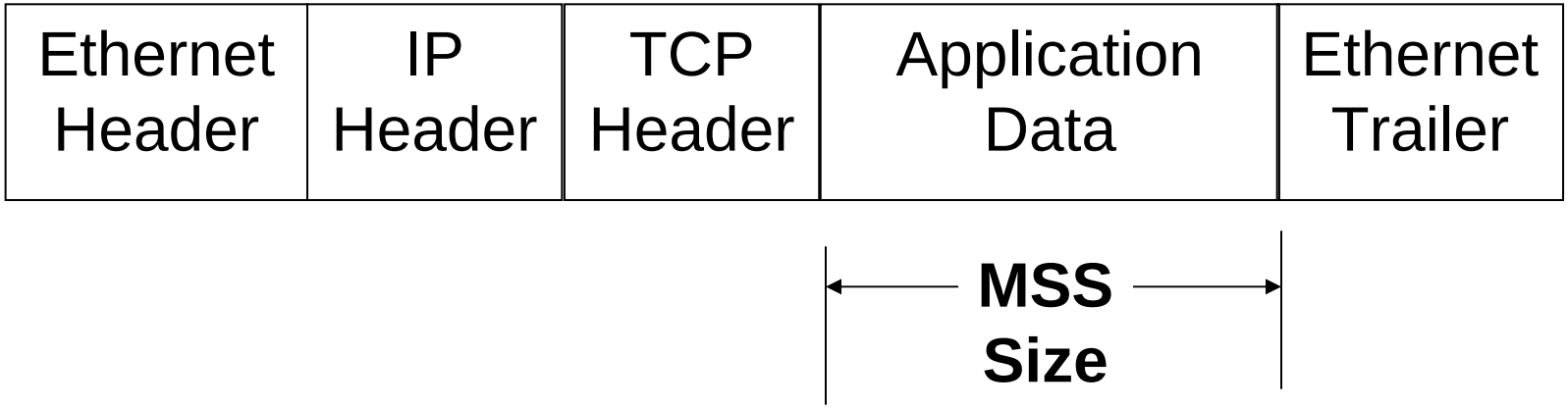
- MTU - Maximum Transfer Unit



Network	MTU (bytes)
Hyperchannel	65535
16 Mbits/sec token ring (IBM)	17914
4 Mbits/sec token ring (IEEE 802.5)	4464
FDDI	4352
Ethernet	1500
IEEE 802.3/802.2	1492
X.25	576
Point-to-Point (low delay)	296

MSS

- MSS – maximum segment Size is the largest "chunk" of data that TCP will send to the other end

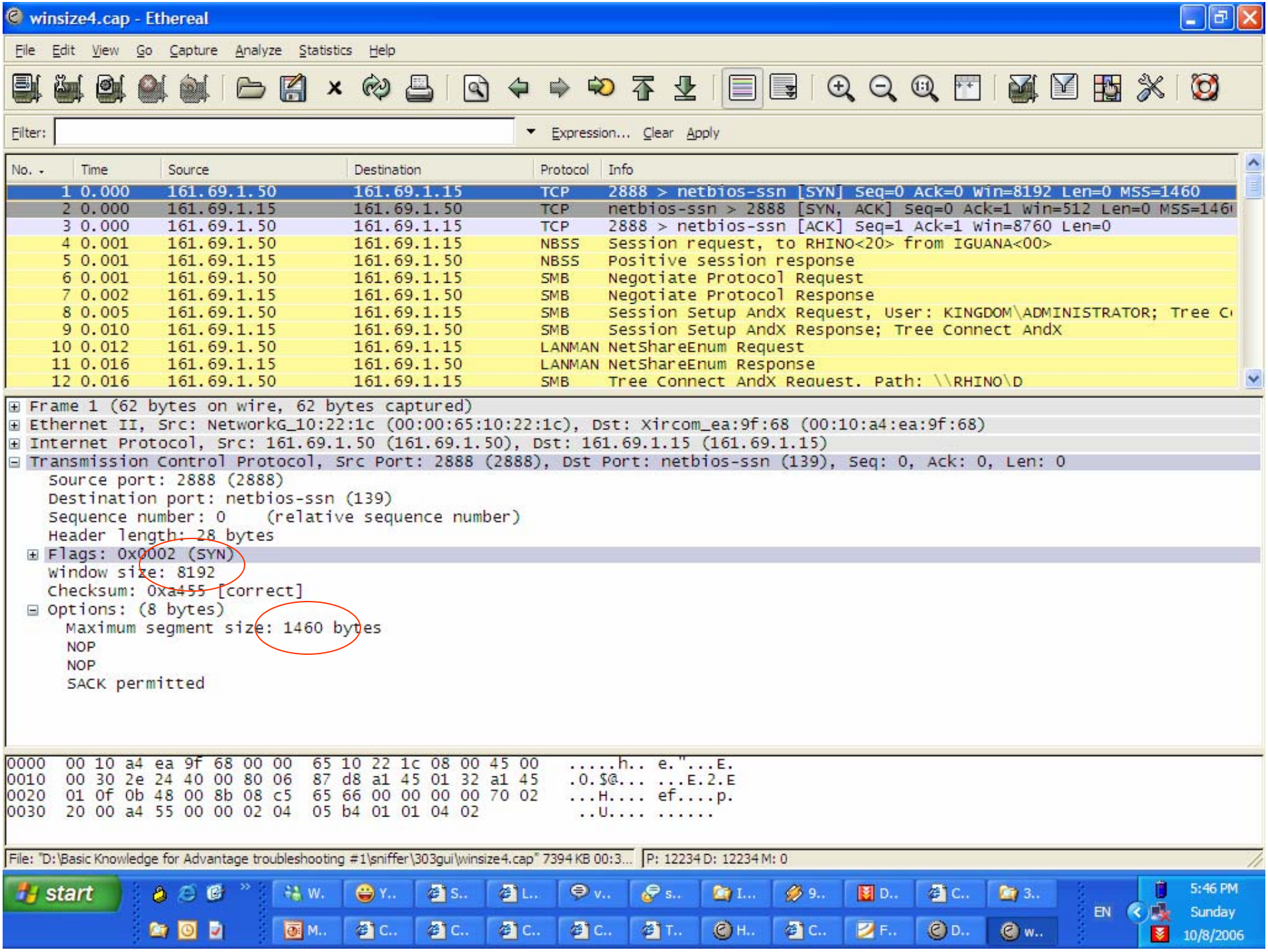


Ethernet:
MSS = MTU(1500) – IP header(20) – TCP header(20) = 1460

Note: Each OS can announce MSS with different value

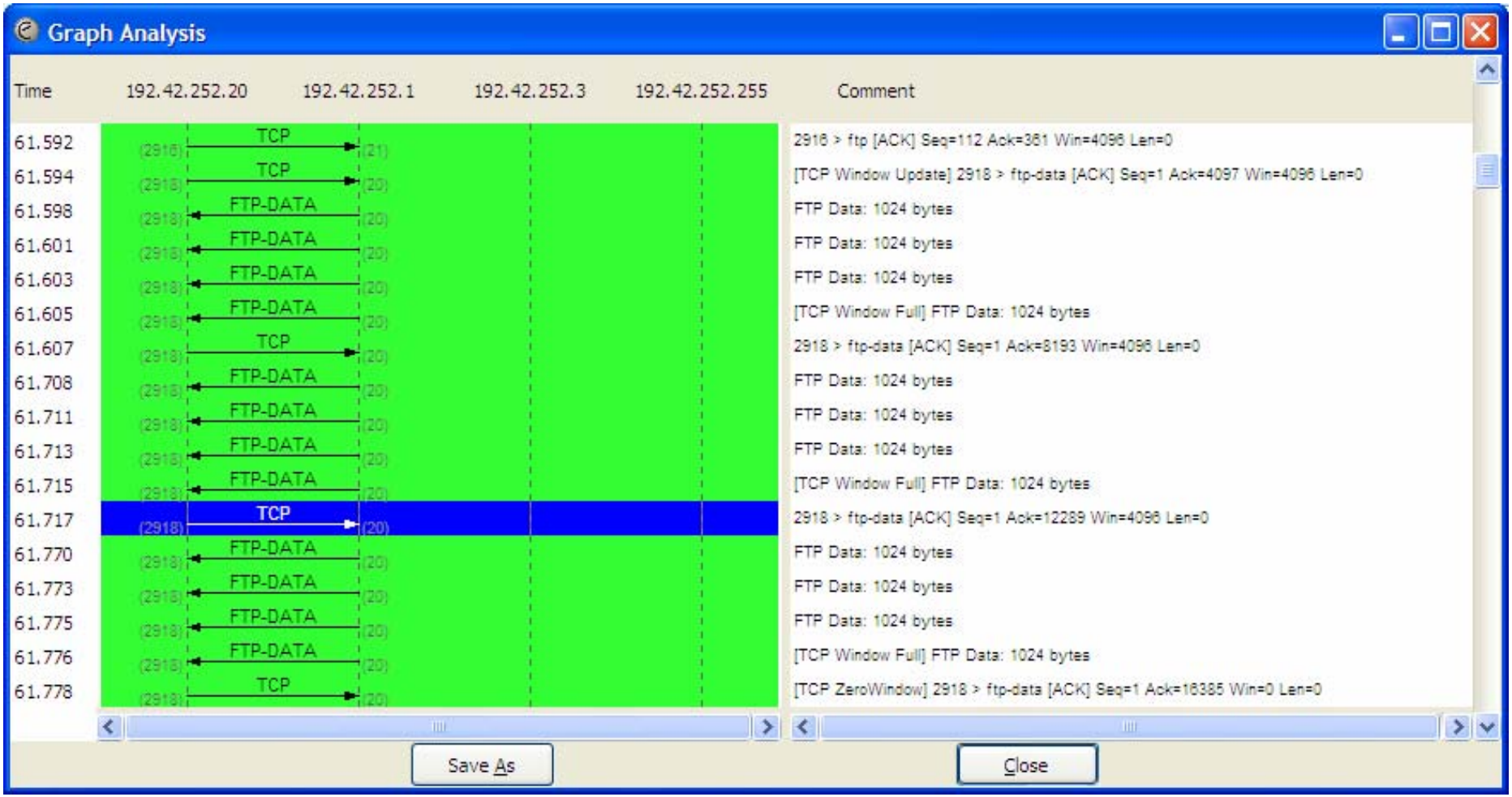
Window Size

- Window Size – is buffer size for packet receiving
- Receiver will announce it’s Windows size (Buffer size) to the sender
- Sender can send data up to window size which announced by Receiver
- Sender has to wait until Receiver clear buffer and announce window size again then it can continue send data

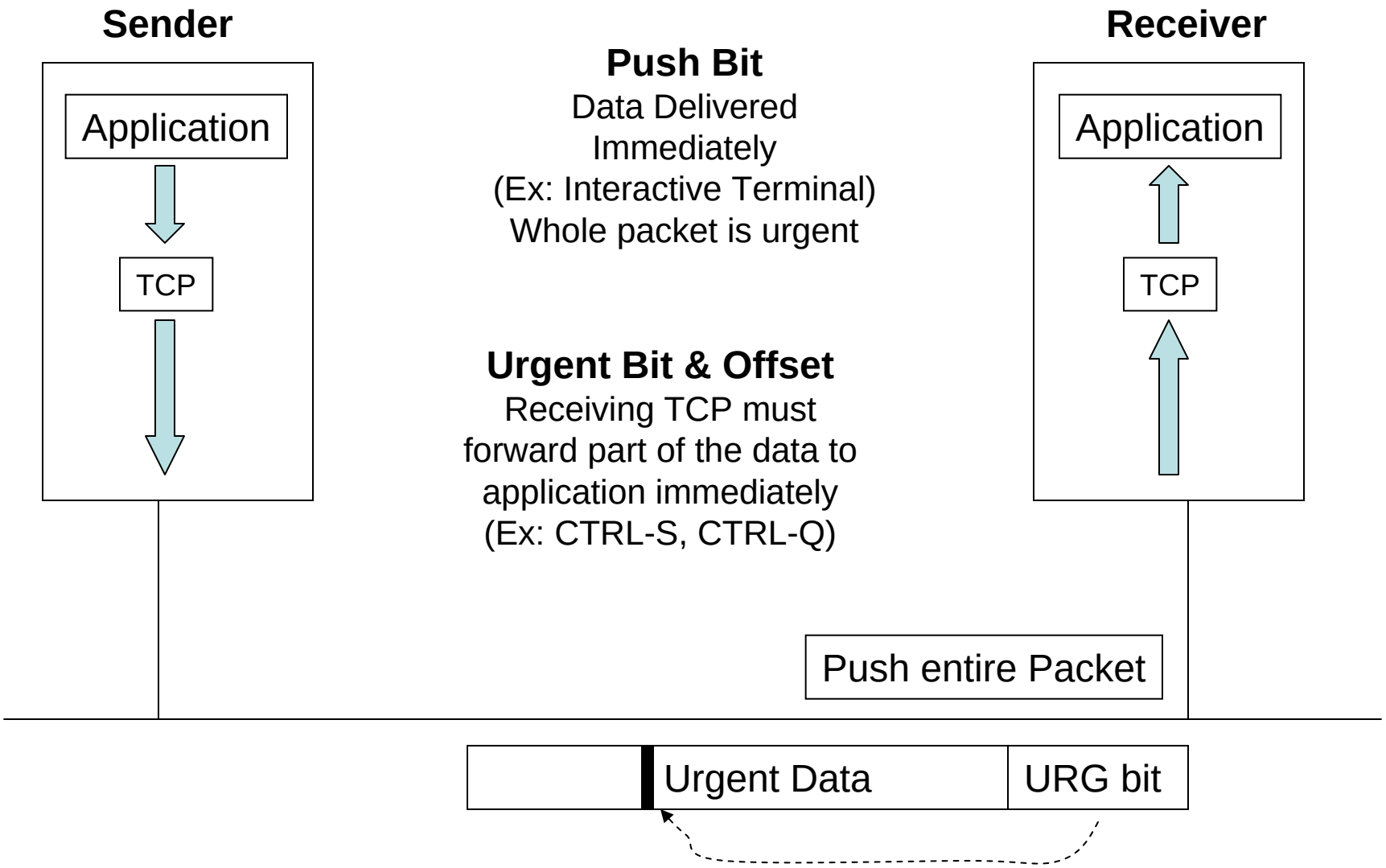

winsize4.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000 161.69.1.50 161.69.1.15 TCP 2888 > netbios-ssn [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460
2 0.000 161.69.1.15 161.69.1.50 TCP netbios-ssn > 2888 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0 MSS=146
3 0.000 161.69.1.50 161.69.1.15 TCP 2888 > netbios-ssn [ACK] Seq=1 Ack=1 Win=8760 Len=0
4 0.001 161.69.1.50 161.69.1.15 NBSS Session request, to RHINO<20> from IGUANA<00>
5 0.001 161.69.1.15 161.69.1.50 NBSS Positive session response
6 0.001 161.69.1.50 161.69.1.15 SMB Negotiate Protocol Request
7 0.002 161.69.1.15 161.69.1.50 SMB Negotiate Protocol Response
8 0.005 161.69.1.50 161.69.1.15 SMB Session Setup AndX Request, User: KINGDOM\ADMINISTRATOR; Tree C
9 0.010 161.69.1.15 161.69.1.50 SMB Session Setup AndX Response; Tree Connect AndX
10 0.012 161.69.1.50 161.69.1.15 LANMAN NetShareEnum Request
11 0.016 161.69.1.15 161.69.1.50 LANMAN NetShareEnum Response
12 0.016 161.69.1.50 161.69.1.15 SMB Tree Connect AndX Request, Path: \\RHINO\D
Frame 1 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: NetworkG_10:22:1c (00:00:65:10:22:1c), Dst: Xircom_ea:9f:68 (00:10:a4:ea:9f:68)
Internet Protocol, Src: 161.69.1.50 (161.69.1.50), Dst: 161.69.1.15 (161.69.1.15)
Transmission Control Protocol, Src Port: 2888 (2888), Dst Port: netbios-ssn (139), Seq: 0, Ack: 0, Len: 0
Source port: 2888 (2888)
Destination port: netbios-ssn (139)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x0002 (SYN)
Window size: 8192
Checksum: 0xa455 [correct]
Options: (8 bytes)
Maximum segment size: 1460 bytes
NOP
NOP
SACK permitted
0000 00 10 a4 ea 9f 68 00 00 65 10 22 1c 08 00 45 00 .....h.. e."...E.
0010 00 30 2e 24 40 00 80 06 87 d8 a1 45 01 32 a1 45 .0.$@... ...E.2.E
0020 01 0f 0b 48 00 8b 08 c5 65 66 00 00 00 00 70 02 ...H.... ef....p.
0030 20 00 a4 55 00 00 02 04 05 b4 01 01 04 02 ..U.... ......
File: "D:\Basic Knowledge for Advantage troubleshooting #1\sniffer\303gui\winsize4.cap" 7394 KB 00:3...
P: 12234 D: 12234 M: 0
start
EN
5:46 PM
Sunday
10/8/2006

ThaiAdmin

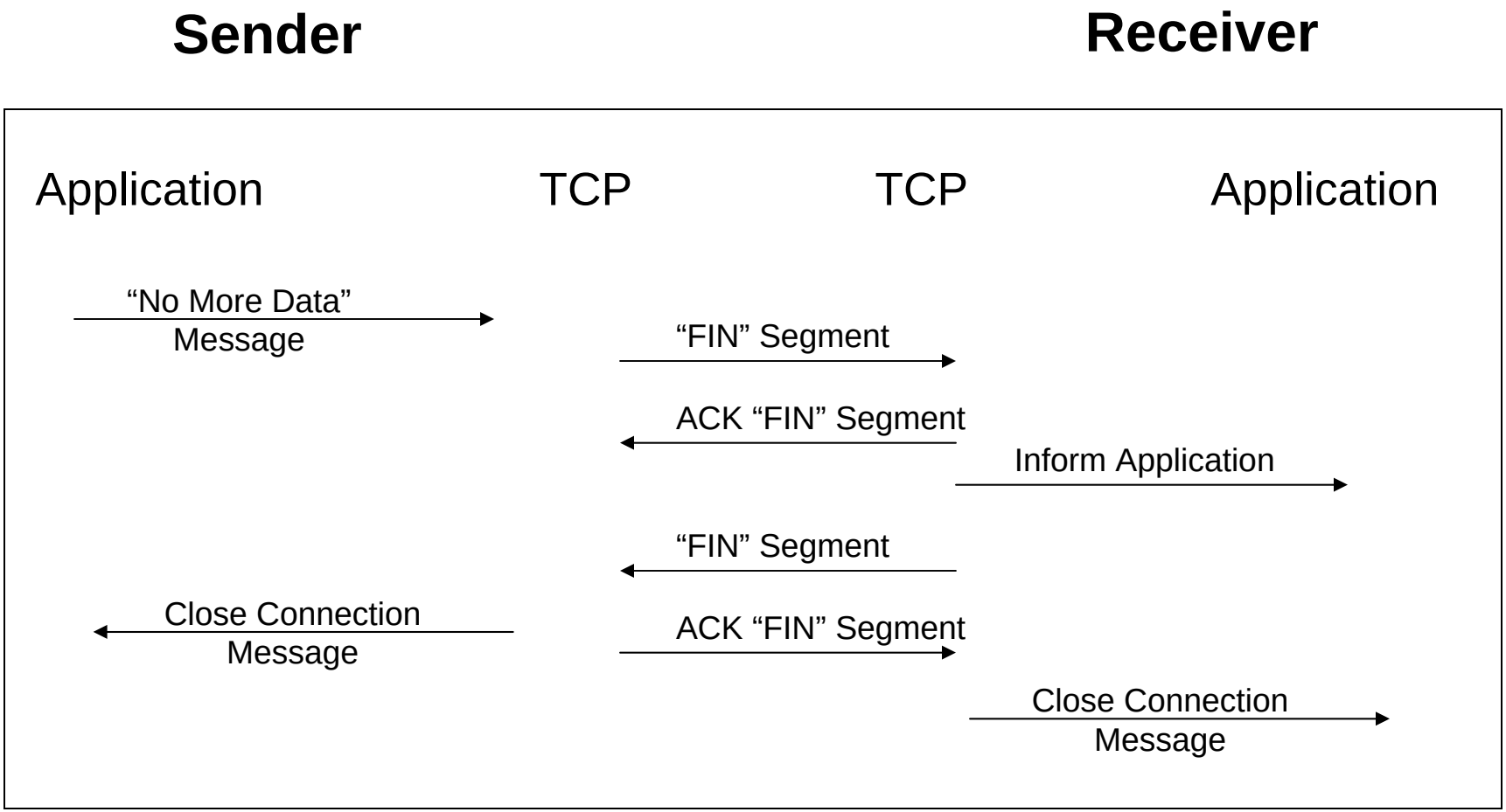
Example – Sliding Window



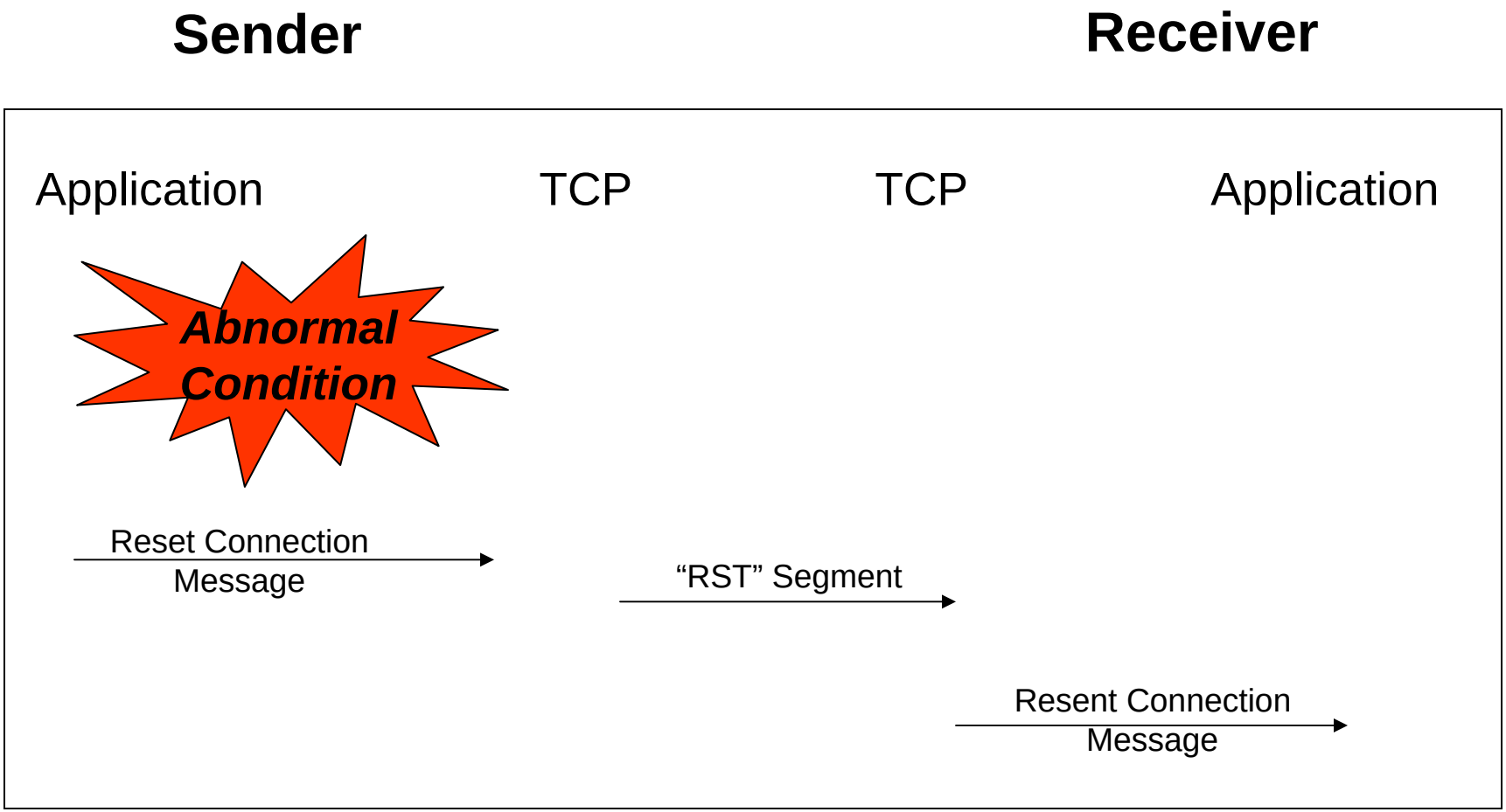
When data must be delivered right away



Closing TCP Connections



Resetting a TCP Connection



Demo Lab

- Sliding window