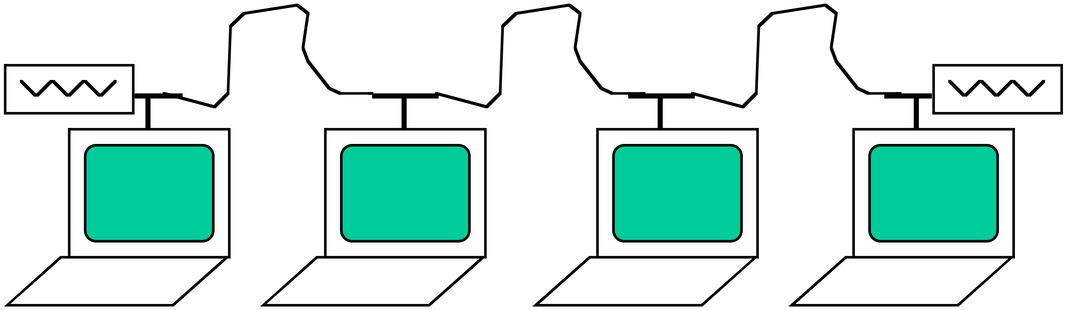
# Ethernet Local Area Networks (LANS)

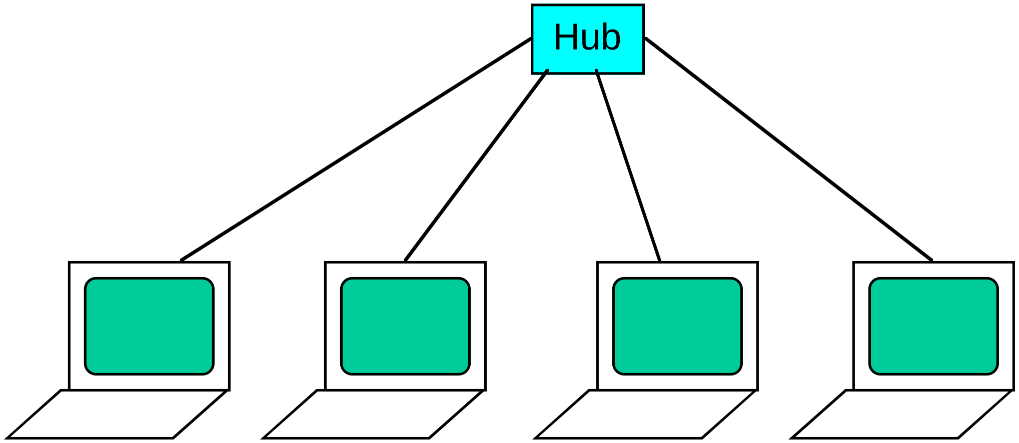
**Two basic ways to cable an 10 Mb/s Ethernet LAN:**

- Bus-style (large Ethernet cable, or thin Ethernet cable)
  - Large Ethernet cable is bulky, uses cable-taps.
  - Smaller cable is more flexible, uses BNC-T connectors.
  - Bus must be terminated at each end. Bus is easily broken by one bad connection or NIC. Difficult to troubleshoot when cable is inside walls or ceilings, or lot of attached workstations
- Star-style (10-base-T twisted-pair wiring and hubs)
  - Star requires a hub. Hub isolates a failure so it doesn’t impact rest of the LAN. Much better fault resilience. Hub requires power.
  - Two 10-base-T units can be connected back-to-back with a cross-over cable not needing a hub.
  - Uses RJ-45 eight-conductor connector.
- Thin Coax <--> Twisted-pair adapters readily available.

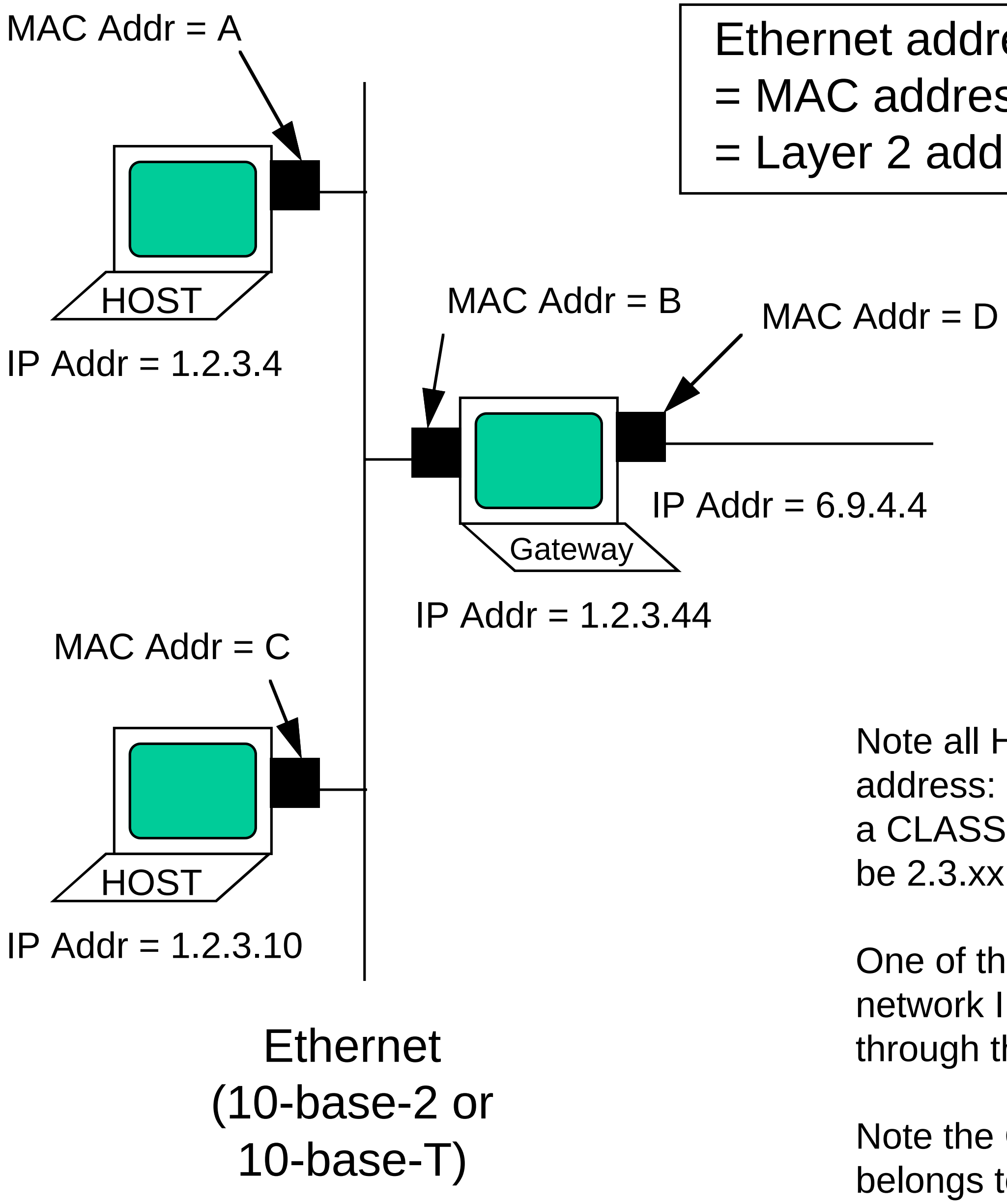
# Bus-Style Cabling



# Star-Style Cabling



# MAC-layer and IP addressing



Ethernet address
= MAC address
= Layer 2 address

MAC address is 48 bits. It is globally unique, and permanently assigned at the time of manufacture of the Ethernet interface.
Ex: 0A.34.F4.02.0C.4

IP address is 32 bits. It is hierarchically assigned, and may be dynamically assigned. It must fit within the **HOST** address space.
Ex: 34.122.251.99

Note all Hosts share the same **NETWORK** address: 1.2.3.xx. Up to 254 Hosts can reside on a CLASS-C network. A CLASS-B network would be 2.3.xx.xx, up to 65534 Hosts could reside on it.

One of these PC’s is the **Gateway**. All off-network IP packets must be sent and received through this host.

Note the Gateway has **two** IP addresses. It belongs to two networks. It routes packets between the two networks 1.2.3.xx and 6.9.xx.xx

# Special IP addresses

There are two types of IP addresses:

**Host** addresses
**Network** addresses

There are two special IP addresses:

**All ones**
**All zeros**

All ones means **‘broadcast address’**
All zeros means **‘this’** address

For example a class-B address is of the form: 128.34.xx.xx

128.34 Specifies which **NETWORK** is being referenced
xx.xx Specifies a particular **HOST** on that network

Thus the address:

128.34.255.255 Is a broadcast to all addresses on the 128.34 network
133.22.255.255 Is a broadcast to all address on the 133.22 network, even if it is remote from us.
128.34.0.0 Refers to ‘**us’** on the 128.34 **network**

The address:

255.255.255.255 Refers to all broadcast addresses, but by convention it is restricted to **‘this’** network (otherwise chaos could result!)
0.0.22.19 Refers to the host 22.19 that is located on ‘**this’** network

**‘this’** is useful when a host does not yet know which network it is on, or when it does not yet know what it’s IP address is.

# Subnetwork Address Mask

A **Subnet Mask** allows dividing up one network into many subnetworks without consuming additional IP addresses. It allows a **single network address** to span multiple physical networks.

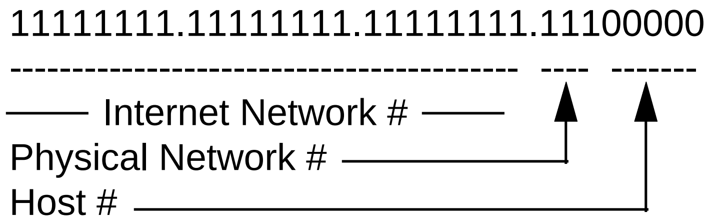
For Example: a class-C Network address is of the form: 172.36.43.xx

| | |
|---|---|
| 172.36.43 | Is the **Network** address |
| xx | Is the **Host** address, 254 possible Hosts. |

But we may wish to have several different networks, connected by Gateways. We could either have multple different network addresses, each consuming 254 host addresses, or we can partition our network space into smaller address spaces. Since the world is running out of IP addresses, the choice is usually clear.

A class-C address has 8 bits in the HOST field. We can claim that 3 of those bits are for subnetworks, and 5 are for hosts. This allows **6 subnetworks** (8 - 2), each of which can have **30 hosts** (32-2).

To do this we specify a subnet mask of:



```
11111111.11111111.11111111.11100000
--------------------------------------  ----  -------
```

A router looks at the network down through the bits covered by the subnet mask. Thus bits 31-5 are network addresses, and bits 4-0 are host addresses. This choice is up to our local administration. The Internet as a whole does not see or care about this distinction. It need only worry about routing to 172.36.43. Gateways between subnetworks inside that one network address must figure out how to route inside. They need to compare addresses against the subnet mask to see if a packet is on ‘this’ network or another network.

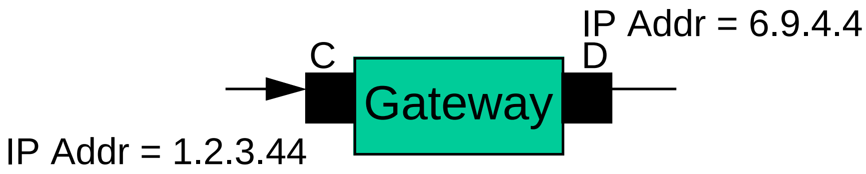
# Address Resolution Protocol (ARP)

ARP is an Ethernet protocol that **binds together** an IP address and a MAC address.  To send a packet from 1.2.3.4 to 1.2.3.10 requires that the packet travel from MAC address A to MAC address C.  How  does the sender know  the MAC address of the computer with the IP address = 1.2.3.10 ?

A host (PC) sends an ARP packet on it's network (Ethernet) whenever it must send to an unknown MAC address.  It contains it's IP address and the desired destination IP address.  The packet is sent to the broadcast Ethernet address so all listeners hear the MAC address, and examine the packet for the IP address.  They then build a **table of MAC-IP address pairs**.  An ARP entry expires after 20 minutes.

Thus the table looks like:

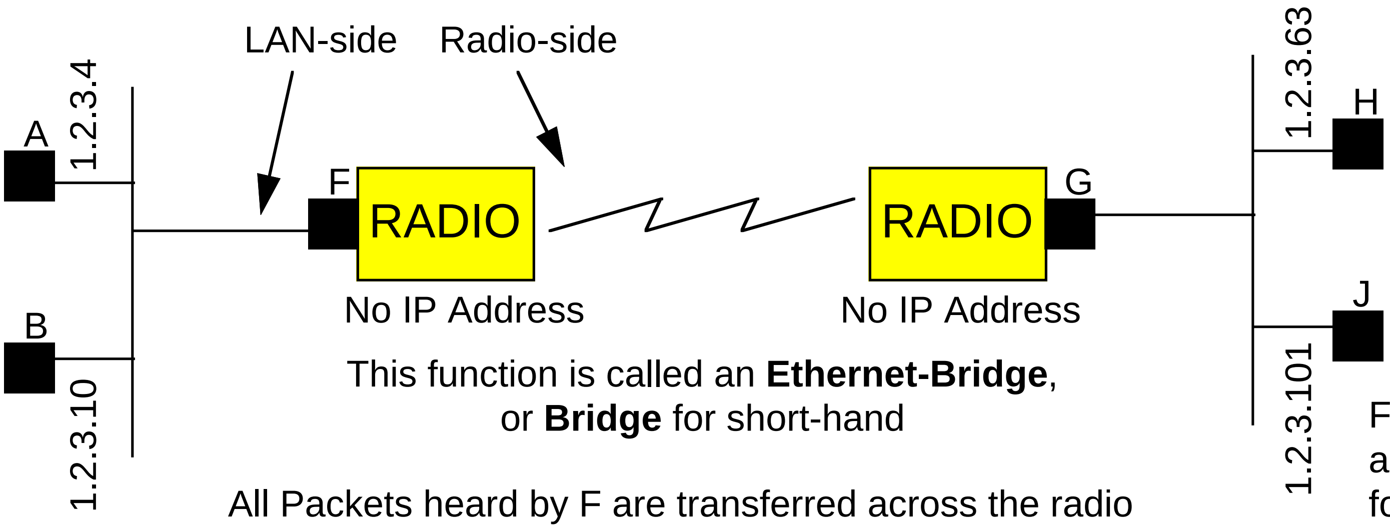
| IP Address | MAC address |
|---|---|
| 1.2.3.4 | A |
| 1.2.3.10 | B |
| 1.2.3.44 | C |



The **Gateway** responds to ARP packets for non-local-network requests. Any packet sent to a host not on this network is sent to the MAC address of the gateway, with the actual destination IP (not the IP of the gateway). The gateway then **forwards the packet** to the desired host, or another gateway that is closer to the destination IP address.

The **IP** address **does not change** from hop to hop.  The **MAC** address **does change** on every hop.

# How does the FHSS radio act as an ‘IP-extension cord’ ?



This function is called an **Ethernet-Bridge**,
or **Bridge** for short-hand

All Packets heard by F are transferred across the radio link and resent by G onto the other LAN (Subnet).

A better method is to have F and G each listen to their LAN side. F **learns** which MAC addresses are on the LAN, and which are across the radio link on the other side. Similarly, G **learns** this also.

Then F only transmits across the radio link only those packets that it knows are not on it’s side of the radio link. Broadcast packets are always transferred, of course.

This is call a **Filtering Bridge**, or an Intelligent Bridge

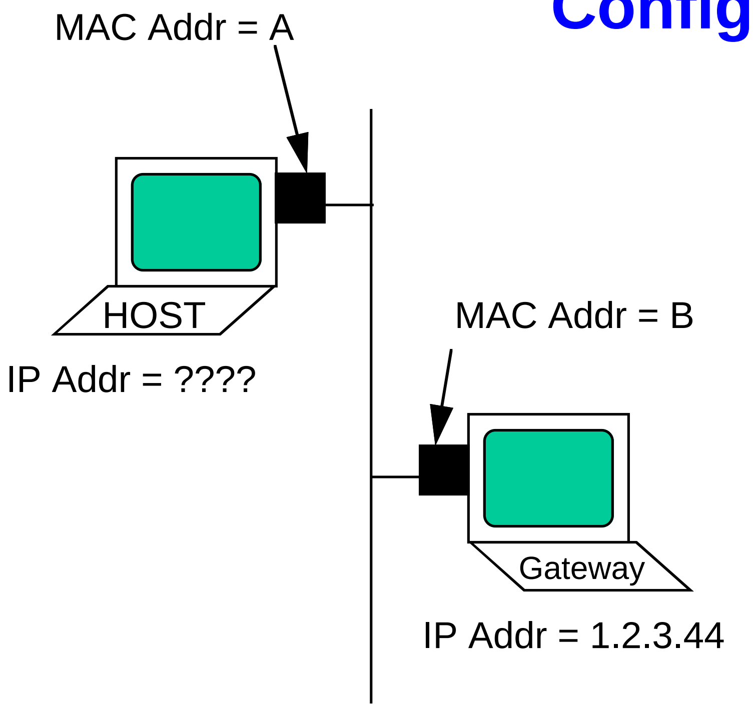
Example: A->B : is not transmitted
A->H: is transmitted

F & G do not participate in any ARP sessions. They forward all ARP packets since they are broadcast packets.

A and B see that F has a whole bunch of IP addresses, and enters all of them into it’s ARP table. This is called a Proxy ARP. Example: ARP table of left-hand hosts:

| IP Address | MAC Address |
|---|---|
| 1.2.3.4 | A |
| 1.2.3.10 | B |
| 1.2.3.63 | F |
| 1.2.3.101 | F |

# DHCP - Dynamic Host Configuration Protocol



1. Host sends a DHCP request to the **Ethernet broadcast address** FF:FF:FF:FF:FF:FF and to the **IP broadcast address** 255.255.255.255. It sends a request for any DHCP servers. HOST also includes it's MAC address A in the packet (client hardware address)
2. DHCP servers 'offer' their services. In this case gateway.
3. Host accepts one gateway's offer.
4. Gateway replies with a DHCP acknowledge to MAC-A from MAC-B, telling HOST what it's **new IP address** is, and how long the lease is good for. Also, DHCP tells HOST what the **router IP address** is, what the **server IP address** is, and the **name of the server**.
5. A MAC-level bridging FHSS radio must relay Ethernet frames sent to the broadcast address. If the FHSS radio also filters, then it must relay IP packets sent to the IP broadcast address and to the IP 'this' address (IP address with network field set to 0).
6. A device that forwards DHCP packets is called a **Relay Agent**. The Server (Gateway) can keep multiple requests through one Relay Agent organized since the client address of the actual requester is inside each DHCP packet.