

## Lab#4: Traffic Analysis II

ดร. อนันต์ พลเพิ่ม

Anan Phonphoem, Ph.D.

[anan@cpe.ku.ac.th](mailto:anan@cpe.ku.ac.th)

<http://www.cpe.ku.ac.th/~anan>

Computer Engineering Department  
Kasetsart University, Bangkok, Thailand

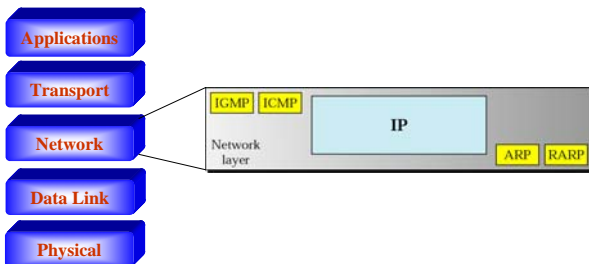
1

## Agenda

- ARP
- ICMP
- FTP
- Http

2

## Network Layer



3

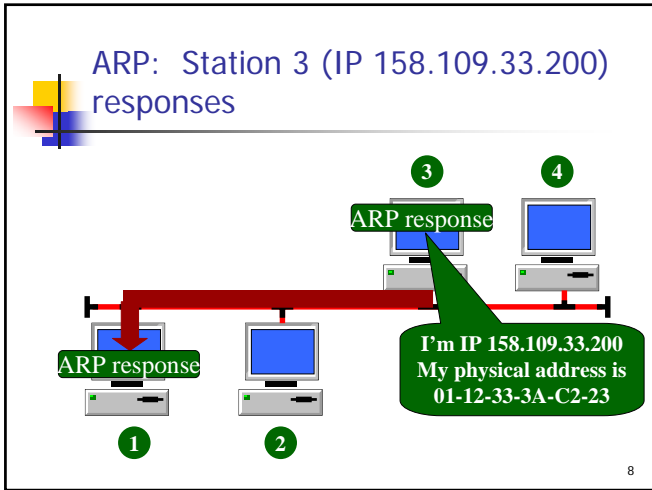
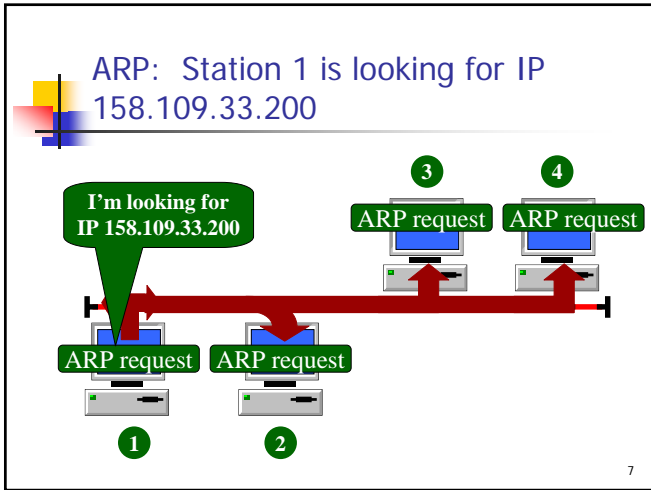
## ARP: Address Resolution Protocol

## IP and MAC address

- Stations need to know MAC address to communicate
- Hardware MAC address
  - Ethernet 6 bytes
  - Token ring 2 or 6 bytes
  - FDDI 2 or 6 bytes
- How does IP Address get mapped to MAC address?
  - manual configuration by hand is tedious
  - automatic process by ARP

## ARP protocol

- RFC 826 - Address Resolution Protocol
- ARP maps any network level address (such as IP) to its corresponding data link address (such as Ethernet)
- supported protocol in datalink layers, not data link layer protocol



### ARP as a command line

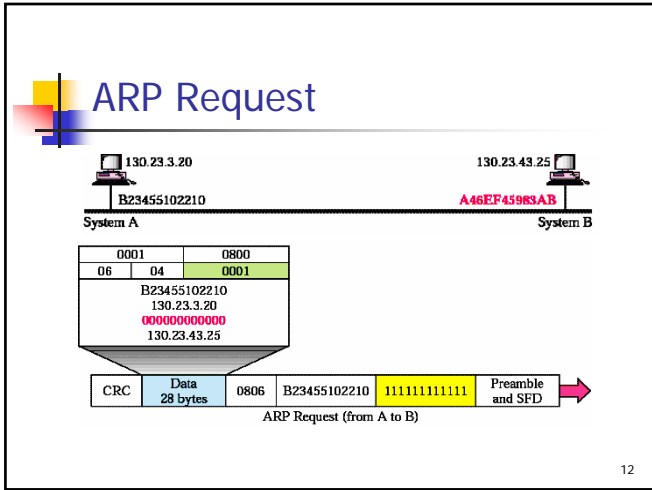
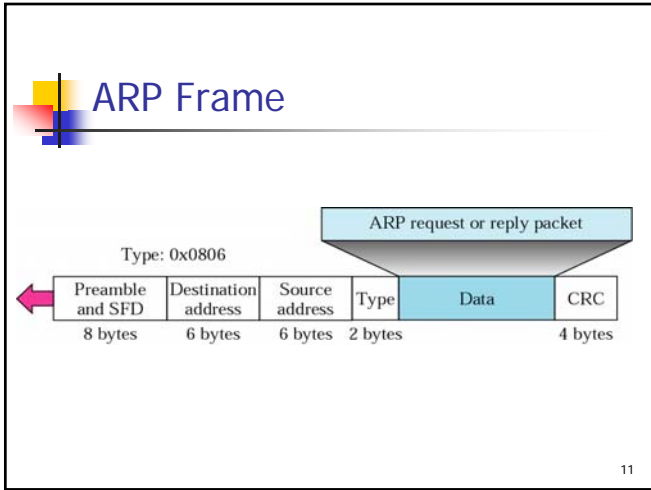
```

% arp -a
www.cpe.ku.ac.th (158.108.33.5) at 0:0:e8:15:cc:c
% telnet cc
:
% arp -a
router.cpe.ku.ac.th (158.108.33.1) at 0:0:c:6:13:4a
cc.cpe.ku.ac.th (158.108.33.2) at 2:60:8c:2e:b5:8b
www.cpe.ku.ac.th (158.108.33.5) at 0:0:e8:15:cc:c
  
```

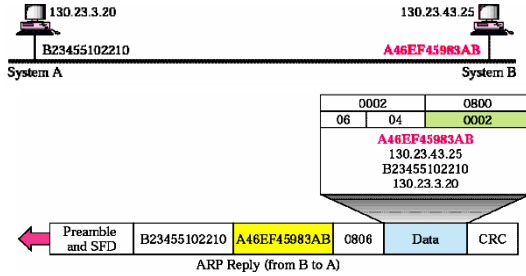
entry in ARP table

more entries added

- ### ARP mechanisms
- Each node maintains the ARP cache
    - it first looks in the cache to find entry first
    - if the entry is not used for a period (~15 minutes), it is deleted.
  - Receive node can add a MAC address entry for source station in its own cache.
  - ARP traffic load
    - hosts quickly add cache entries.
    - If all hosts on a subnet are booted at the same time? => flurry of ARP requests and reply.



## ARP Reply



13

## ICMP

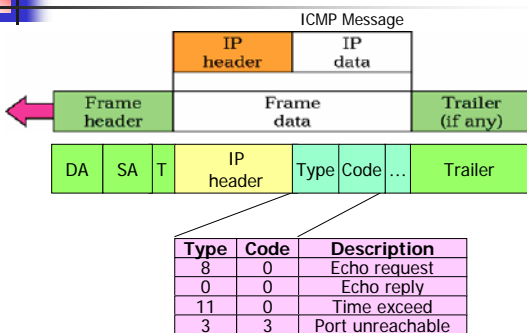
## ICMP

- No Flow and error control for IP
- Error Reporting to help IP Layer
- Function of ICMP
  - a node recognizing a transmission problem.(ttl exceed, destination unreachable, etc.) generates ICMP messages
  - ICMP provides some useful diagnostics about network operation (ping, traceroute)

## ICMP

- ICMP error messages never generates due to:
  - ICMP error messages selves
  - Broadcast/Multicast
  - This to prevent broadcast Storms
- What are Broadcast Storms
  - a large number of broadcast datalink frames transmitted nearly simultaneous from several hosts
  - LAN may have been brought to a standstill

## ICMP Encapsulation



17

## ping - ICMP echo request/reply

- ping sends an ICMP echo request to a remote host, which then return an ICMP echo reply to the sender
- All TCP/IP node is supposed to implement ICMP and respond to ICMP echo



## ping command

- Send an echo request message every seconds and records the time it takes for each reply
  - every echo request contains a unique sequence number to match replies and request
  - Record round-trip timing
  - Show packet lost statistics

## ping example

```
% ping -s nontri.ku.ac.th
PING nontri.ku.ac.th: 56 data bytes
64 bytes from nontri.ku.ac.th (158.108.2.71): icmp_seq=0. time=3. ms
64 bytes from nontri.ku.ac.th (158.108.2.71): icmp_seq=1. time=2. ms
64 bytes from nontri.ku.ac.th (158.108.2.71): icmp_seq=2. time=3. ms
64 bytes from nontri.ku.ac.th (158.108.2.71): icmp_seq=3. time=2. ms
^C
----nontri.ku.ac.th PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/3
```

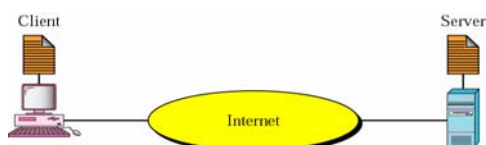
## ping as debugging tools

- What do we get from ping?
  - Timing information
  - Connection reliability
  - Destination is reachable (routable)
  - Layer is functional, but not guaranteed telnet!

## ping results

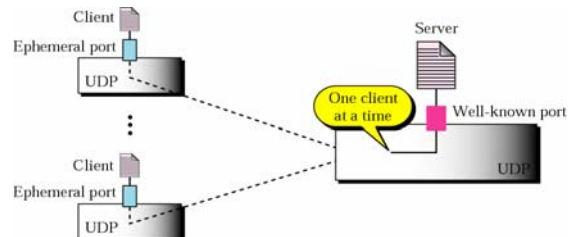
- no response
  - no end node, no connection
- lost packet (significant when >2-3%)
  - transmission error on WAN/LAN, overloading bridges/routers
- time acknowledge vary
  - host/network overloading, >100 ms make telnet less acceptable)
- no lost and echo time is reasonably constant
  - Congratulation! That's all we want.

## Client Server



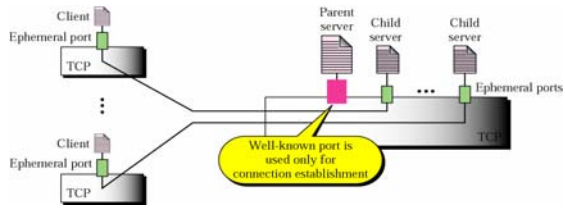
23

## Connectionless iterative server



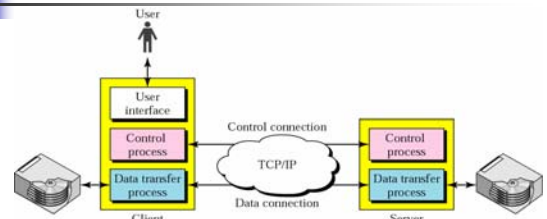
24

## Connection-oriented concurrent server



25

## FTP



26

## Sample software for Client-Server

- FTP
  - Server (wftpd)
  - Client (wsftp light, Cute Ftp)
- HTTP
  - Server (Web Active, Apache)
  - Client (IE5, Netscape, MediaPlayer)

27