Networking and Internet Services Part-1

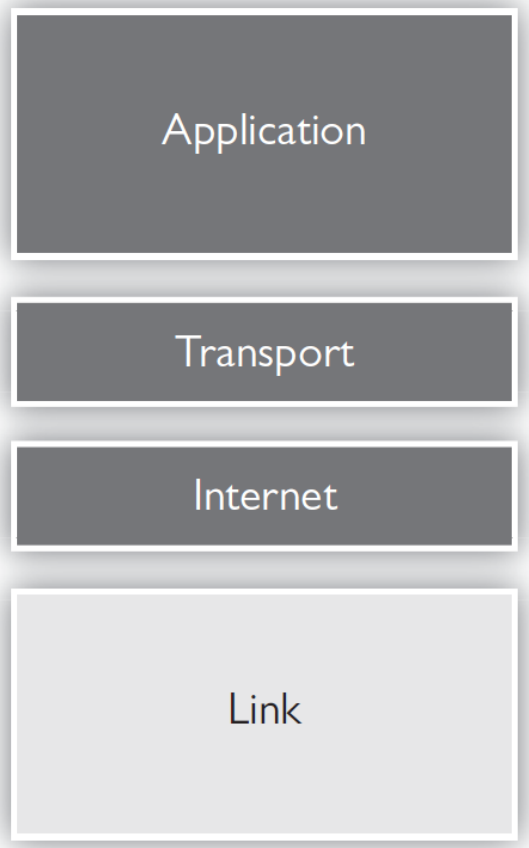
Presented by
Omid Panahi

Champlain
COLLEGE SAINT-LAMBERT

IP Addressing

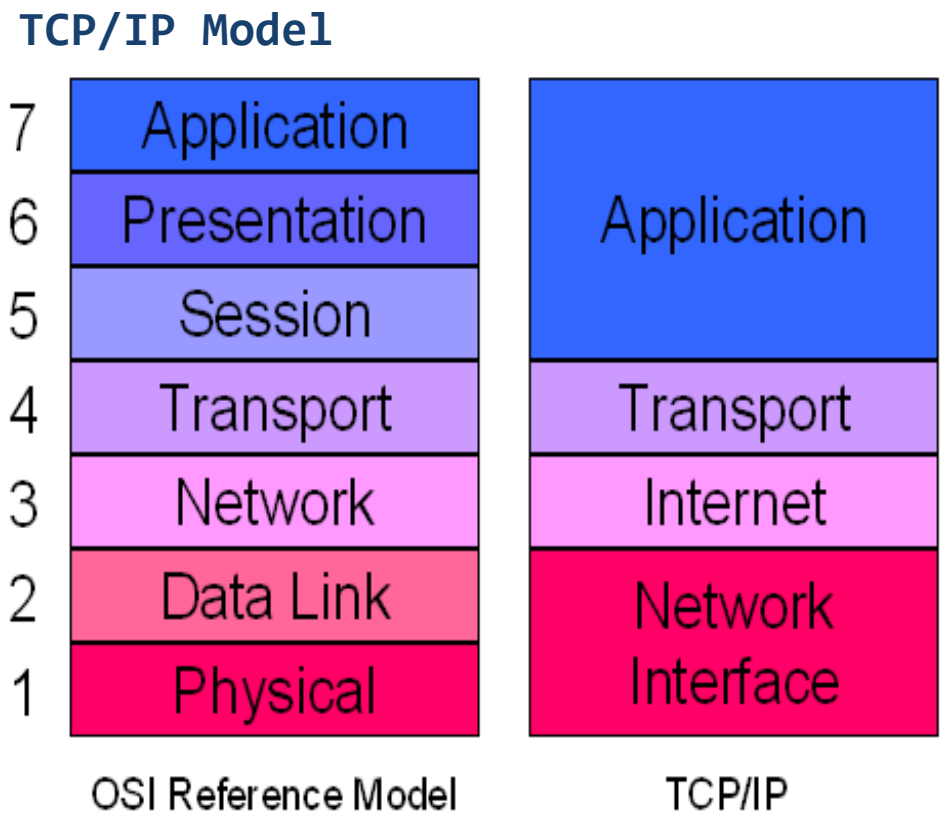
TCPIP Protocol Suite

- We will look at the Internet step of the TCP suite
- Recall the function of the Internet step (frame vs. packet, MAC vs. IP).

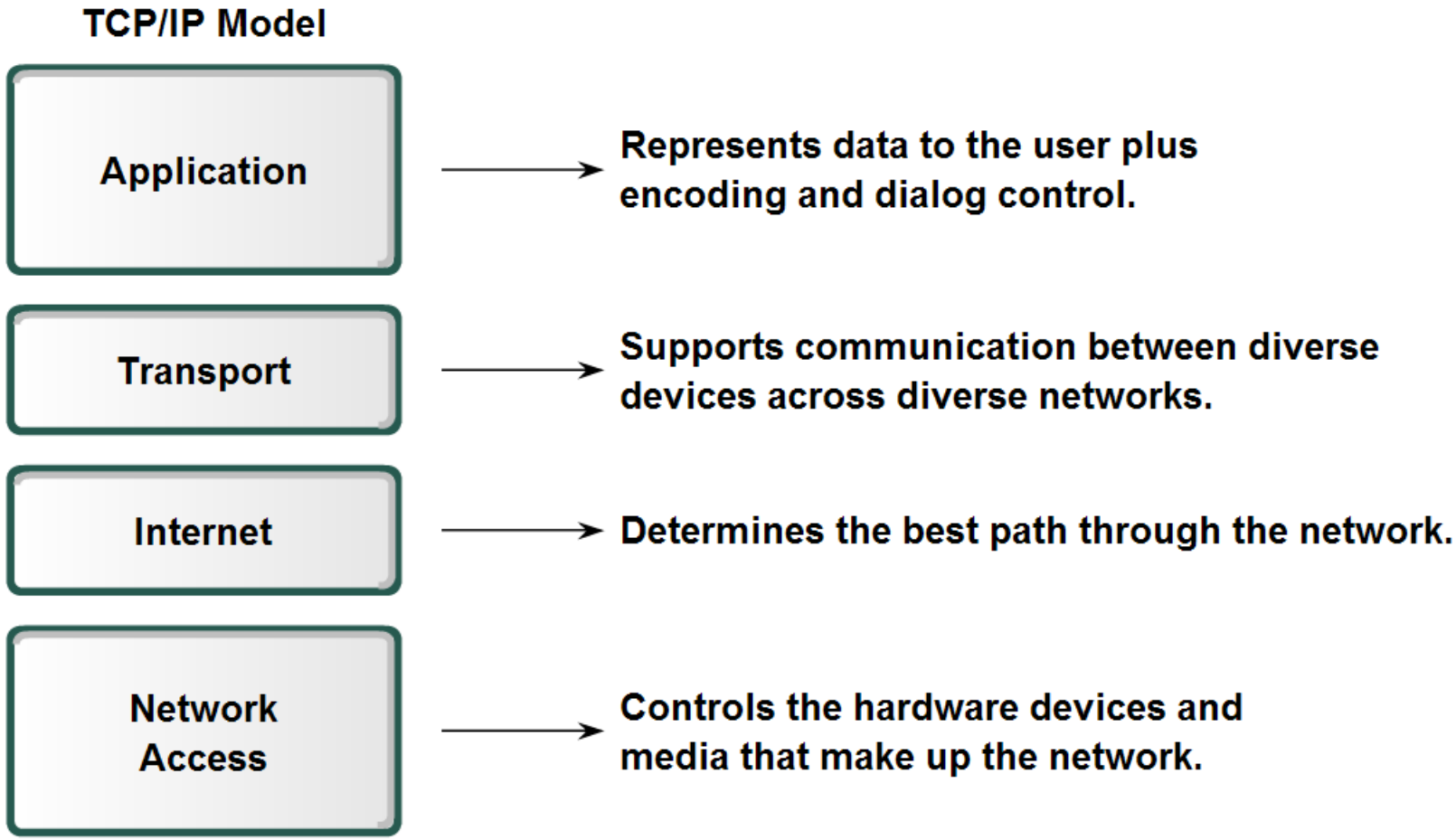


TCPIP MODEL

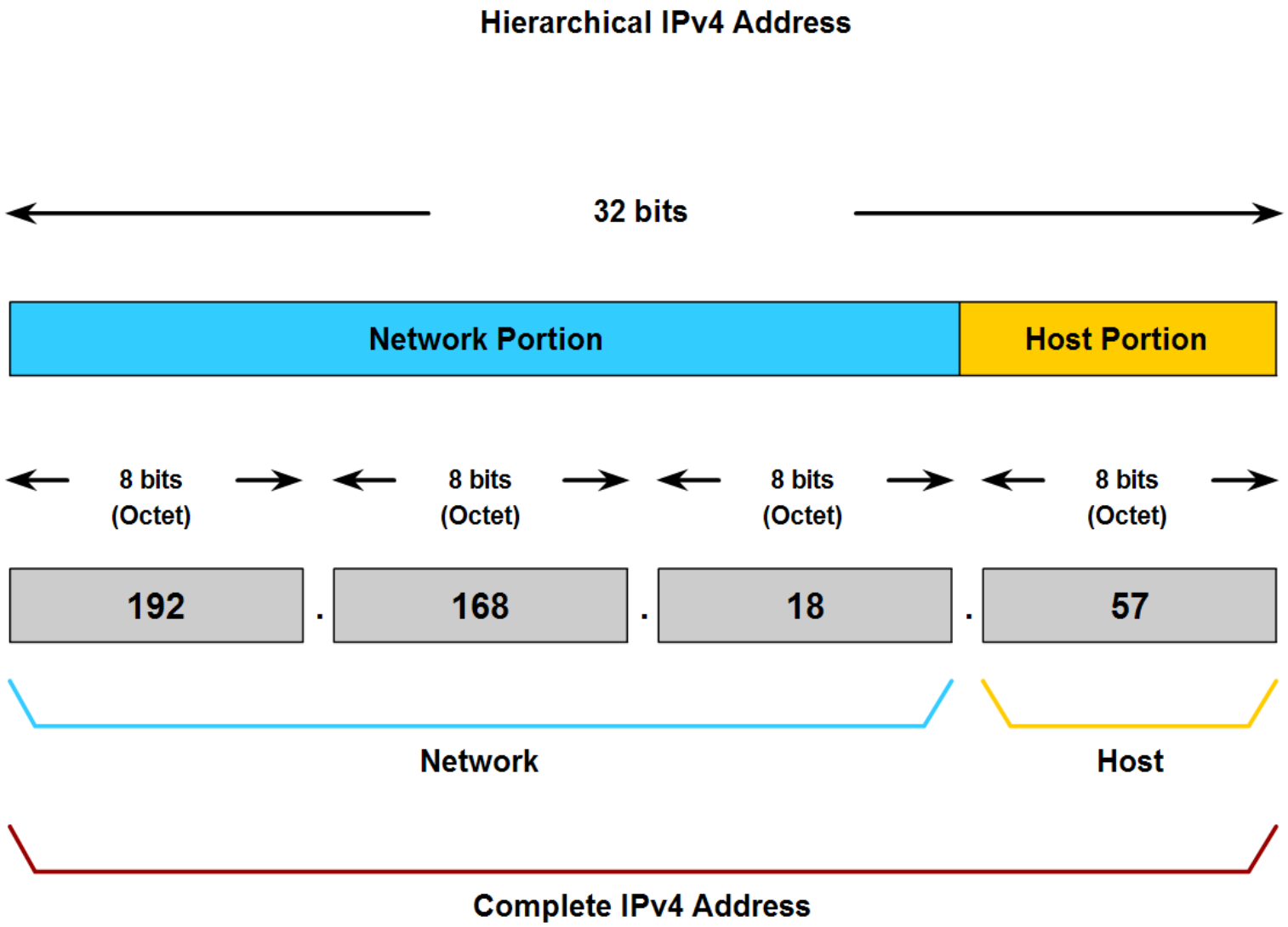
- Divided into 4 Layers
  - Application
  - Transport
  - Internet
  - Network Interface



TCP-IP Model


TCP/IP Model
Application
Represents data to the user plus encoding and dialog control.
Transport
Supports communication between diverse devices across diverse networks.
Internet
Determines the best path through the network.
Network Access
Controls the hardware devices and media that make up the network.

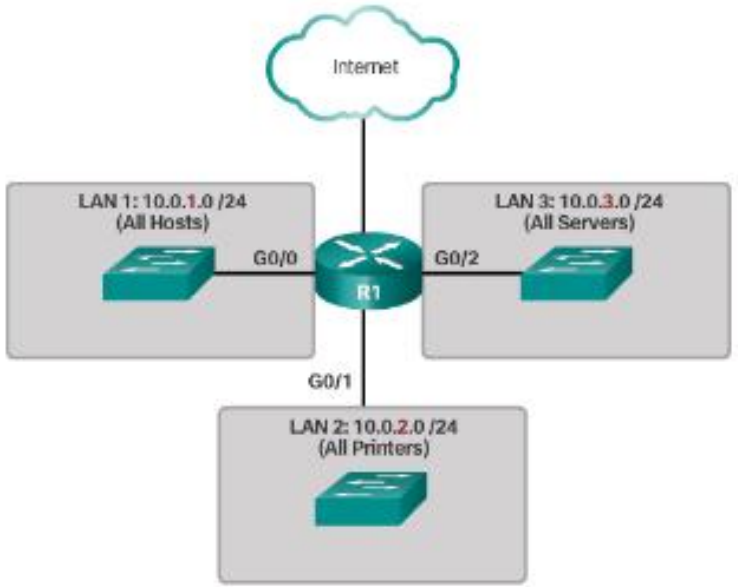
Overview of IP Addressing



Slides - courtesy of Cisco Systems

Network Segmentation

- Broadcast Domains
  - Each router interface connects a broadcast domain.
  - Broadcasts are only propagated within its broadcast domain.
- Problems with Large Broadcast Domains
  - Slow network operations due to the significant amount of broadcast traffic.
  - Slow device operations because a device must accept and process each broadcast packet.



Slides - courtesy of Cisco Systems

Collision Domain vs. Broadcast Domain

Collision Domain:

- **Definition**: A collision domain refers to a network segment where data packets can collide with one another, especially in older half-duplex Ethernet networks.
- **Implication**: In a collision domain, only one device can transmit at a time. If two devices transmit simultaneously, a collision occurs, causing both devices to back off and wait a random amount of time before attempting to retransmit.
- **Reduced by**: Each port on a switch creates its own collision domain. This means that in modern switched Ethernet networks, collisions are essentially eliminated because each device (connected directly to a dedicated switch port) has its own collision domain.
- **Legacy**: Collisions were common in older hub-based Ethernet networks (using hubs instead of switches) because all devices shared the same transmission medium.

Collision Domain vs. Broadcast Domain

Broadcast Domain:

- **Definition**: A broadcast domain encompasses all devices that can be reached by a broadcast frame originating from any device within that domain. In simple terms, it's a segment of a network in which all other devices receive a broadcast sent by one device.
- **Implication**: Large broadcast domains can create a lot of unnecessary traffic since every broadcast must be processed by every device in the domain. This can reduce the overall efficiency and performance of the network.
- **Controlled by**: Routers (and Layer 3 switches) are devices that separate broadcast domains. While Layer 2 switches forward broadcast frames to all ports (except the source port), routers do not forward broadcast frames, effectively limiting the broadcast domain's size.
- **Relation to VLANs**: In modern networks, Virtual Local Area Networks (VLANs) can be used to segment broadcast domains. Each VLAN creates a separate broadcast domain, even if the devices in different VLANs are connected to the same physical switch.

Subnetting

Decimal to Binary conversion

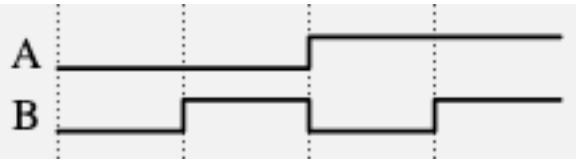
- Enter the correct binary value for each position given the decimal value

Decimal value	209							
Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	1000 0000	0100 0000	0010 0000	0001 0000	0000 1000	0000 0100	0000 0010	0000 0001

And

A	B	X	Y
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	0

assign X = A & B;



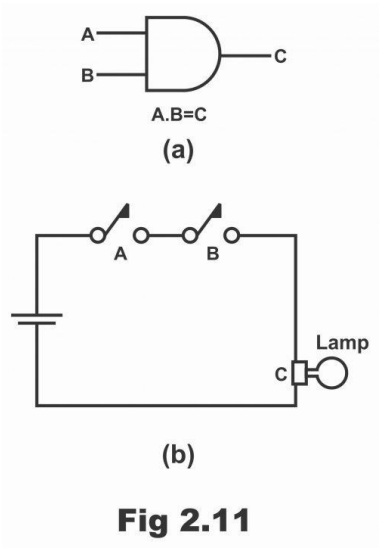
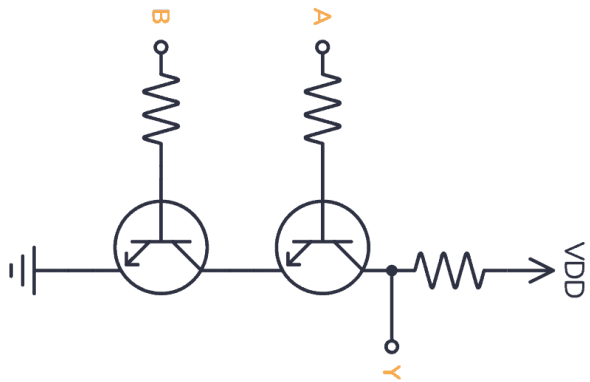


Fig 2.11



Subnet Masks

A subnet mask is a 32-bit number that segments an IP address into its network and host portions. It's used in IP networking to facilitate the operation of subnets, allowing a single IP network to be divided into smaller networks.

In the context of IP addressing, this helps manage and allocate IP addresses more efficiently within networks and allows for network traffic to be routed optimally.

Subnet Masks

Here are some fundamental points about subnet masks:

1. Binary Representation: Like an IP address, a subnet mask can be represented in binary. Each bit in the mask that is set to 1 denotes that the corresponding bit in the IP address is part of the network address. Each bit set to 0 denotes that it's part of the host address.

Subnet Masks

2. Dotted Decimal: Subnet masks are usually represented in the same dotted-decimal format as IP addresses.

3. Purpose: The subnet mask allows a device to determine the network portion of its IP address, which helps determine whether a target IP address is on the local network or a remote network.

4. CIDR Notation: With Classless Inter-Domain Routing (CIDR), subnet masks can be represented more concisely. Instead of 192.168.1.0 with a subnet mask of 255.255.255.0, you can use 192.168.1.0/24, where /24 indicates the first 24 bits are used for the network portion.

Subnet Mask

5. Subnetting: By customizing the subnet mask, network administrators can divide a larger network into smaller sub-networks or subnets. This can help optimize performance, improve organization, and enhance security within larger networks.

6. WildCard Mask: This is the inverse of a subnet mask and is used in some network configurations, particularly with certain access control lists (ACLs) in Cisco devices. If a subnet mask is 255.255.255.0, its wildcard mask is 0.0.0.255.

When configuring a network or a network device, it's crucial to ensure that the subnet mask is correctly set. This ensures proper communication within local subnets and optimal routing to external networks.

Subnet Masks

- Every TCP/IP computer needs a tool to tell the sending computer whether the destination IP address is local or long-distance. This tool is the subnet mask.

- A subnet mask looks like: 255.255.255.0

Resume of IP so far

	Dotted Decimal	Binary
IP address	192.168.5.23	11000000.10101000.00000101.00010111
Subnet mask	255.255.255.0	11111111.11111111.11111111.00000000
Network ID	192.168.5.0	11000000.10101000.00000101.*x*
Host ID	*x.x.x*.23	*x.x.x*.00010111

Remote address

- A situation where the computer is identified as NOT being in the local network by using the subnet mask.

Subnet mask:	11111111111111111111111111	00000000
Computer A IP:	11000000101010000000000101	00010111
Computer B IP:	10110110110111010000000011	00101101

Example of using a Subnet Mask

- Computer A = 192.168.5.23
- Computer B = 192.168.5.45
- Computer C = 192.168.4.22

- Computer A, B (On LAN 1)
- Computer C (On LAN 2)

- Subnet mask is defined as : 255.255.255.0

Subnetting

- Subnet Mask
  - 11111111.11111111.11111111.00000000
- Computer A
  - 192.168.5.23
  - 11000000.10101000.00000101.00010111
- Computer B
  - 192.168.5.45
  - 11000000.10101000.00000101.00101101
- Computer C
  - 192.168.4.22
  - 11000000.10101000.00000100.00101101

ARP

ARP stands for **Address Resolution Protocol**. It's a protocol used in the Internet Protocol (IP) suite to map 32-bit IP addresses to MAC (Media Access Control) addresses within a local network, allowing for correct packet delivery within a subnet.

Here's how ARP works and why it's essential:

Function:

- When a device, like a computer, wants to communicate with another device on the same local network, or same broadcast domain or same collision domain it needs to know the target device's MAC address.
- The MAC address is a unique identifier for network interfaces used in local communications within a network segment.
- While the sender might know the IP address of the target device (from higher-level protocols or previous communications), it often won't know the target's MAC address. ARP helps bridge this gap.

ARP

ARP Process:

- **ARP Request**: The device wanting to know the MAC address sends an ARP request. This request is a broadcast packet that essentially asks, "Who has this IP address, and what's your MAC address?"
- **ARP Response**: The device with the specified IP address will reply with an ARP response, which contains its MAC address.
- **ARP Table**: Once the original device gets the MAC address, it stores this information in its ARP cache or ARP table for future reference. This caching avoids the need to repeat the ARP process for every packet sent to the same destination in a short period.

ARP

ARP Spoofing:

- While ARP is a crucial protocol for IP-based networks, it's also susceptible to a type of attack called ARP spoofing or ARP poisoning. In this attack, a malicious actor sends fake ARP messages to a local network, associating its MAC address with the IP address of another device, usually a gateway. This can lead the attacker to intercept, modify, or even stop data flows.

Other ARP-related Protocols:

- RARP (Reverse Address Resolution Protocol): As the name suggests, it's the opposite of ARP. RARP allows a device to request its IP address given its MAC address. However, RARP is considered obsolete and has been replaced by other protocols like BOOTP and DHCP.

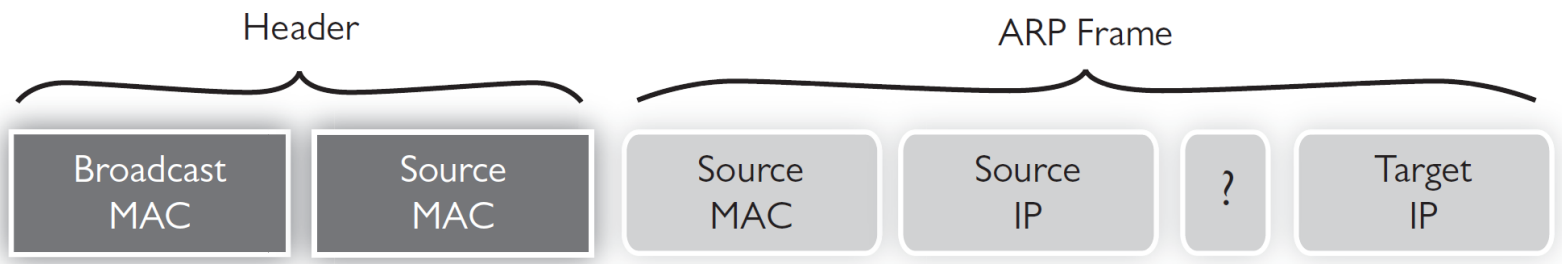
ARP

- **Proxy ARP**: A technique where one device, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts the responsibility for routing packets to the "real" target device.

In summary, ARP is a foundational protocol in IP networking, ensuring that devices can find the correct MAC address for a given IP address within their local network.

Find the IP of another computer then determine if it's local or not.

- Send an ARP request.
- Broadcast the ARP request
- ARP Frame:



Steps for a remote conversation

- Send out a broadcast to find the default gateway.
- Get the MAC and IP of the default gateway.
- More on what happens later.

Exercise:

Champlain

COLLEGE SAINT-LAMBERT