Tunneling, NAT, PAT, ARP, DHCP

Dr. G. Omprakash

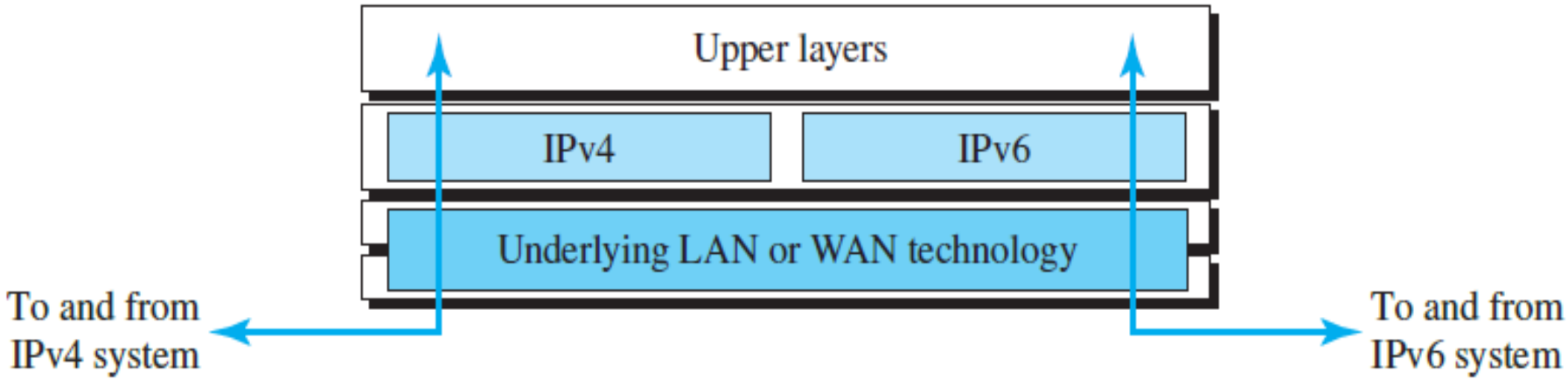
Assistant Professor, ECE, KLEF

How can we make the transition to stop using IPv4 and start using IPv6?

- Three strategies have been devised for the transition
  - Dual stack
  - Tunneling
  - Header translation

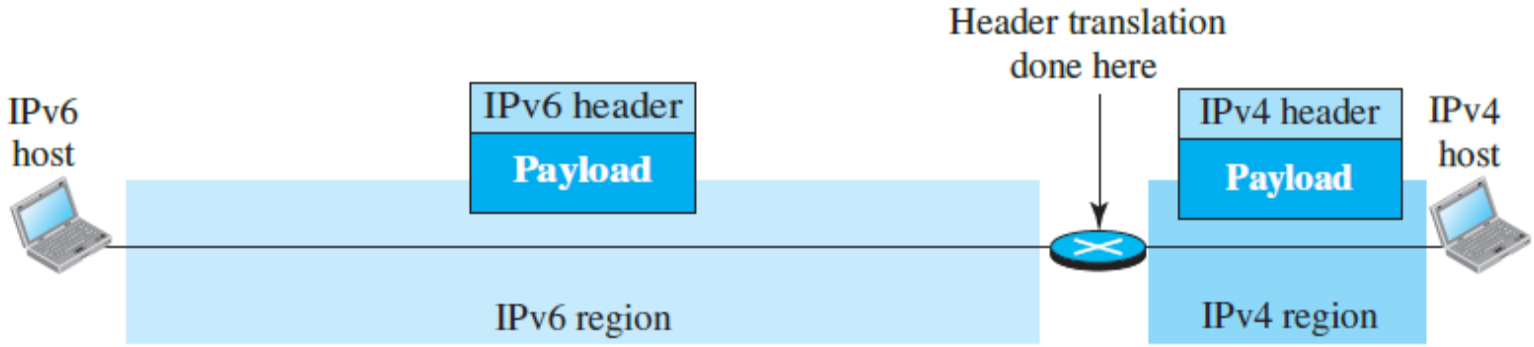
Dual Stack

- Station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6
- When sending a packet to a destination, the source host queries the DNS
  - If the DNS returns an IPv4/IPv6 address, the source host sends an IPv4/IPv6 packet



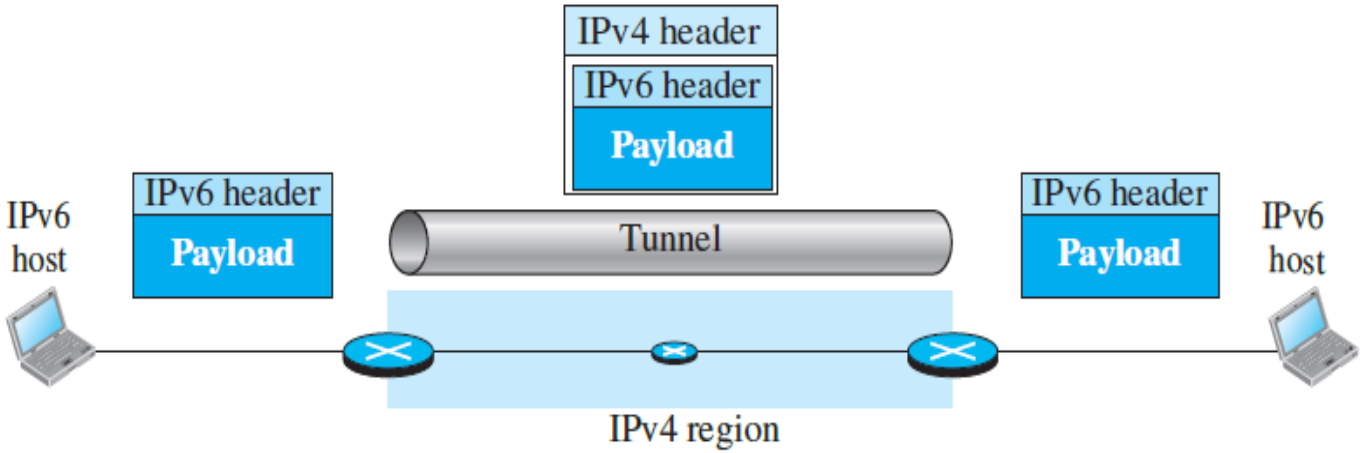
Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4



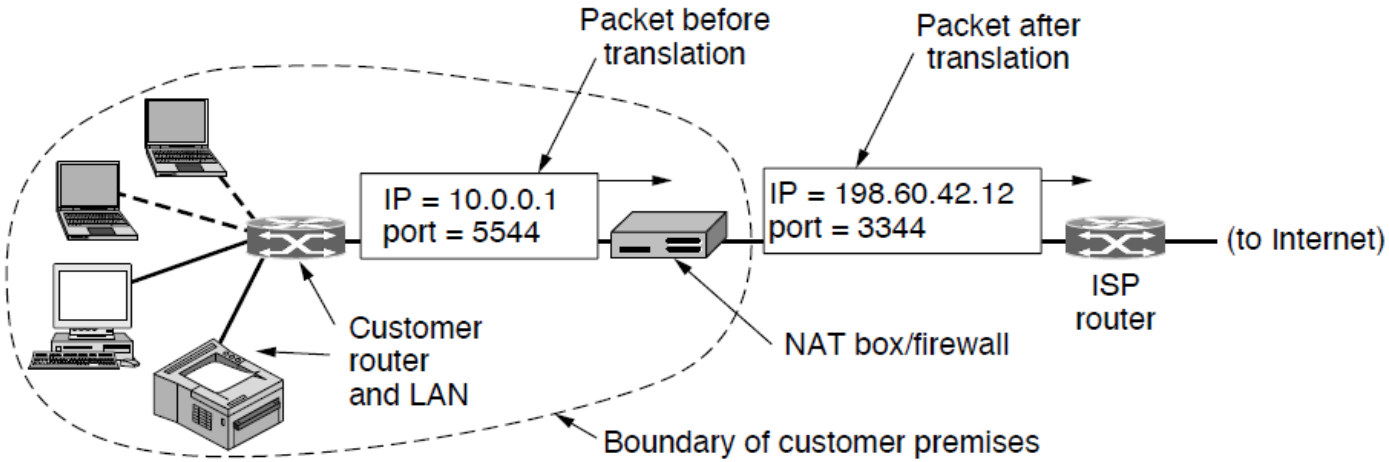
IP Tunneling

- Two computers using IPv6 want to communicate
- Packet has to pass through IPv4 Network
- **IPv6 packet is encapsulated in an IPv4 packet in the region**
  - IPv4 packet is carrying an IPv6 packet as data
  - Only the multiprotocol routers have to understand both IPv4 and IPv6 packets.



Network Address Translation (NAT)

NAT is a technology that allows a private network to use a set of private addresses for internal communication and a set of global Internet addresses for external communication.



Basic idea of NAT

- ISP assigns each home/business a single IP address
- *Within* the customer network, every computer gets a unique IP address
  - used for routing intramural traffic
  - Address translation takes place just before a packet exits the customer network
- The three reserved ranges are:
  - 10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
  - 172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
  - 192.168.0.0 – 192.168.255.255/16 (65,536 hosts)
- Firewall provides security carefully controlling what goes into the customer network

NAT

When the reply comes back (e.g., from a Web server), it is naturally addressed to 198.60.42.12, so how does the NAT box know which internal address to replace it with?

- Most IP packets carry either TCP/UDP payloads
- TCP/UDP have headers containing a source port and a destination port.
- The ports are 16-bit integers that indicate where the TCP connection begins and ends

Port Address Translation (PAT)

Port Address Translation (PAT) allows multiple devices on a local network to be mapped to a single public IP address but with a unique port number for each session.

Private IP:Port	Translated Public IP:Port
192.168.1.10:5000	203.0.113.1:40001
192.168.1.11:5001	203.0.113.1:40002
192.168.1.12:5002	203.0.113.1:40003

PAT device sits at the network perimeter where one side connects the external network, usually the public Internet, and on the other side an internal network using private IP addressing

How PAT Works

- **Source IP and Port Change**
  - When a device inside a private network sends data to the internet, PAT changes its private IP address to a public IP address and assigns a unique port number.
    - 192.168.1.10:5000 $\Longrightarrow$ 203.0.113.1:40001
- **Mapping in the NAT Table**
  - The router keeps a mapping table of private IPs and their assigned port numbers.
  - When a response comes back, the router uses this table to send the data back to the correct internal device
- **Returning Traffic**
  - The internet sends responses to the router's public IP with the assigned port number.
  - The router checks its PAT table, translates the address back to the original private IP, and delivers the packet to the correct device

PAT

- Advantages:
  - **Conserves Public IP Addresses** – Multiple devices can use a single public IP.
  - **Enhances Security** – Internal IPs remain hidden from external networks.
  - **Simplifies Network Management** – No need to assign multiple public IPs.
- Disadvantages
  - **Port Exhaustion** – If too many devices try to communicate, there might be a shortage of available ports.
  - **May Cause Issues with Certain Applications** – Some applications (e.g., VoIP, gaming) rely on direct IP communication and may not work well with PAT.

Internet Control Protocols: ICMP,ARP,DHCP

Internet Control Message Protocol*

IPv4 has no error-reporting or error-correcting mechanism. What happens if something goes wrong?

- What happens if
  - a router must discard a datagram because it cannot find a route to the final destination?
  - the time-to-live field has a zero value?
  - the final destination host must discard the received fragments of a datagram because it has not received all fragments within a predetermined time limit?

ICMP*

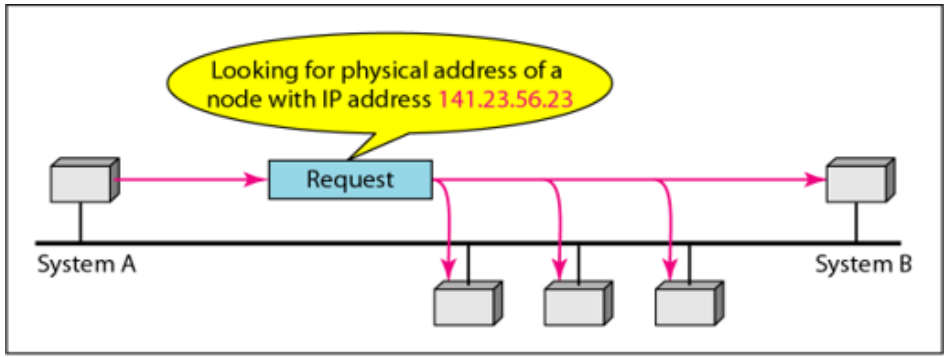
When something unexpected occurs during packet processing at a router,the event is reported to the sender by the ICMP (Internet Control Message Protocol).

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

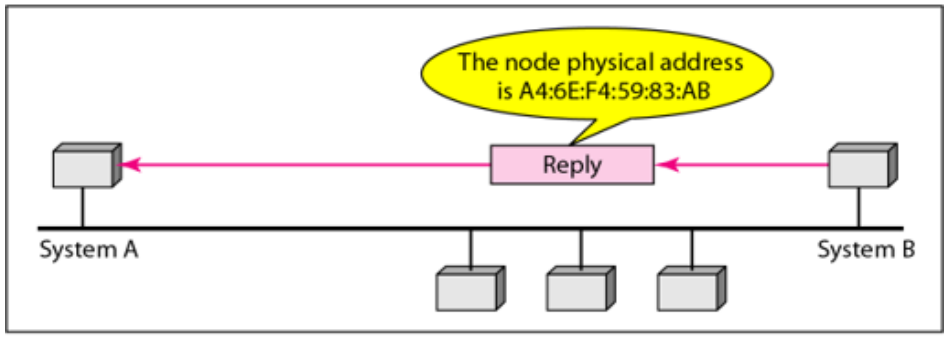
Figure: Principal ICMP message types

ARP—The Address Resolution Protocol

- Every machine on the Internet has one or more IP addresses
- Network Interface Cards in DLL do not understand Internet addresses
- **How do IP addresses get mapped onto data link layer addresses?**



a. ARP request is broadcast



b. ARP reply is unicast

Figure: ARP operation

ARP Packet

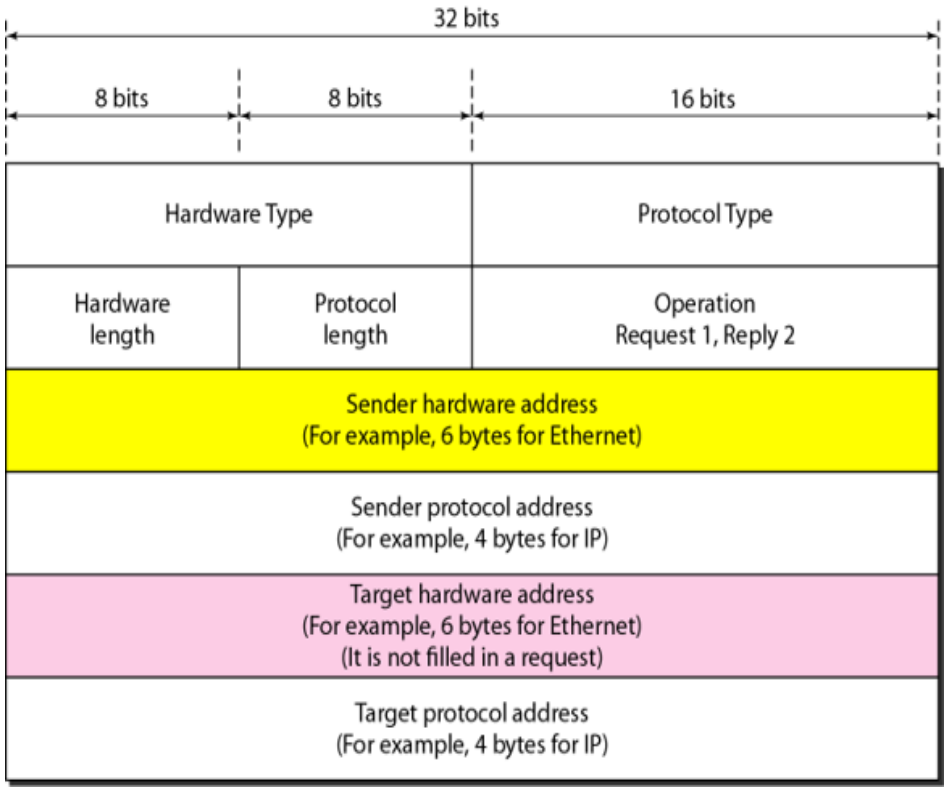


Figure: ARP Packet

Address Mapping

- The sender knows the target's IP address
- ARP request message is created containing
  - The sender physical address
  - The sender IP address
  - The target physical address field is filled with 0s
  - The target IP address
- The message is passed to the data link layer to encapsulate in a data link frame
  - Physical destination address is broadcast address

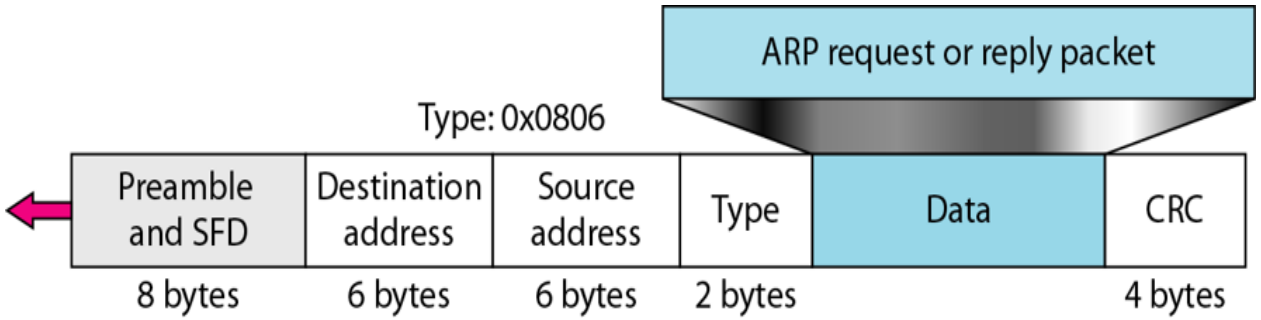


Figure: Encapsulation of ARP

ARP

- Every host or routers receives the frame
- All machines except the one targeted drop the ARP packet
- The target reply with an ARP reply message that contains its physical address and is unicast
- The sender receives the reply message and knows the target's physical address

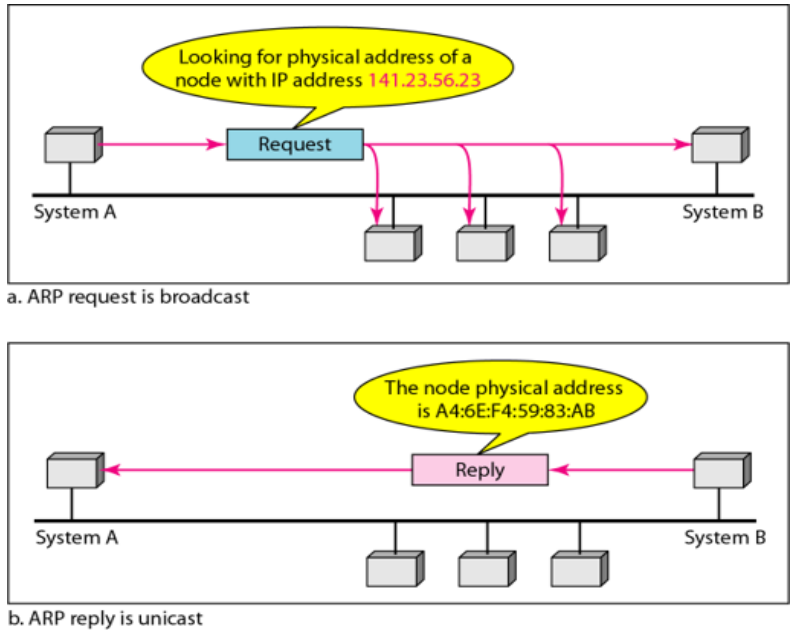


Figure: ARP operation

Dynamic Host Configuration Protocol-DHCP

- ARP makes the assumption that hosts are configured with some basic information, such as their own IP addresses
- Manually configuring IP address to each computer is tedious and error-prone.
- **Better way**: DHCP
- Every network must have a DHCP server that is responsible for configuration

DHCP

- **DHCP DISCOVER packet**
  - After we switch ON a computer, it broadcasts a request for an IP address on its network: DHCP DISCOVER packet
  - This packet must reach the DHCP server (via router)
- **DHCP OFFER Packet**
  - When the server receives the request, it allocates a free IP address and sends it to the host in a DHCP OFFER packet (relayed via the router)
- Even when hosts do not have IP addresses, the DHCP server identifies a host using its Ethernet address

Acknowledge various sources for the images.
Thankyou