Network Layer Protocols

802.*

ARP

Network layer Protocols (layer 3)

- There are many different network layer protocols
- Older protocols
  - SLIP – Serial Line Internet Protocol
  - PPP – Point to Point Protocol. IP connect 2 isolated routers.
- Some of the most common are the IEEE 802 suite of protocols
- There are many 802 protocols[1], although only two are widely used – **802.3 (Ethernet)** and **802.11 (Wireless)**

- 1 Most standards are developed well before widespread use, and so it is impossible to tell which ones will be widely used

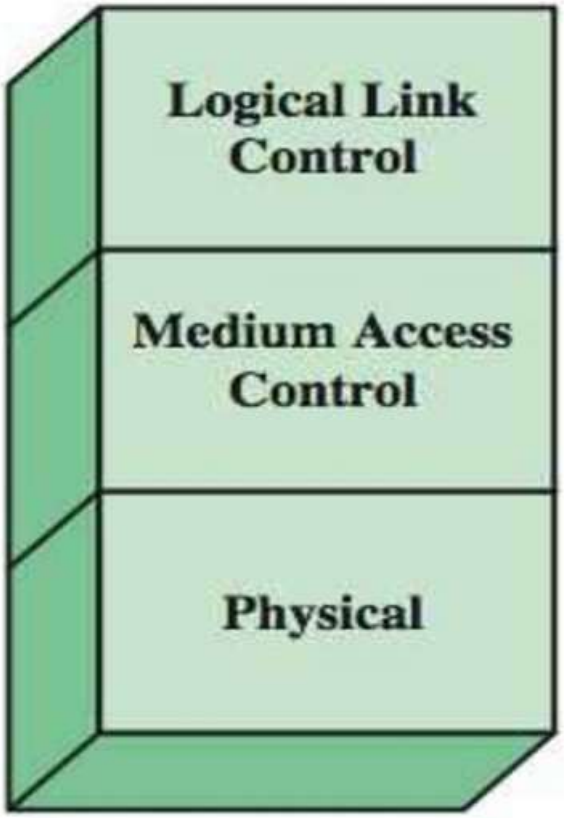
IEEE 802.* standards

802. –		Certification	Status
1.	Bridgeing and Network Management		
2.	Logical Link Layer	Ethernet	
3.	**Ethernet (CSMA/CD)**		
4.	Token Ring		(disbanded)
5.	MAC layer for Token Ring		(inactive)
6.	Metropolitan Area Network		(disbanded)
7.	Broadband LAN using Coax		(Disbanded)
8.	Fiber Optic		(disbanded)
9.	Integrated serices LAN		(disbanded)
10.	Interoperable LAN Security		(disbanded)
11.	**Wireless LAN and Mesh**	**WiFi + 5G WLAN**	
12.	Demand Priority		(disbanded)
13.	(not used)		
14.	Cable Modem		(disbanded)
15.	Wireless PAN		
	15.1 **Blue-tooth**	**Bluetooth**	
	15.4 **Zigbee (v low power) for IoT**	**Zigbee**	
16.	Wireless MAN (Broadband)	WiMAX	
	16e **Mobile Broadband Wireless Access**	**WiMAX1 + 4G**	
17.	Resilient Packt Ring		
24	Smartgrid	**Smart Grid**	

802 protocols

- The IEEE 802 protocols implement the bottom two layers of TCP/IP (Network and Physical layers) and actually comprise three layers (Network access is split into two parts)
  - Logical Link Control (802.2) – same for all 802 protocols
  - Medium Access Control
  - Physical

IEEE 802 Protocol Architecture



	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow control Error control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocols
Physical	Encoding/decoding of signals Bit transmission/ reception Transmission medium	Frequency band definition Wireless signal encoding

Functions of TCP/IP Network Access Layer

- Interfacing with the computer's network adapter.
- Coordinating the data transmission with the conventions of the appropriate access method.

Link Assembly

- Formatting the data into a unit called a frame and converting that frame into the stream of electrical or analog pulses that passes across the transmission medium.

Link Control

- Checking for errors in incoming frames.
- Adding error-checking information to outgoing frames so that the receiving computer can check the frame for errors.
- Acknowledging receipt of data frames and resending frames if acknowledgment is not received.

802 frame structure

Ethernet (802.3) Frame Format

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

802.3

For TCP/IP communications, the payload for a frame is a packet

WiFi (802.11) Frame Format

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

Formatting Data for transmission on the Physical Network

- Breaks IP layer data into smaller chunks, if necessary, which will be sent in the data field of the ethernet frames. The total size of the ethernet frame must be between 64 bytes and 1,518 bytes (not including the preamble).

- Package the chunks of data into frames. Each frame includes data as well as other information that the network adapters on the ethernet need to process the frame. An IEEE 802.3 ethernet frame includes the following:

(See next slides)

Ethernet Frame Components 1

- ***Preamble***: A sequence of bits used to mark the beginning of the frame (8 bytes, the last of which is the 1-byte Start Frame Delimiter).
- ***Recipient address***: The 6-byte (48-bit) physical address of the network adapter that is to receive the frame.
- ***Source address***: The 6-byte (48-bit) physical address of the network adapter that is sending the frame.
- ***Length***: A 2-byte (16-bit) field indicating the size of the data field.
- ***Data***: The data that is transmitted with the frame.

Ethernet Frame Components 2

- ***Frame Check Sequence (FCS):*** A 4-byte (32-bit) checksum value for the frame. The FCS is a common means of verifying data transmissions. The sending computer calculates a Cyclical Redundancy Check (CRC) value for the frame and encodes the CRC value in the frame. The receiving computer then recalculates the CRC and checks the FCS field to see whether the values match. If the values don't match, some data was lost or changed during transmission, in which case the frame is retransmitted.

- Passes the data frame to lower-level components corresponding to OSI's physical layer, which will convert the frame into a bitstream and send it over the transmission medium.

Some Important Protocols

DHCP – Dynamic Host Control Protcol

- Used by devices to obtain an IP address. Without an IP address a devices cannot access the internet
- An application layer protocol, but needed by the lower level protocols to “work out” IP addresses

ARP – Address Resolution Protocol

- Used to map logical IP addresses to physical MAC addresses on the local network
- A network layer protocol

ARP

- Within a single network where devices are directly connected, either by Ethernet or wireless, each device can communicate with another by means of the device MAC (Media Access Control) address.

- The MAC address can be thought of as the unique hardware identifier code of any network device. It is a 48 bit (6 byte) code, normally written byte at a time in hexadecimal, separated by colons, eg D0:D2:B0:D4:3A:9B

- The ethernet address is an example of a MAC address.

Use of MAC on single Network

- The allocation of MAC addresses to device manufactures is controlled by the IEEE via standard EU-48. There are 2^{48} or about 10^{15} available, which was originally forecast to last until 2080.(There is a replacement standard EU-64 which specifies 64 bit MAC addresses, but this have not been used yet)

- However to be able to communicate over the internet, a device needs an internet (or IP) address

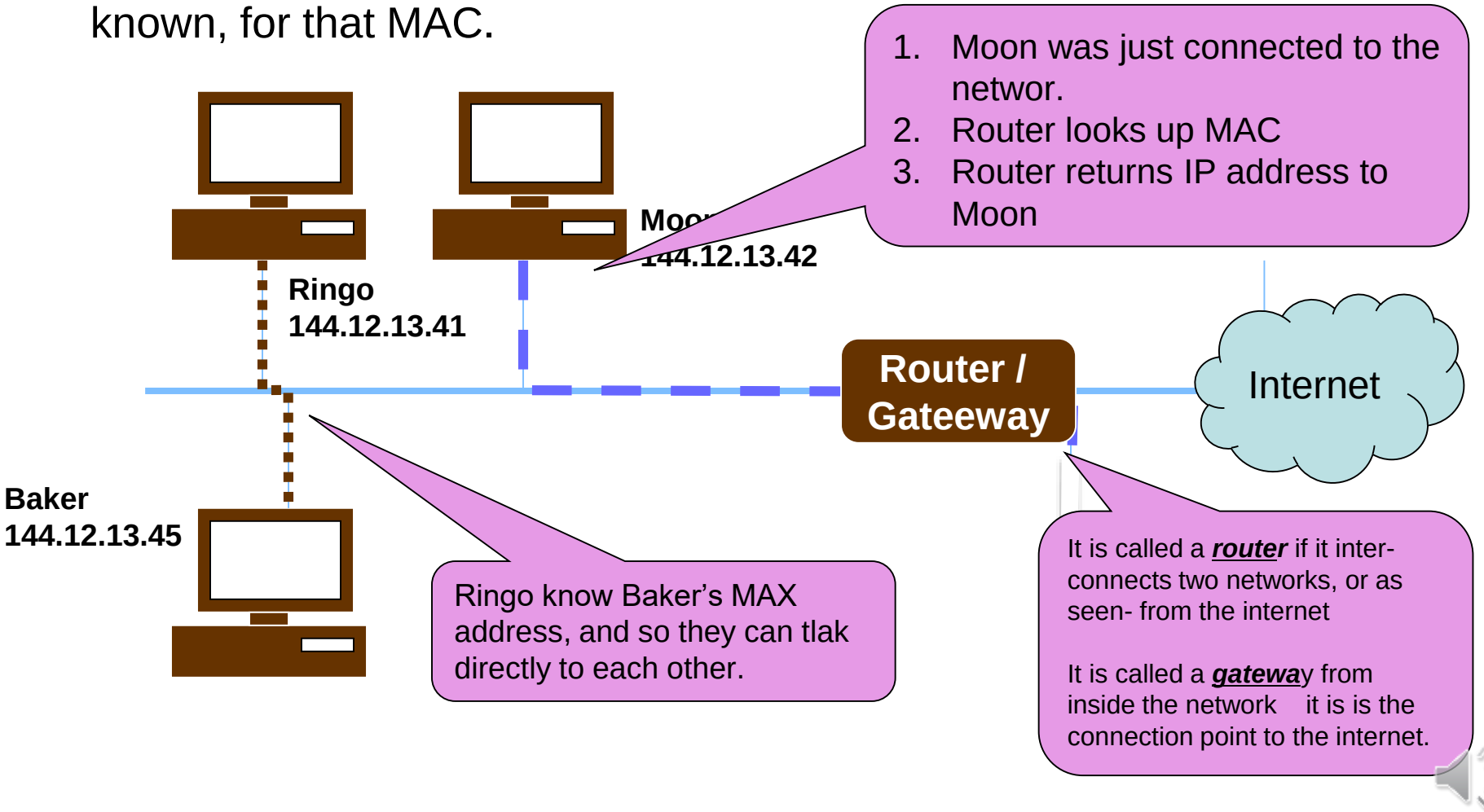
Types of ARP Messages

- Note that two different types of messages are used:
  - ***Broadcast*** – sent to all devices on the network
    - A broadcast message uses a MAC address of FF:FF:FF:FF:FF
  - ***Unicast*** – A message sent to a **single device**

- Each device on the local net builds up at table of IP addresses and corresponding IP addresses

Using ARP to discover IP

- When a machine initially connects to a LAN, it can broadcast an ARP "who am I ?" message. The router gets the MAC from this message, looks it up in its internal tables, and replies with the IP number if known, for that MAC.



Internetworking

- To discover the IP address of another device on the same network, a device uses the ARP protocol, which can be thought of as sitting between the internet (3) and network (2) layers

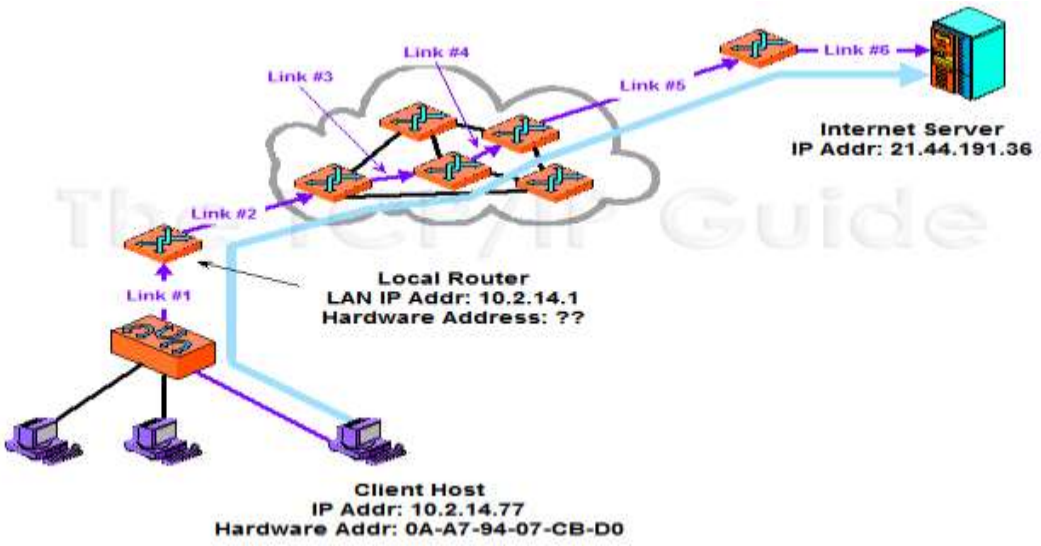
- Note that this is nothing to do with the allocation of IP addresses which is generally done by an application layer (4) protocol called DHCP

Router to Router

- At higher levels packets travel across the internet from one IP address to another. At these levels there is routing information to direct packets along sequence of routers designated by IP addresses.

- In reality, packets are traveling from one router to another. To go from one router to the next, the sending router needs to know the MAC address of the next router it needs to send the message to.

The need for ARP protocol



Router IP 10.2.14.77 needs to send data to router IP 10.2.14.1, but doesn't know its MAC address

ARP

- Watch youtube video Address Resolution Protocol (ARP) Explained

- https://www.youtube.com/watch?v=xTOyZ6TWQdM

The link is also in this weeks Canvas recommended readings