The Address Resolution Protocol (ARP)

Internet Protocols

CSC / ECE 573

Fall, 2005

N. C. State University

Today's Lecture

I. ARP: Mapping IP (logical) Addresses to Link Layer (MAC, hardware) Addresses

II. RARP: Mapping Link Layer Addresses to IP Addresses

copyright 2005 Douglas S. Reeves

ARP

The Address Resolution Problem

- Applications specify destinations by IP address (or DNS name that gets translated into IP address)
- IP packets are sent over links that only recognize MAC addresses

⇒ How map IP address to Ethernet address?

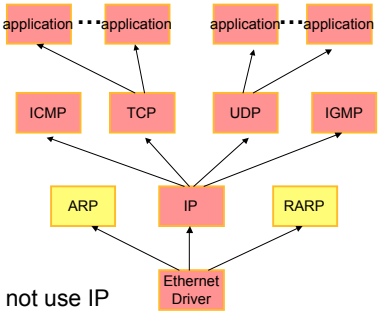
copyright 2005 Douglas S. Reeves

An Analogy

- Phone call to <Employee@Company> must be translated into <extension #> for connection
  - what's the best way to do this? what factors should be considered?

copyright 2005 Douglas S. Reeves

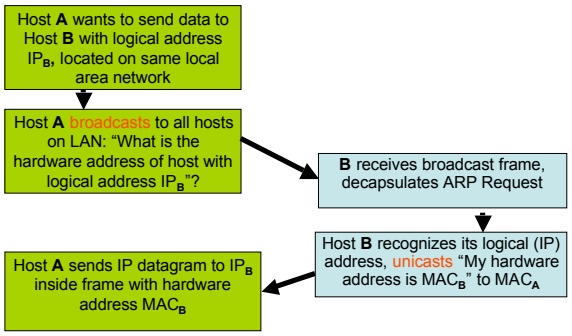
What Layer is ARP?



- Does not use IP

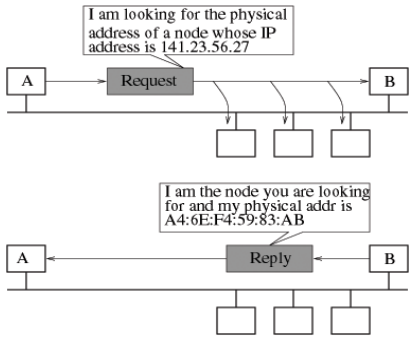
copyright 2005 Douglas S. Reeves

Solution: Dynamic Binding (RFC 826)



copyright 2005 Douglas S. Reeves

ARP in a Picture



copyright 2005 Douglas S. Reeves

ARP PDU Format

- Two message Types (ARP Request and ARP Reply), with same format (28 bytes)

Hardware Type (e.g. Ethernet)

Protocol Type (e.g. IPv4)

Length of Physical (MAC) Address (e.g., Ethernet=6)

Length of Logical Address (e.g. IPv4=4)

Operation Type (e.g. Request, Reply)

Sender Physical Address (MAC)

Sender Logical Address (IP)

Target Physical Address (MAC)

Target Logical Address (IP)

copyright 2005 Douglas S. Reeves

Details

Host A **ARP Request**

Broadcast to everybody on the LAN

SenderMAC = MAC_A
SenderIP = IP_A
TargetMAC = ???
TargetIP = IP_B

Host B **ARP Reply**

SenderMAC = MAC_B
SenderIP = IP_B
TargetMAC = MAC_A
TargetIP = IP_A

Unicast just to A

- Q: Is Target MAC ever useful?

copyright 2005 Douglas S. Reeves

Possible Outcome?

- What if two hosts claim same IP address, but reply with different hardware addresses?
  - could this be legit?

copyright 2005 Douglas S. Reeves

ARP Cache

- Wish to avoid sending an ARP Request for every data packet
- Solution: cache address mapping for reuse
  - A caches the ARP Reply (MAC_B, IP_B) mapping
  - All hosts on LAN cache ARP Request (MAC_A, IP_A) mapping

copyright 2005 Douglas S. Reeves

ARP Cache

- Problems with caching
  - cache space may be limited
  - hosts move or change IP addresses
  - what problems does this cause?
- Solution: drop (invalidate) cache entries after "a while" (20 minutes is normal)

copyright 2005 Douglas S. Reeves

"Gratuitous" ARP

- Every machine (should) broadcast its IP→ hardware address mapping when it boots up
- Ex.: A sends ARP Request with its own IP address as the target IP address
  - SenderMAC = MAC_A, SenderIP = IP_A
  - TargetMAC = ???, TargetIP = IP_A
- Will there be a Reply, and if so, what does it mean?

copyright 2005 Douglas S. Reeves

What Happens When Sending a Datagram

1. Determine how this datagram should be forwarded towards the destination
   - the "first-hop" receiver X is either a) the final destination, or b) the next router on the path to the destination
   - in both cases, the first-hop receiver is "directly connected" to the sender
2. **If** A already has an ARP cache entry for X…
   - send IP datagram in a link-layer frame to X

copyright 2005 Douglas S. Reeves

Sending a Datagram (cont'd)

3. **Else if** A has not already sent an ARP Request for X's hardware address…
   - send an ARP Request
   - store the datagram for later transmission
   - wait for an ARP Reply
4. **Else** … */* ARP Request for X has already been sent, but ARP Reply has not been received */*
   - store the datagram for later transmission
   - wait for an ARP Reply

copyright 2005 Douglas S. Reeves

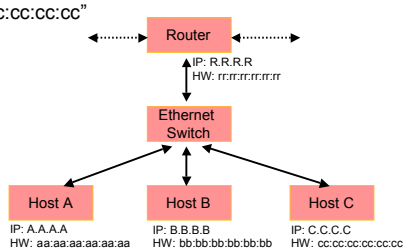
Sending a Datagram (cont'd)

5. When ARP Reply is received from X…
   - update the cache
   - send out all the queued packets for X
- What if you never get an ARP Reply?
  - how long is "never"?
  - any harm?

copyright 2005 Douglas S. Reeves

ARP *Spoofing*

- A host may "lie" about IP→ hardware addr. mapping
  - A sends ARP Request: "Who has B.B.B.B"?
  - C replies "B.B.B.B's hardware address is cc:cc:cc:cc:cc:cc"



copyright 2005 Douglas S. Reeves

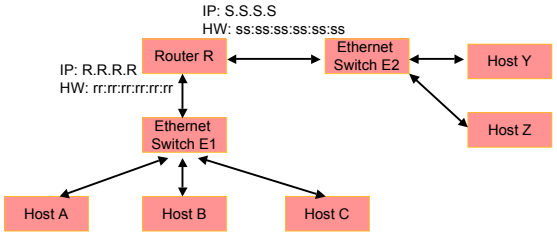
Questions about Spoofing

- What are the possible results?
- Won't B notice that C is claiming its IP address?
- What can B do about it?
- Will C know if B asserts its own mapping for B.B.B.B to other hosts?
  - what should C do?
  - who "wins"?
- Ways to prevent spoofing?

copyright 2005 Douglas S. Reeves

Proxy Arp

- Example: bridging two Ethernets at the IP layer



- Can we make A, B, C, Y, and Z think they are all on the same Ethernet segment?

copyright 2005 Douglas S. Reeves

Proxy Arp (cont'd)

- Solution
  - R intercepts ARP Requests from Y for B's hardware address, and replies with its own hardware address (ss:ss:ss:ss:ss:ss)
  - Y will sends data for B.B.B.B to R
  - R substitutes rr:rr:rr:rr:rr:rr for Source Hardware Address in link layer frame, forwards to B
- Sometimes it's good to lie ☺

copyright 2005 Douglas S. Reeves

RARP (REVERSE ARP)

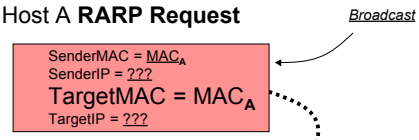
RARP (RFC 903)

- One or more RARP servers store IP addresses for hosts on their network
- A client host can request its IP address from the server(s), using its own hardware address
- RARP Request is broadcast on the LAN
- RARP uses the same message format as ARP, except for the Operation Field

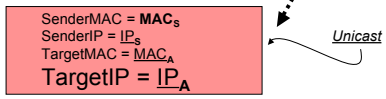
copyright 2005 Douglas S. Reeves

Example

- Host A **RARP Request**



- RARP Server S **RARP Reply**



- Q: Is Target MAC ever useful?

copyright 2005 Douglas S. Reeves

Some Questions

- Client repeats the RARP Request if no RARP Reply is received
  - how many times?
  - how much delay (time-out) between retransmissions?
- What if multiple Replies?
  - could this be legit?

copyright 2005 Douglas S. Reeves

RARP Servers

- Primary ARP server
  - provides mapping for many hosts
  - Sends RARP Reply directly to the client
- Secondary ARP server(s)
  - does not respond to first RARP Request from the client
  - responds to second RARP Request received within a short time
  - each server randomly delays the Reply to avoid collisions with other servers
- If we use RARP servers, why don't we use ARP servers?

copyright 2005 Douglas S. Reeves

More Questions for RARP

1. Who data fills the server with mappings?
2. What if you want mapping to be only temporary?
3. How handle changes in mapping?
4. What if you want to request more than just IP address, e.g.,…
   1. DNS server
   2. Routing information
   3. Time of day
   4. …?

copyright 2005 Douglas S. Reeves

Summary

1. ARP maps IP (logical) addresses to MAC (hardware) addresses, so IP datagrams can be delivered over arbitrary link layers
2. ARP caches reduce the frequency of ARP Requests
3. ARP spoofing is a substantial security problem
4. RARP maps MAC (hardware) addresses to IP addresses
   - much more widely used: BOOTP / DHCP

copyright 2005 Douglas S. Reeves

Next Lecture

- Classful IPv4 Addresses and Datagram Forwarding

copyright 2005 Douglas S. Reeves