v.1.4 - 2019

LOCAL IP, ARP AND ICMP

Practical on communicating local hosts and the ARP and ICMP protocols

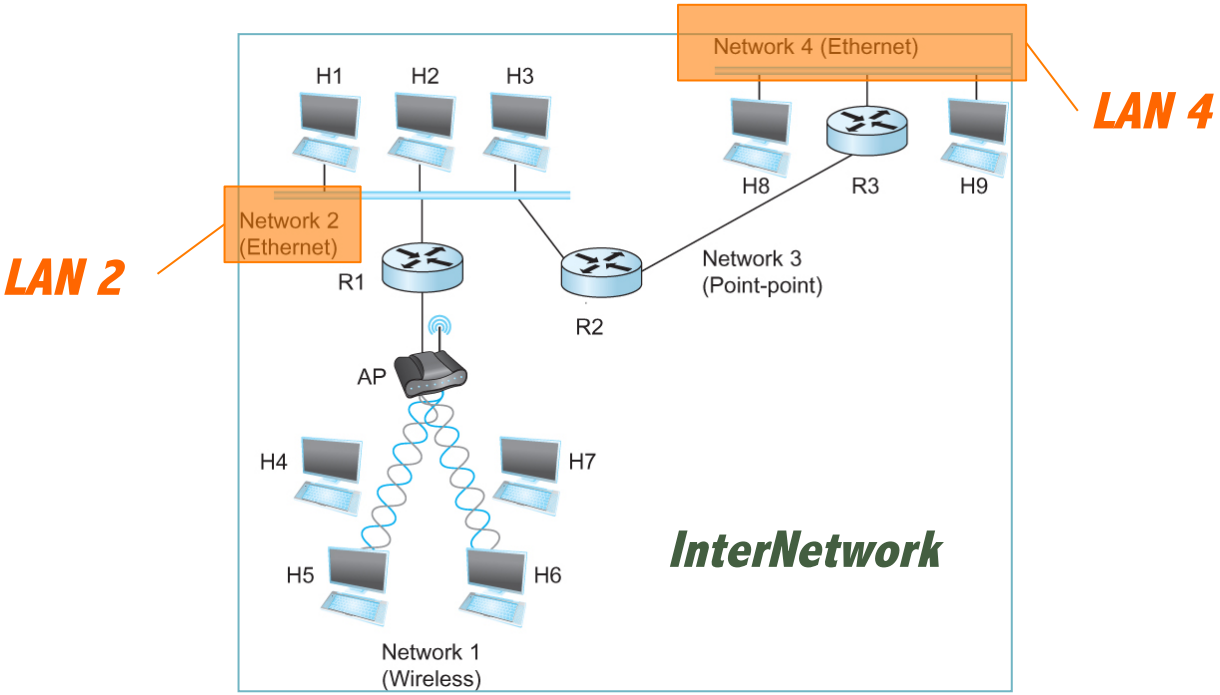
Computer Networks, Universidad de León, 2014-2019

Motivation for InterNetworking

*"A vast majority of IP traffic begins and ends on a **LAN**"*

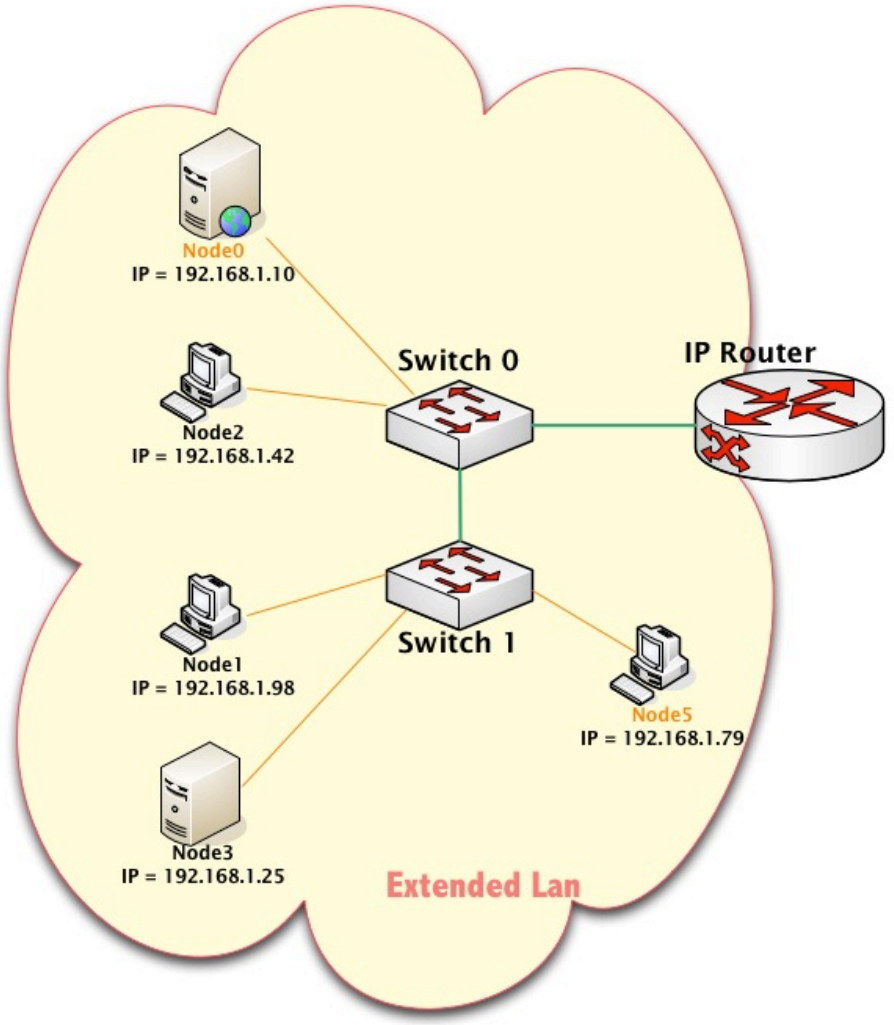
"A vast majority of distributed applications use IP"

- Therefore, IP addresses are used to locate and identify all hosts (H1, H2,…)



IP addresses, used for locating every end node

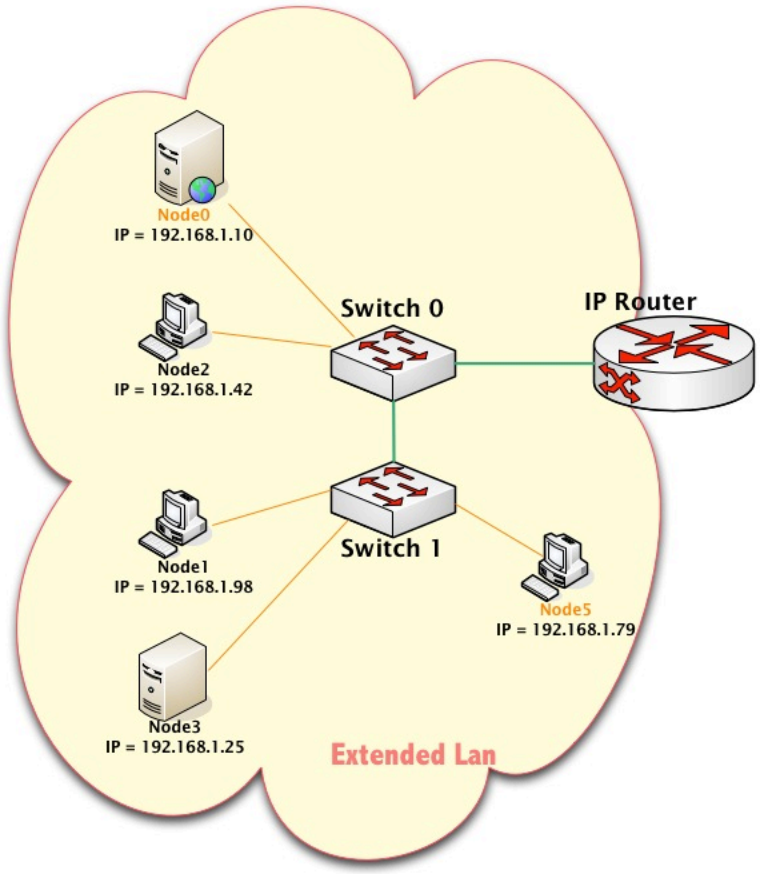
- **Then, within a specific LAN** how can an IP packet from node0 be sent to node5?
- We know that IP addresses are used in the InterNetwork but how about within a specific network?



Send an IP packet from node0 to node5

Node 0 has to **encapsulate** the IP packet within an Ethernet frame:

- 1. Preamble
- 2. Destination MAC address:
  We only know its **IP = 192.168.1.79**, how come? Where's the MAC?
- 3. Source MAC address: We know it, it's our adapter's MAC
- 4. Ethertype multiplexing key (IP=0x0800)
- 5. Payload: The IP packet
- 6. CRC



Address Translation Protocol (ARP)

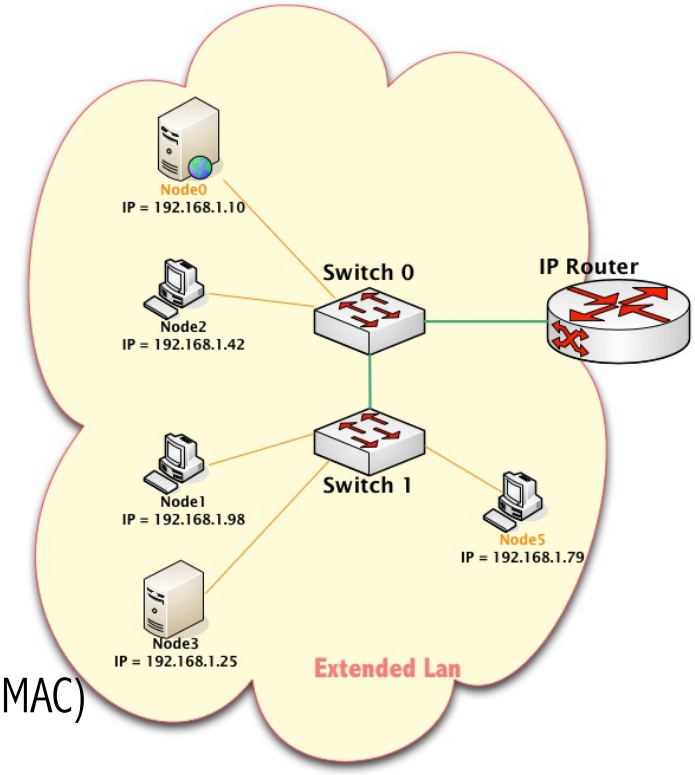
- That is, how can we get the MAC of 192.168.1.79?

Possibilities:

- *Encode physical address in host part of IP address*
- *Fixed table*
- A **Dynamic Table** at each host: Managed by ARP protocol
  - **Broadcast** if 192.168.1.79's MAC address is not in table
  - target machine will **respond** with its physical address (MAC)
  - table entries are **discarded** after a few minutes

Address Translation Protocol (ARP)

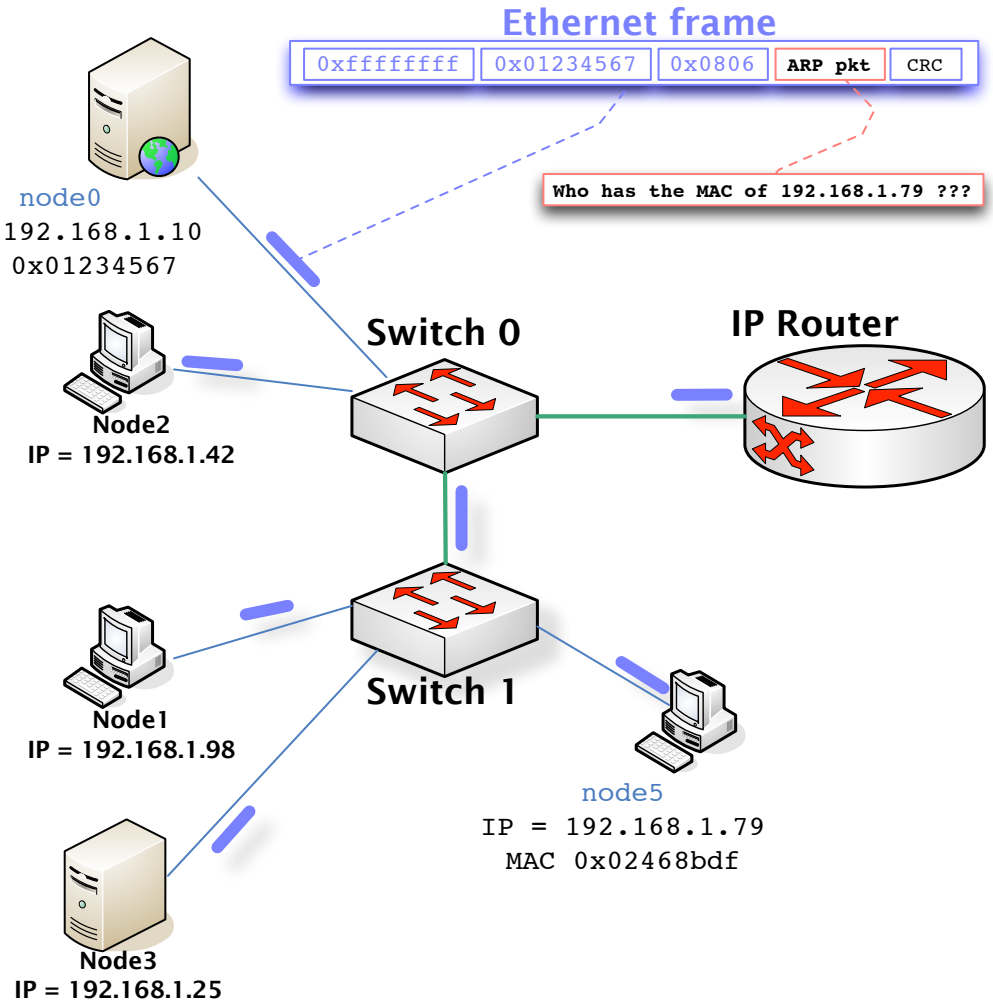
- How does node0 discover node5's MAC address?
  - node0 has its own ARP table
    - node5's MAC address is not there yet
  - **Broadcast** the following question (Send it to the whole extended LAN):
    - Who has the MAC address of 192.168.1.79? Tell 192.168.1.10
  - Target machine will **respond** with its physical address (MAC)
  - Question/Response sent in an ARP packet:



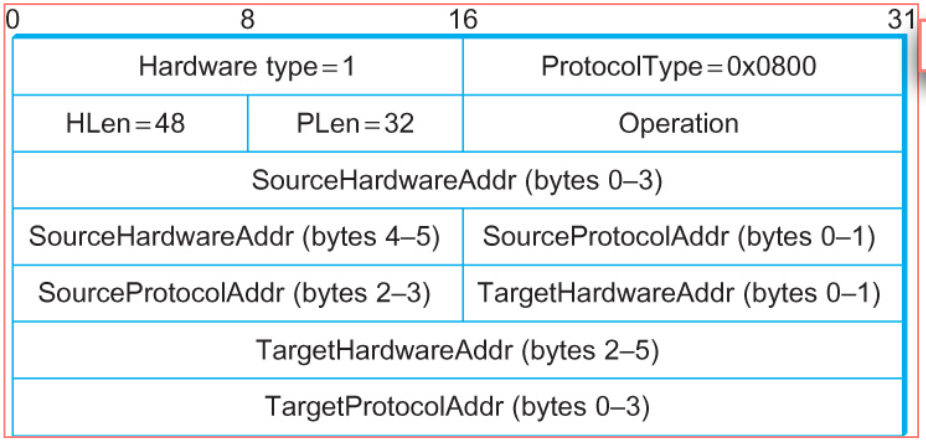
0	8	16	31
Hardware type = 1		ProtocolType = 0x0800	
HLen = 48	PLen = 32	Operation	
SourceHardwareAddr (bytes 0–3)			
SourceHardwareAddr (bytes 4–5)		SourceProtocolAddr (bytes 0–1)	
SourceProtocolAddr (bytes 2–3)		TargetHardwareAddr (bytes 0–1)	
TargetHardwareAddr (bytes 2–5)			
TargetProtocolAddr (bytes 0–3)			

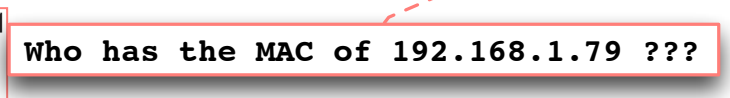
Address Translation Protocol (ARP)

- **Broadcast** the following ARP REQUEST (Send to the whole extended LAN):
  - Who has the MAC address of 192.168.1.79? Tell 192.168.1.10



ARP Packet Format



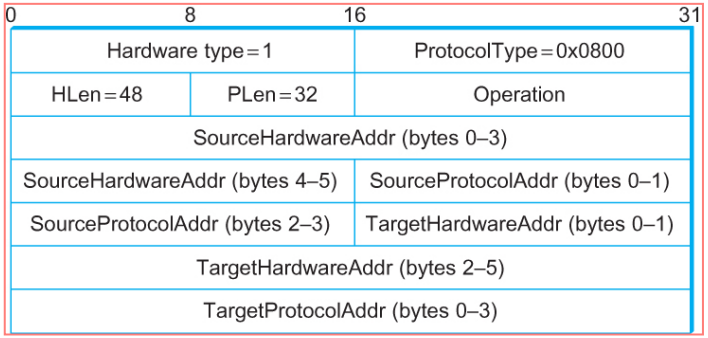


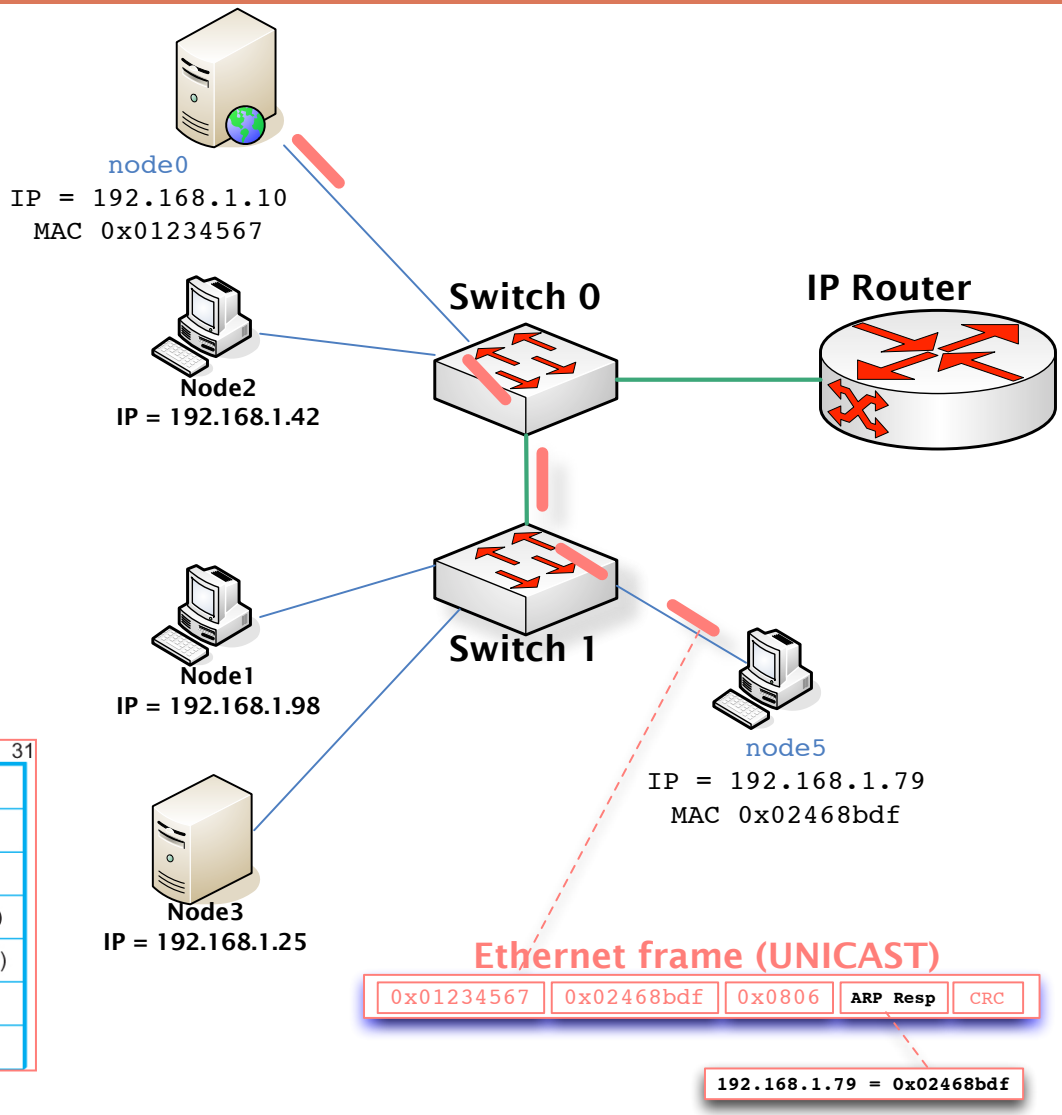
- HardwareType: type of physical network (e.g., Ethernet)
- ProtocolType: type of higher layer protocol (e.g., IP)
- HLEN & PLEN: length of physical and protocol addresses
- Operation: request or response
- Source/Target Physical/Protocol addresses

Address Translation Protocol (ARP)

- Only the requester, node0, receives the ARP RESPONSE
  - In a **Unicast** frame
  - This time:

    OPERATION = RESPONSE

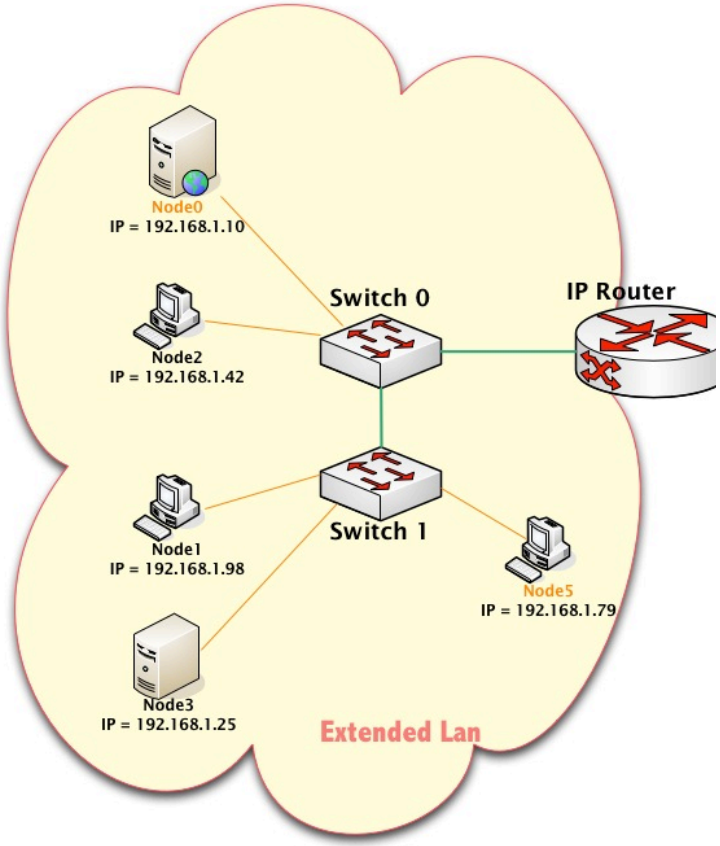




Summary: …send an IP packet from node0 to node5

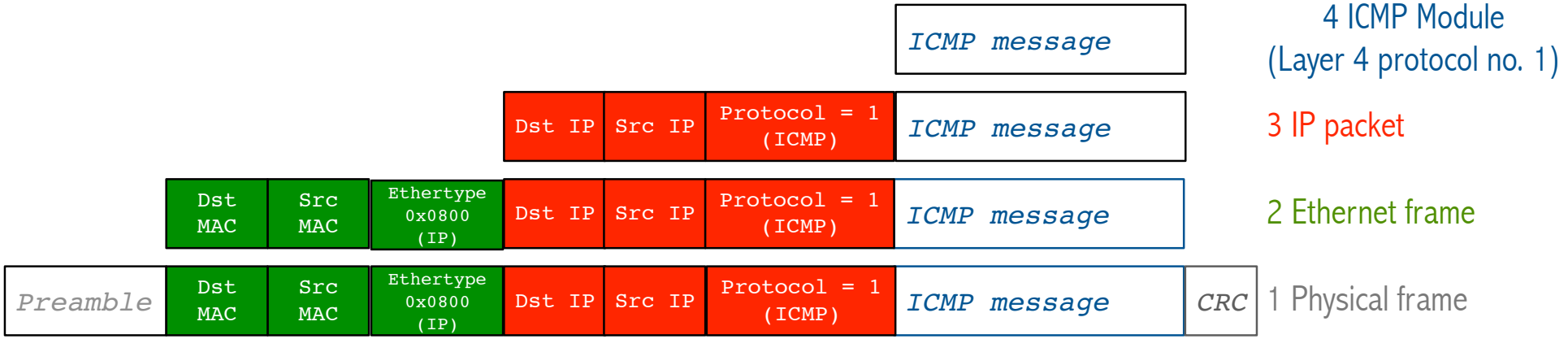
Now, node0 DOES KNOW THE MAC of node5, proceed to encapsulate the IP packet in an Ethernet frame:

- 1. Preamble
- 2. Destination MAC address is resolved via ARP
- 3. Source MAC address: We know it, it's our adapter's MAC
- 4. Protocol de-multiplexing key (IP=0x0800)
- 5. Payload: The IP packet
- 6. CRC



Internet Control Message Protocol (ICMP)

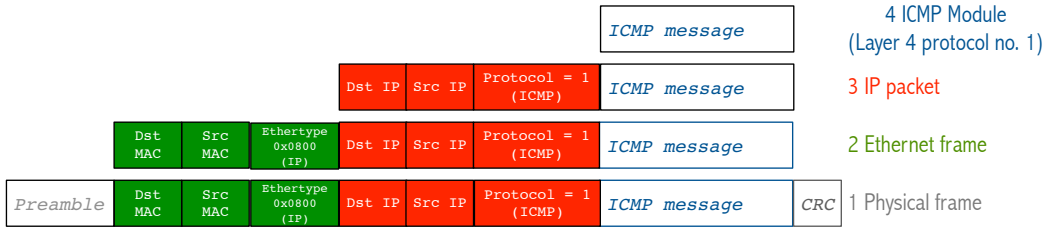
- Defines a collection of error messages used for IP communications



Internet Control Message Protocol (ICMP)

- Defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully
  - Destination host unreachable due to link /node failure
  - Reassembly process failed
  - TTL had reached 0 (so datagrams don't cycle forever)
  - IP header checksum failed

- ICMP-Redirect
  - From router to a source host
  - With a better route information



Host Configurations

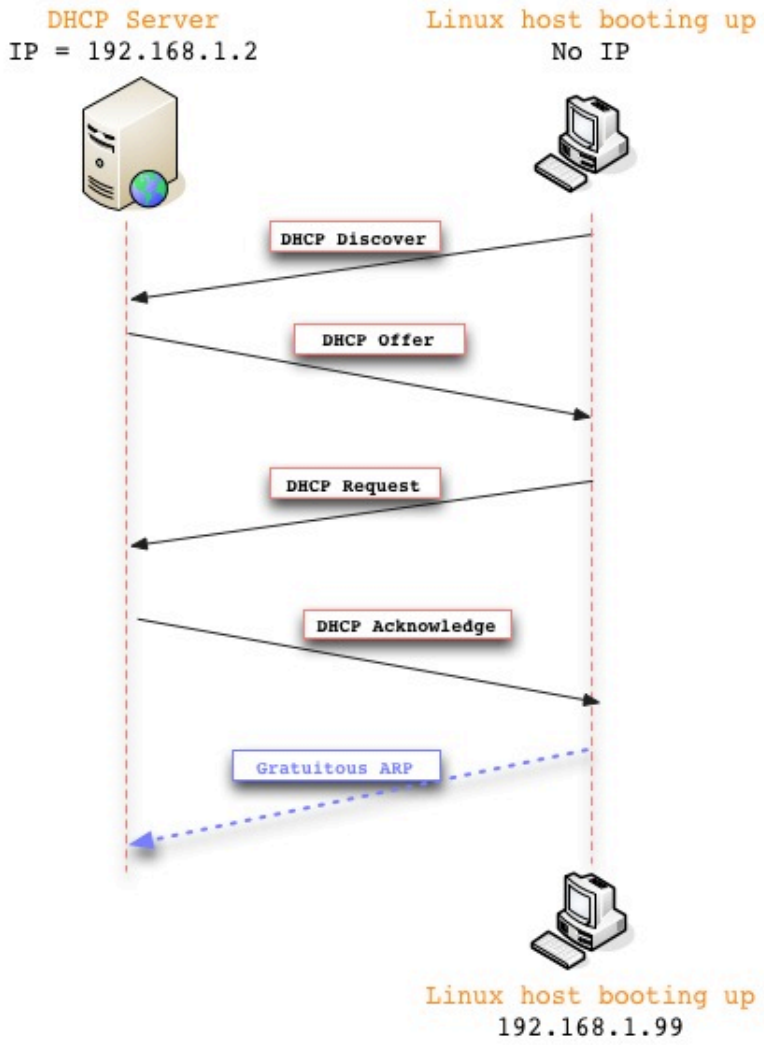
- Notes
  - (MAC) Ethernet addresses are configured into network by manufacturer and they are unique
  - IP addresses must be unique on a given internetwork but also must reflect the structure of the internetwork
  - Most host Operating Systems provide a way to manually configure the IP information for the host
  - Drawbacks of manual configuration
    - A lot of work to configure all the hosts in a large network
    - Configuration process is error-prune
  - Automated Configuration Process is required

Dynamic Host Configuration Protocol (DHCP)

- DHCP server is responsible for providing configuration information to hosts
  - The network adapter's IP address
  - The network adapter's network mask
  - The default router's IP address
  - The DNS IP address
  - etc
- There is at least one DHCP server for an administrative domain
- DHCP server maintains a pool of available addresses

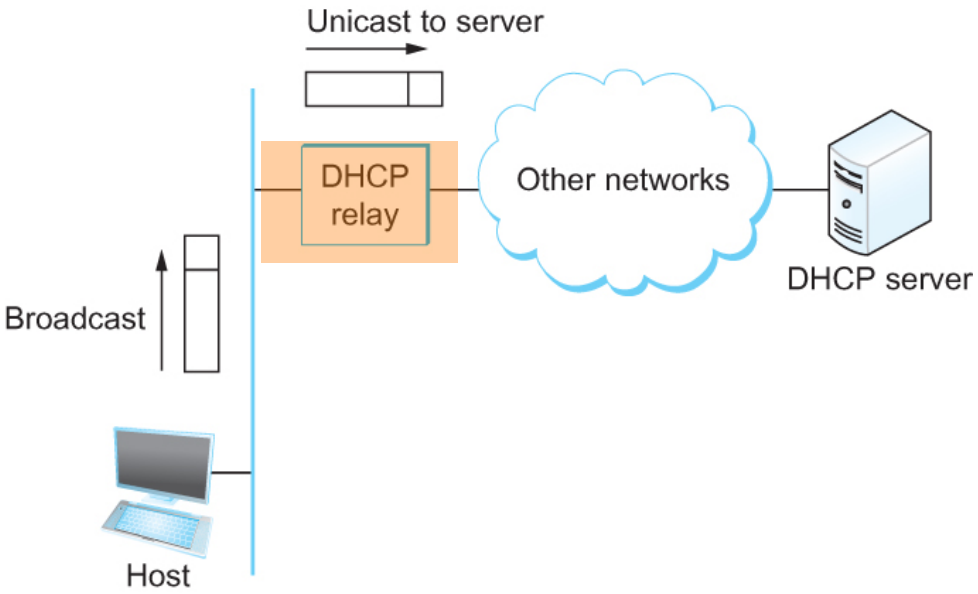
DHCP server on the same network

- Newly booted or attached host sends DHCPDISCOVER message to a special IP address (255.255.255.255, the broadcast IP address)
- Host receives DHCP offers
- Sends request for a specific offered IP
- Server sends DHCP ACK to confirm assignment



DHCP server on a different network

- Newly booted or attached host sends DHCPDISCOVER message to a special IP address (255.255.255.255)
- DHCP relay agent unicasts the message to DHCP server and waits for the response



The end