SIEMENS

Connected Manufacturing

Ethernet 101

usa.siemens.com/industry

Why Ethernet

Ethernet is Everywhere!

Bob Metcalfe's 1973 sketch of his origional "ethernet" vision
Image provided courtesy of Palo Alto Research Center Inc., a Xerox Company

SIEMENS

Ethernet is everywhere

• Ethernet is the most common computer networking medium

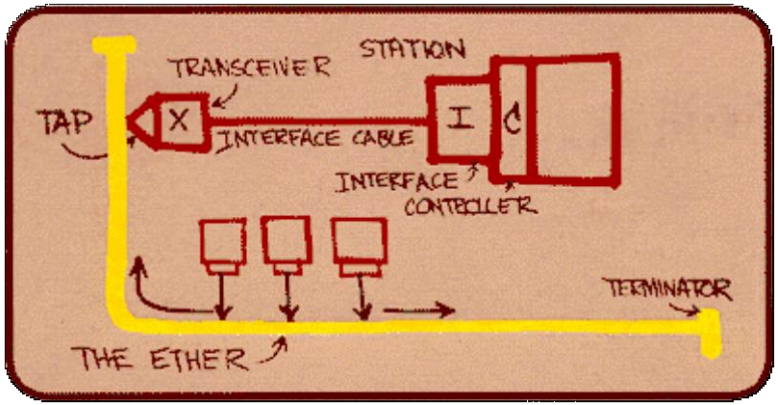
•Standardization on this technology has created some of the easiest ways to connect devices.

•Ethernet has been developed to be flexible, powerful, and easy to implement

•Many manufactures have field bus technologies that are Ethernet based

Ethernet - Origins

- Ethernet is a network specification that was published in 1975 by the XEROX company



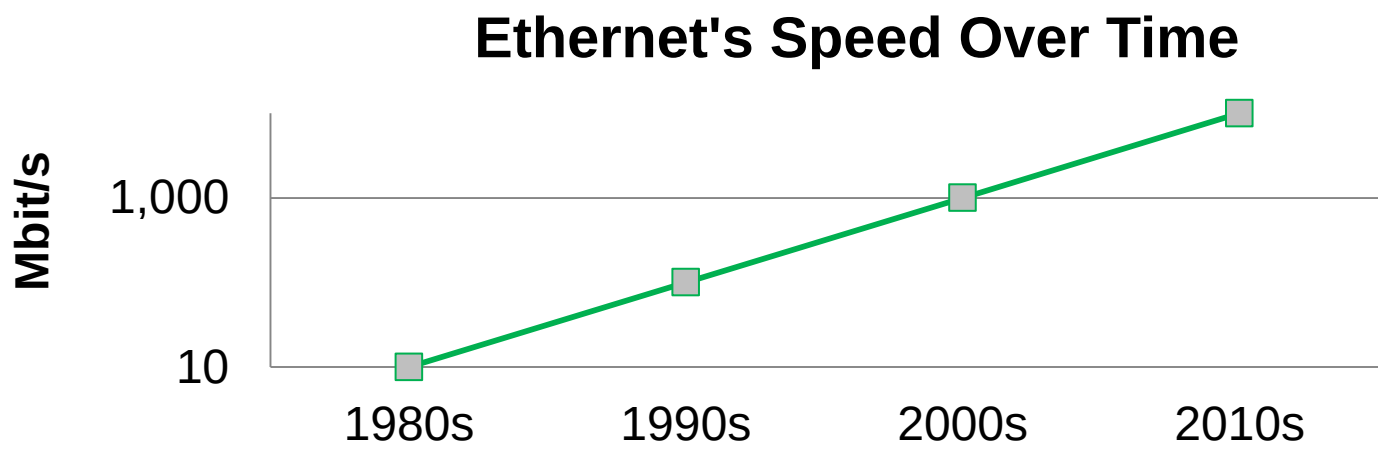
Sketch by Bob Metcalfe, who was active in the Xerox Palo Alto Research Center (PARC) in the early '70s.

- Ethernet version 1 was further developed from 1980 onwards by the IEEE (Institute of Electrical and Electronics Engineers) in workgroup 802.

Ethernet – Standardization IEEE802.3

- IEEE created the Ethernet specification
- Created a competitive market where innovation thrived
- Ethernet's capabilities have evolved to meet the ever increasing demand

IEEE 802.3 is the Ethernet Standard



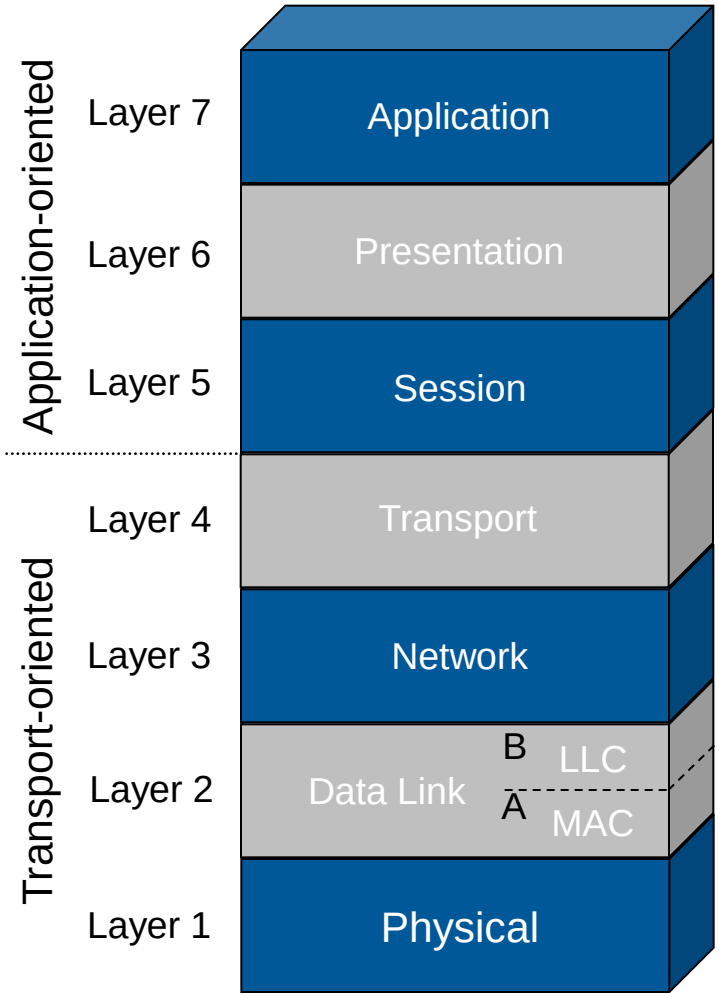
Standards

There are two important standards that define Ethernet.

IEEE 802.3 – This is the Ethernet standard that is concerned about the transport and physical medium of the network.

IEC 7498-1 - This is the **ISO/OSI 7 layer model**, it defines both the transport oriented part of Ethernet as well as the Application oriented parts. **It includes IEEE 802.3**

The OSI 7 Layer Reference Model



OSI

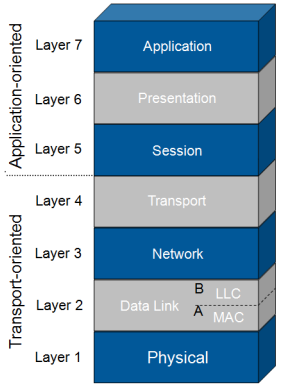
Open Systems Interconnection

Defines a 7 layer model of how communication functions are logically layered

These layers include IEEE 802.3

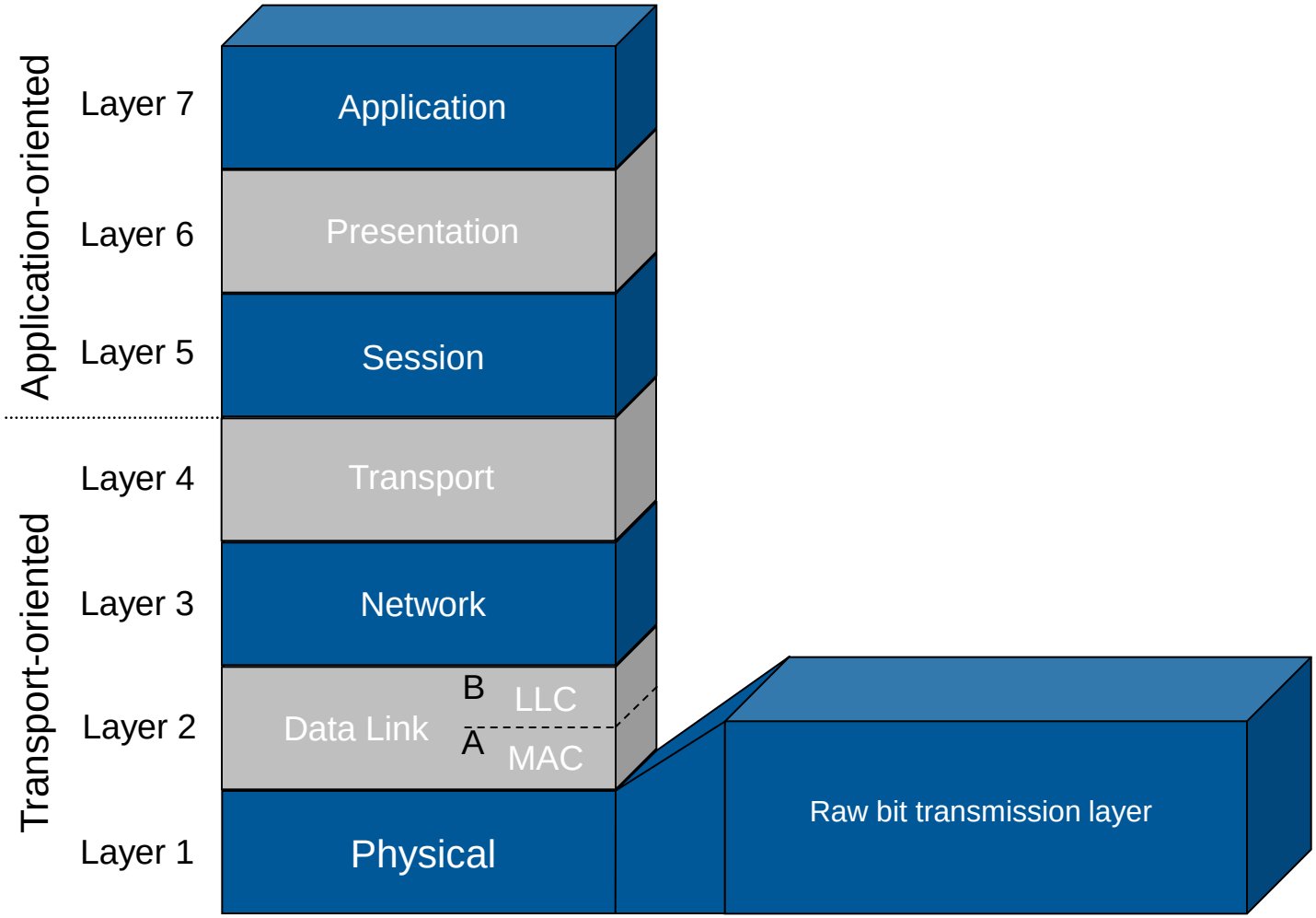
Defined by IEEE 802.3

Ethernet 101



During this presentation, the OSI seven layer model will show what layer we are discussing

The Physical Layer (Layer 1)



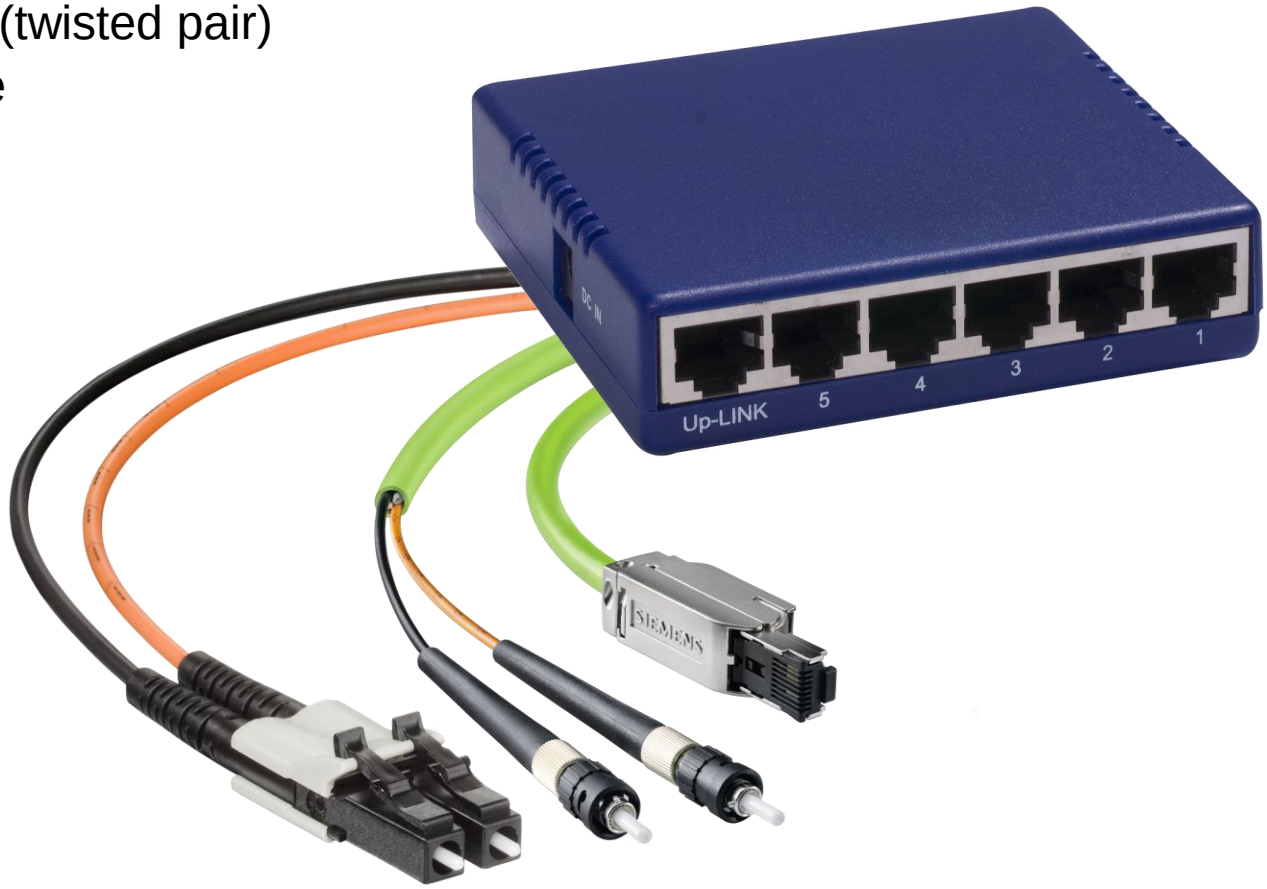
The Physical Layer (Layer 1)

This is the hardware associate with creating the network.

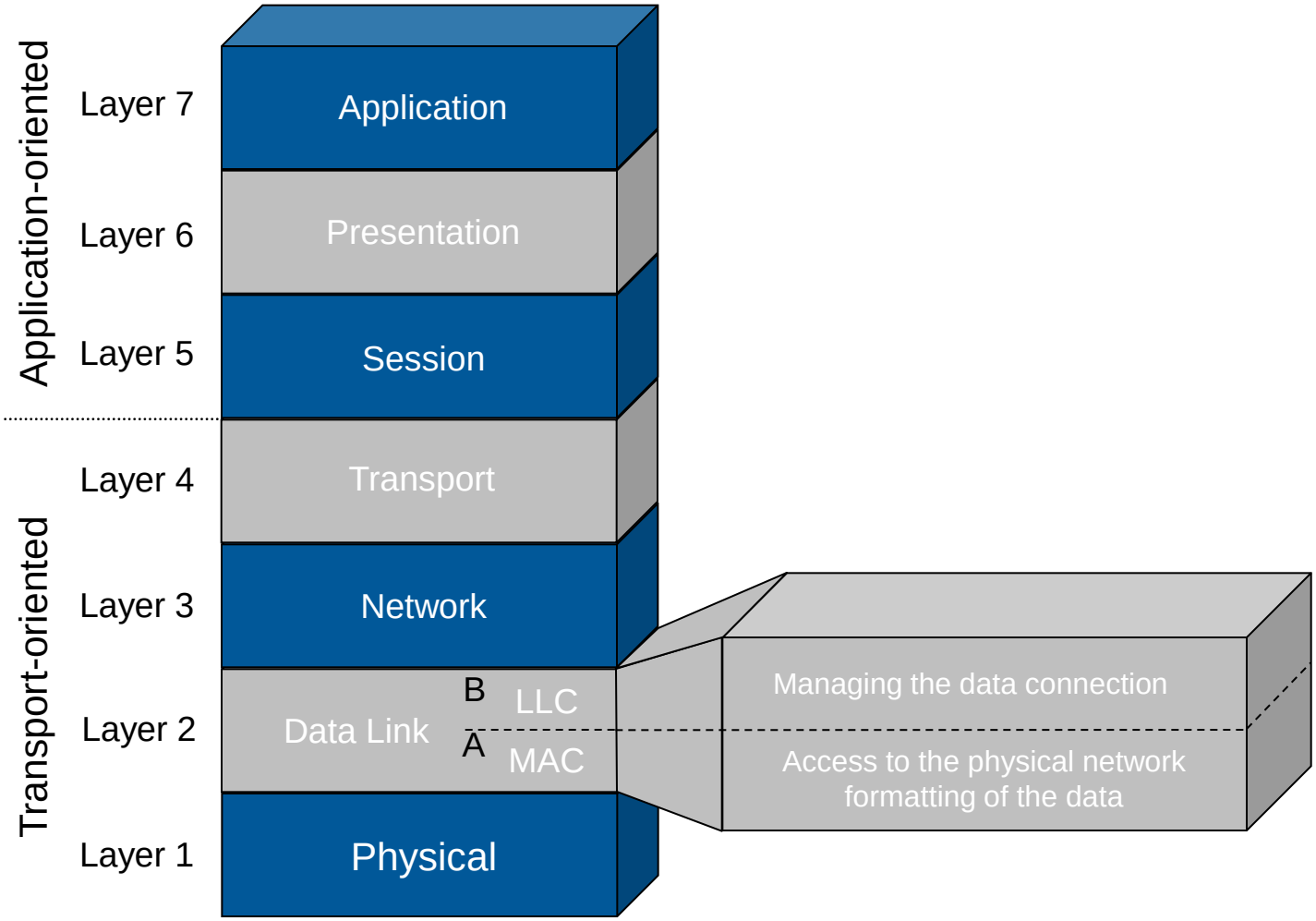
Copper wiring such as
- CAT-5 cable (twisted pair)
- Coaxial cable

Fiber-optic cable
- Glass
- Plastic

Network devices
- Hubs
- Repeaters

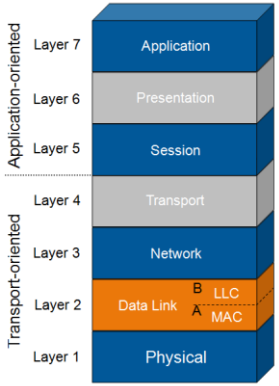


The Data Link Layer (Layer 2)



The Data Link Layer (Layer 2)

- Each device in the local area network has a unique address
- Handles datagram (message frames) transport between devices within the local area network
- The Data Link Layer is divided into two parts
  - MAC – Layer 2a - Media Access Control
  - LLC – Layer 2b - Logical Link Control



Did you know?

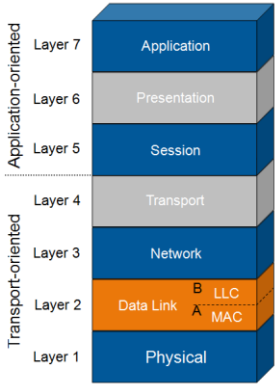
The Ethernet specification (IEEE 802) includes layer 1 and 2a of the ISO/OSI reference model

Media Access Control (MAC)

- Protocol layer for the Physical Layer

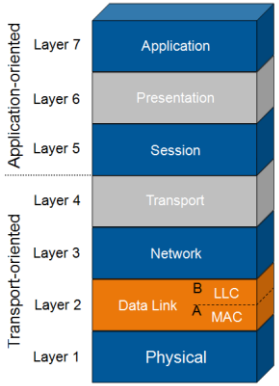
- Specifies that each network device will have a unique address
  - **MAC address** – 6 byte address

- Provides the following communication services
  - **Unicast**
  - **Multicast**
  - **Broadcast**



Media Access Control (MAC) Address

MAC address (hexadecimal)	Vendor
00-50-8b-xx-xx-xx	Compaq
00-07-E9-xx-xx-xx	Intel
08-00-06-xx-xx-xx	**SIEMENS**
00-60-2F-xx-xx-xx	Cisco
00-15-F2-xx-xx-xx	Asus



The **MAC address** (Media Access Control address) is a unique hardware address of every single network adapter and is used to **uniquely identify** each device.

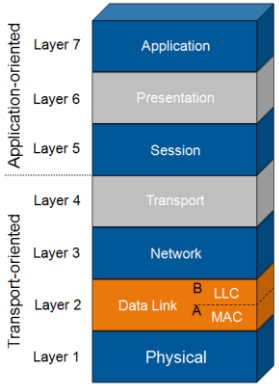
Did you know?

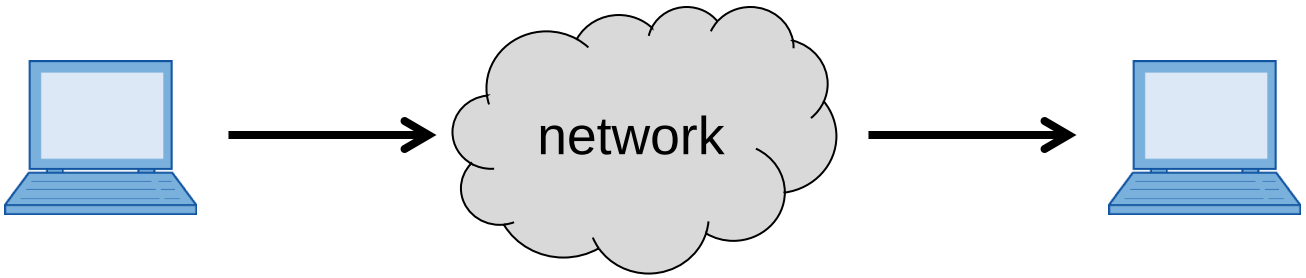
Each manufacturer has a range of MAC addresses. You can determine which company made the device just by looking at its MAC address

Unicast, Broadcast, Multicast

Unicast - one host sends to one client

- + The data only travels to the specified client
- + Lower overall network traffic
- + Works very well with wireless networks

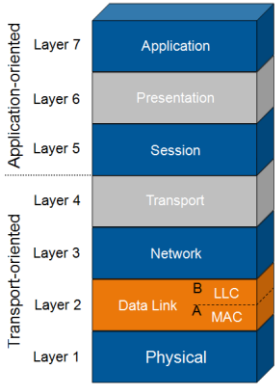


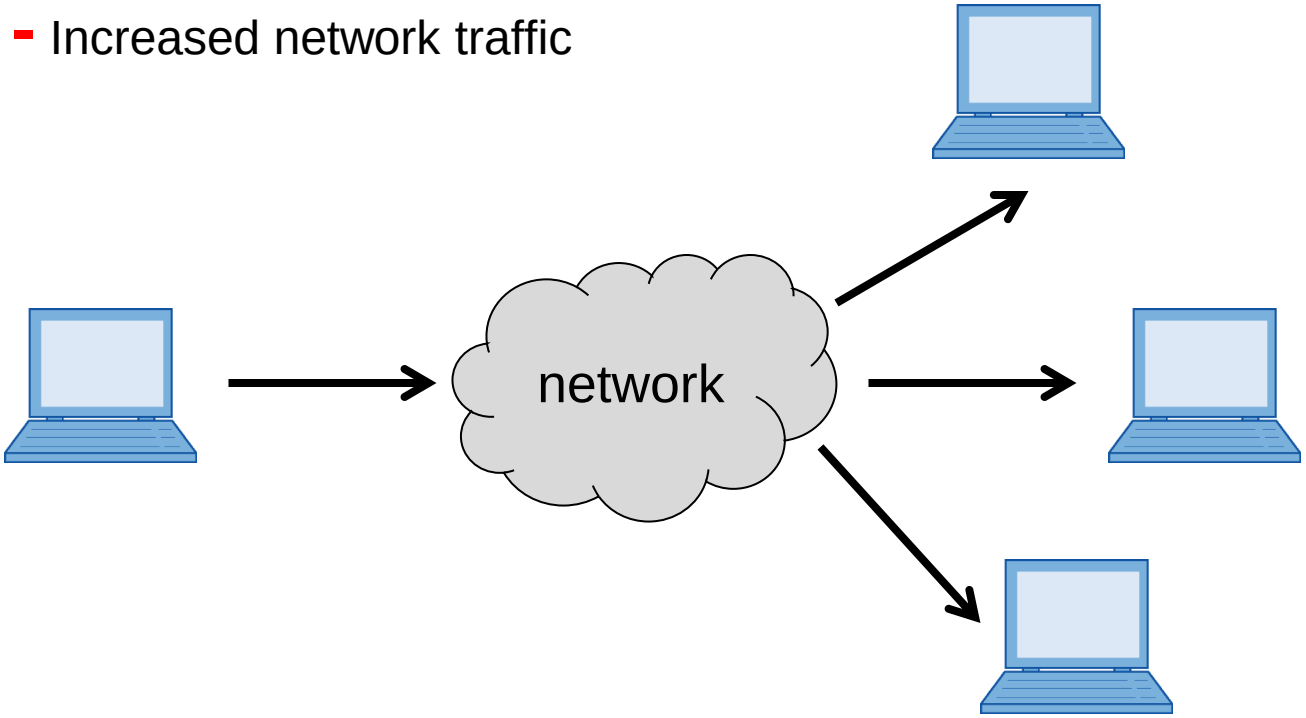


Unicast, Broadcast, Multicast

Broadcast - one host sends to multiple clients

+ Easy to send data to multiple clients
- Data is sent to all clients weather they need it or not
- Increased network traffic

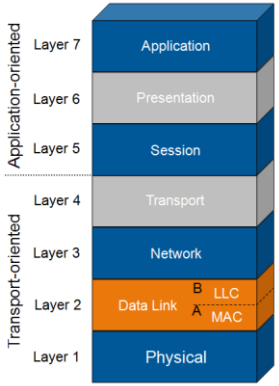


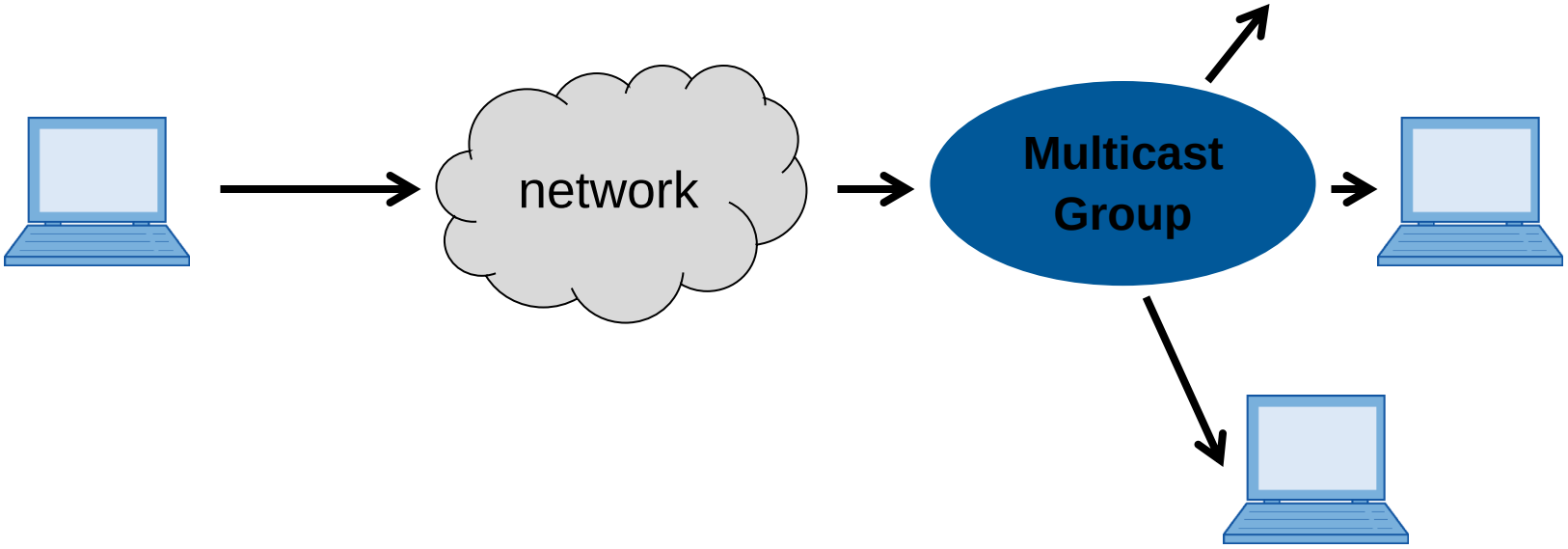


Unicast, Broadcast, Multicast

Multicast - one host sends to a group of clients

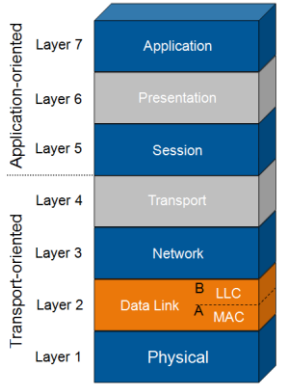
+ Easy to send data to multiple clients
- Data is sent to all client weather they need it or not
- Increased network traffic
- Clients must subscribe to the multicast group



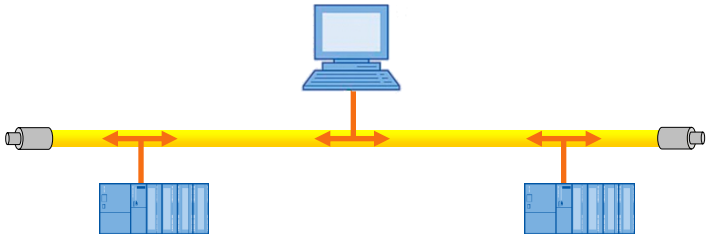


Shared Media Ethernet

Shared Media Ethernet consists of a network connecting multiple devices via a single cable or a network hub



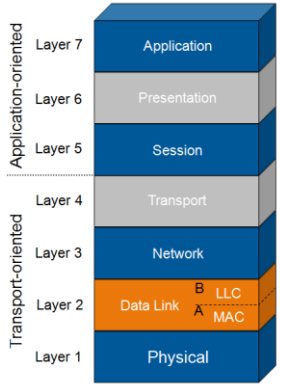
Shared Media



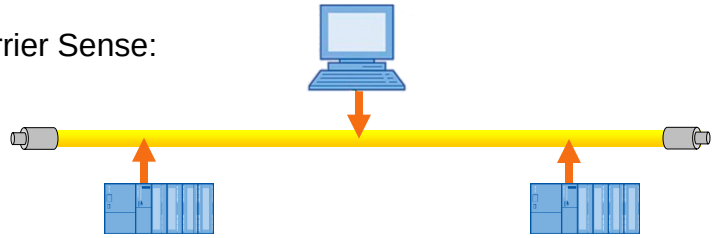
- Devices share the same physical network

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

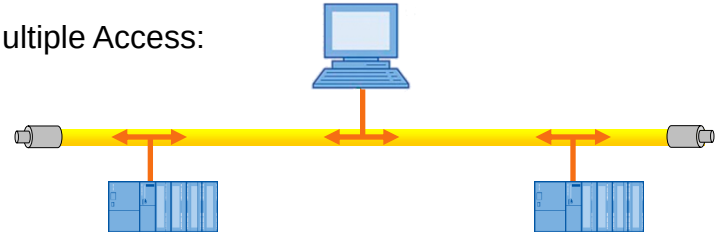
Carrier Sense Multiple Access/Collision Detection (CSMA/CD)



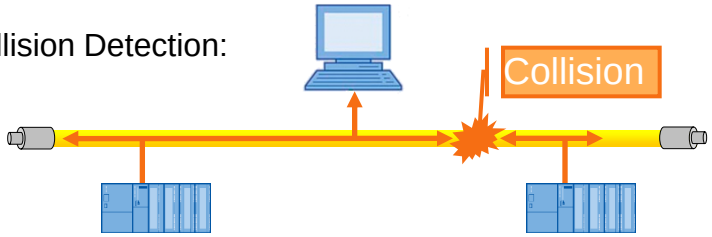
1st step – CS Carrier Sense:



2nd step – MA Multiple Access:



3rd step – CD Collision Detection:

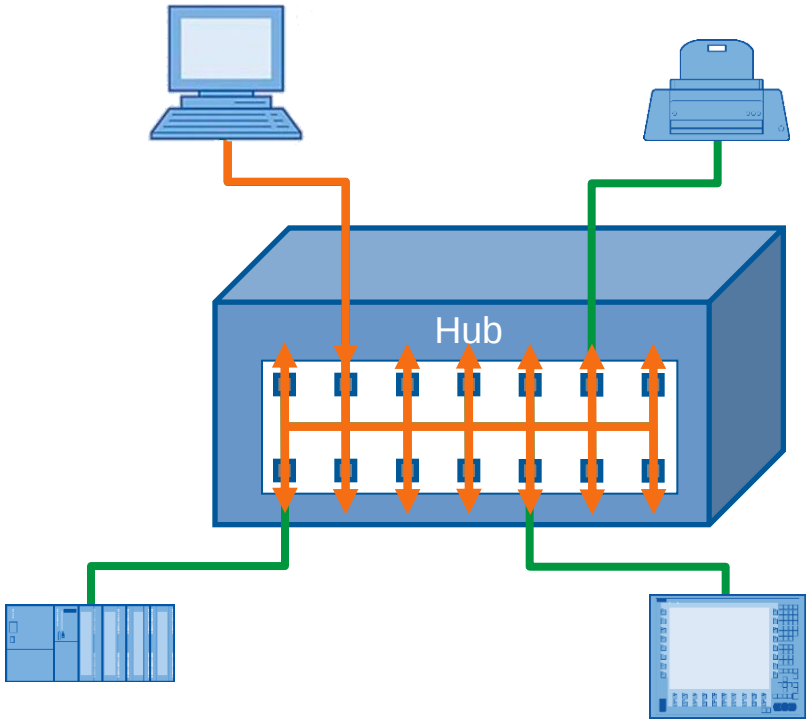


Dinner Table Analogy

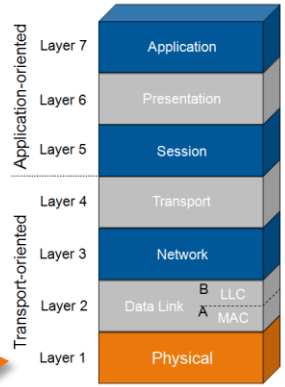
Before speaking, each guest waits for the current speaker to finish talking. If two guest start talking at the same time, both stop and wait for random periods of time before trying to speak again

Ethernet Hub

- **forward frames to all ports**.
- leads **to increased bus load**
- Allows for **data collisions**.



Hubs function at Layer 1

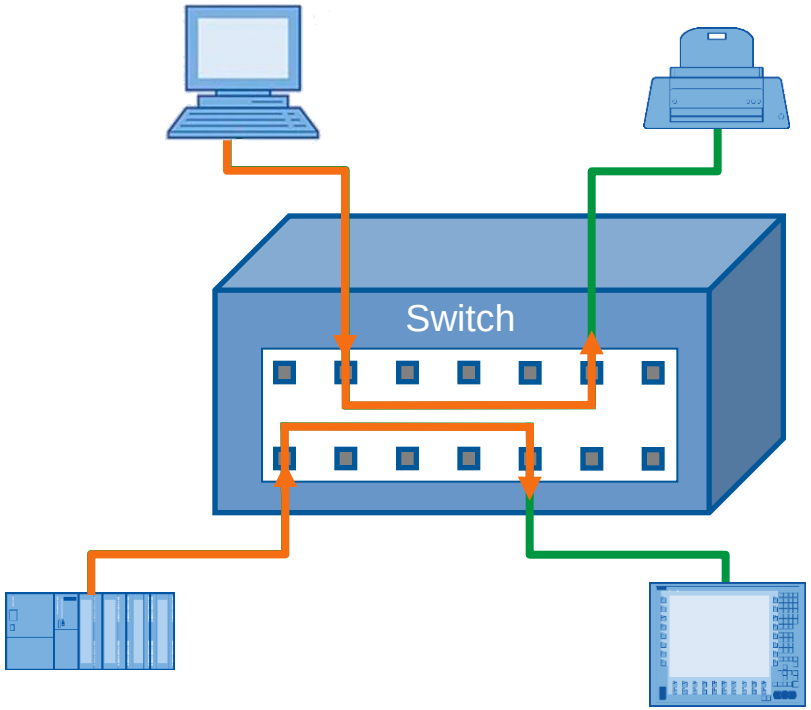


Did you know?

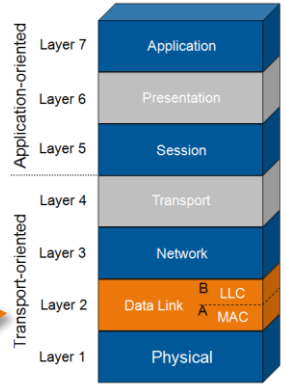
Only one node can communicate at a time on a hub. All nodes must share the available bandwidth.

Ethernet Switch

- Eliminates the need for CSMA/CD
- Eliminates the possibility of data collisions
- Increases overall network throughput



Switches function at Layer 2



Did you know?

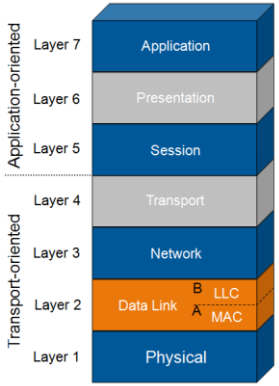
Switches eliminate data collisions and provide the full bandwidth of the port to each node

Also, several nodes can communicate at the same time

Ethernet Switch types

Unmanaged Switched

- They have **no configuration** options
- They usually have **no interface**

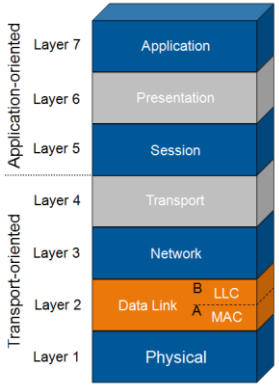


Managed

- Include all the functionality of the unmanaged switch
- Usually includes an interface such as a built in web server
- Usually includes **higher level configuration options** to better help control network traffic
- Usually **includes diagnostics** functions

Ethernet switch port function – Auto-negotiation

Most switches today provide **auto-negotiation** for each of their ports.



Auto-negotiation

- The switch can determine things about each device connected at its ports such as
  - **Speed**
  - **Duplex mode**
  - **Flow control**

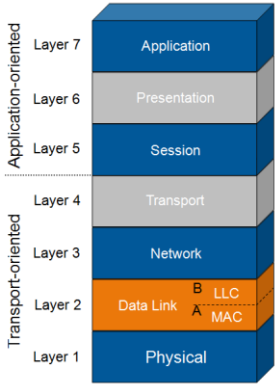
Did you know?

In most cases you should leave the switch set to auto negotiate and it will determine the highest performance transmission mode.

Ethernet Switch transmission modes

Ethernet switches can communicate using two different transmission modes

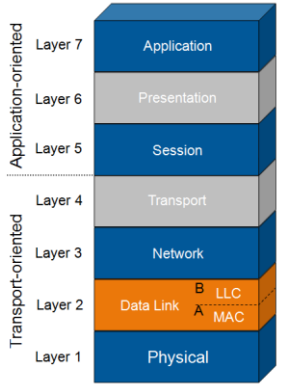
- **Half duplex (HX)**
- **Full duplex (DX)**

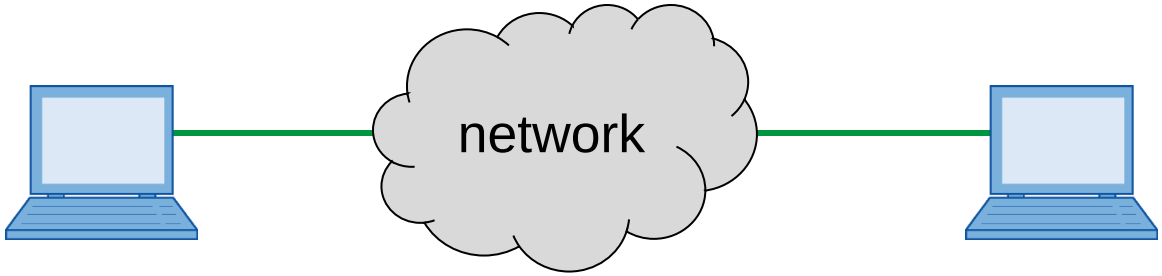


Half Duplex

Half duplex (HX):

- **Two channels** are available for transmission
- Data can only be transmitted **alternately** on each channel
  not at the same time
- Devices operate in "**alternating mode**".

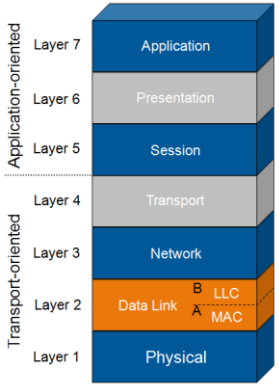


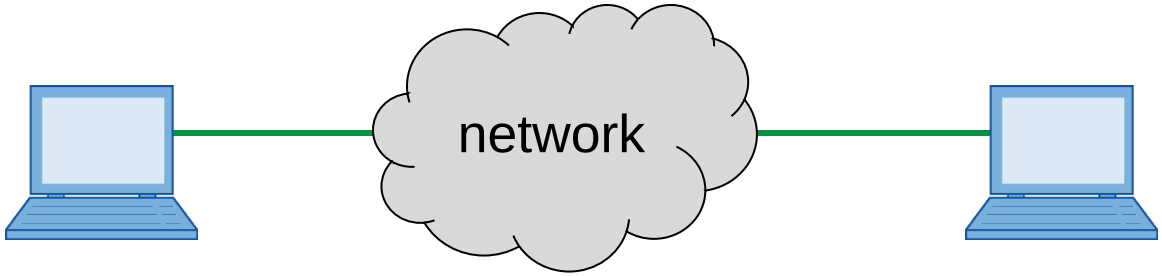


Full Duplex

Full duplex (DX):

- Data can be transmitted via both channels simultaneously





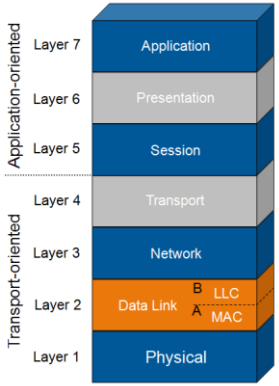
Did you know?

Using half duplex can have a huge negative impact on the network performance

Ethernet switch port function – Auto-sensing

SIEMENS

Most switches today provide Auto-sensing for each of their ports



Auto-sensing (Auto Crossing)

- The switch can determine which type of Ethernet implementation to use (MDI , MDIX)

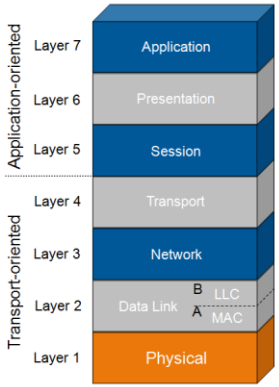
- This means that you can *use* either type of cable without concern
  - **straight through**
  - **crossover**

Did you know?

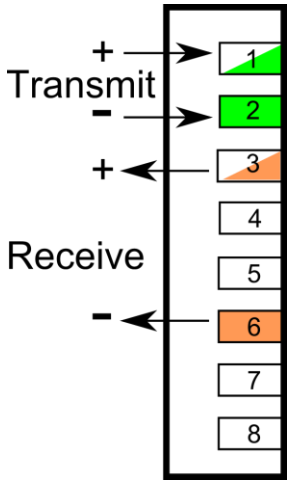
In most cases you should leave the switch set to auto sensing mode and it will determine the proper MDI/MDIX mode automatically

MDI - MDIX

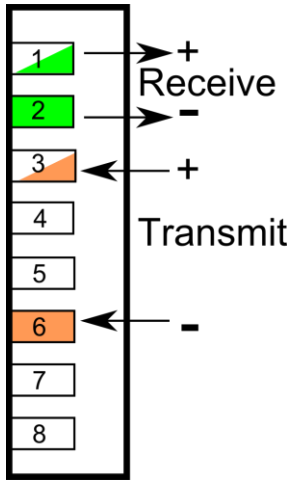
There are two different implementations of the Ethernet adapter for twisted pair.



MDI - Medium Dependent Interface

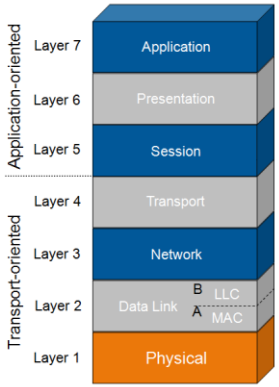


MDIX - Medium Dependent Interface Crossover

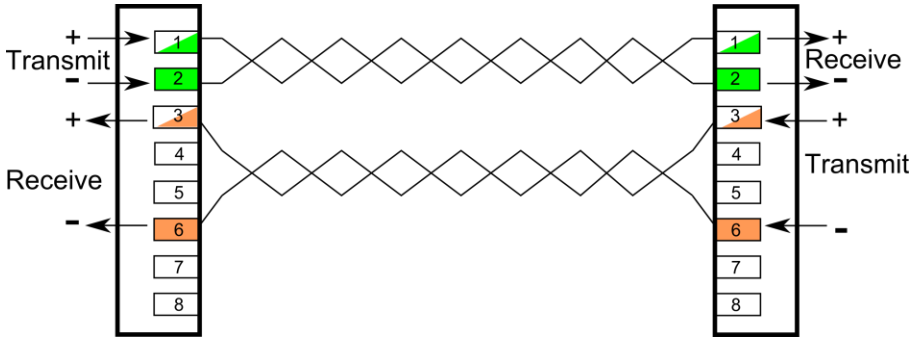


Straight through and crossover cables

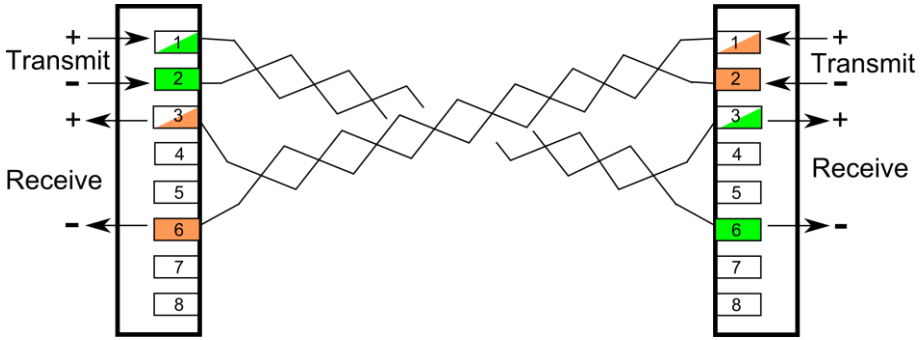
There are two types of Ethernet (over twisted pair) cables



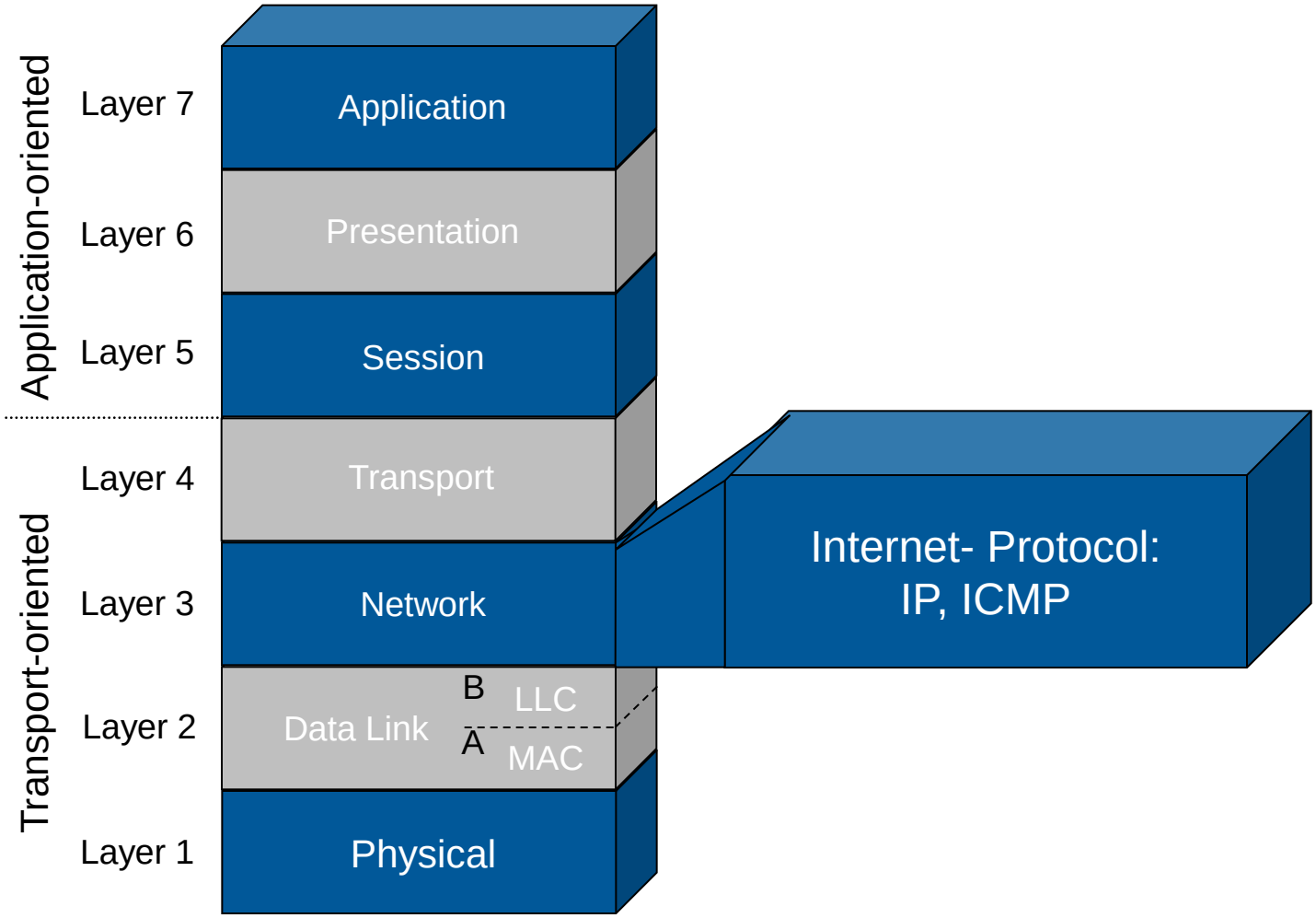
- **Straight through**



- **Crossover**

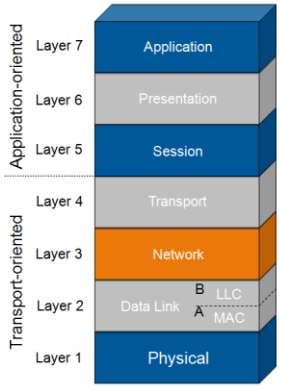


The Network Layer (Layer 3)



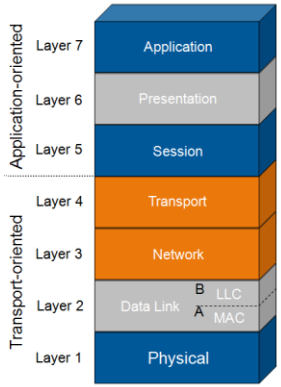
Characteristics of the Network Layer

- IP is connectionless and works without acknowledgement.
- Data packages could be received in a different order than were sent.
- The most important declaration is the IP address.



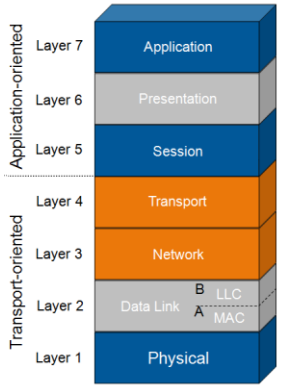
What is TCP/IP?

- TCP/IP is a network protocol
- It is the basic protocol for many applications which are communicating across network segments.
- It contains:
  - **TCP**: Transmission Control Protocol, for secure transport of data
  - **IP**: Internet Protocol, to send data across network segments



Connectionless: User Datagram Protocol (UDP)

- Compared to TCP, UDP is connectionless
- Unsure reception because there is no acknowledgment upon receipt of data.
- UDP is used for:
  - Simple datagram service or
  - as simple Transport, if higher protocols provide
    - error and consistency check (i.e. SNMP)



Did you know?

UDP is like using a Walkie-Talkie

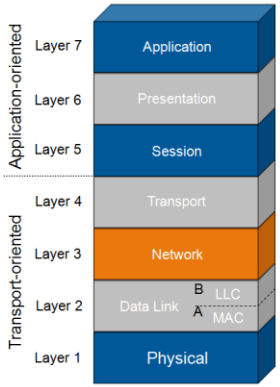
TCP is like using a Telephone

TCP vs. UDP

	TCP	UDP
Messages automatically resent if partner does not receive	✸	
One message can be broadcast to several partners		✸
Can determine if partner is connected	✸	
Has checksum with recovery	✸	
Has sequence checking	✸	
Used for time critical applications		✸

The IP Address (IPV4)

- Every device on a network has an IP address
- The IP address is like the street address of your home
- The IP address is formatted as 4 numbers separated by periods
  Example: 192.168.1.144



- NOTE: IPV4 uses 32bit addressing which allows for about 4.3 billion addresses.

Subnet Mask (IPV4)

The IP Address actually contains two useful pieces of information

1. The **local network ID** that the device belongs too
2. The **unique local address** of the device

The Subnet mask defines

- How many bits are used for the local network ID
- The remaining bits of the IP address are used for the local address of the device

Example

IP Address: 192.168.1.144

Subnet Mask: 255.255.255.0

IP address and subnet mask example (IPV4)

Example #1

IP Address: 192.168.1.144

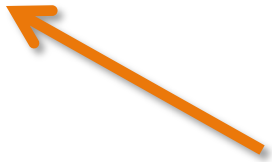
Subnet Mask: 255.255.255.0

IP address and subnet mask example (IPV4)

Example #1

IP Address: 192.168.1.144

Subnet Mask: **255.255.255**.0



The subnet mask 255.255.255.0

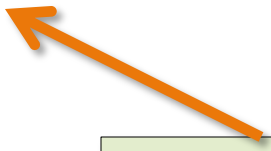
Indicates that all of the bits of the first 3 bytes of the IP address indicate what **local network ID** the device is a member of

IP address and subnet mask example (IPV4)

Example #1

IP Address: **192.168.1**.144

Subnet Mask: 255.255.255.0



This means the device is on the 192.168.1.xxx local network

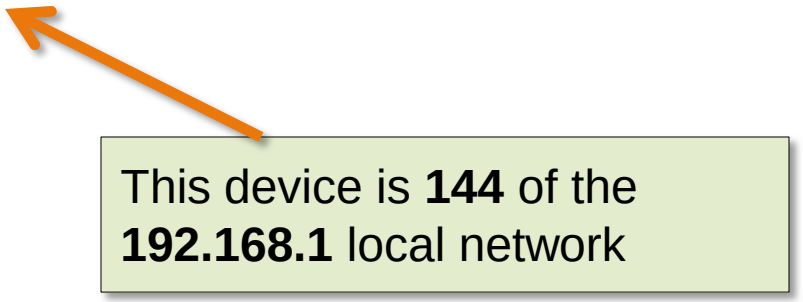
It can communicate with other devices that are also part of the 192.168.1.xxx local network

IP address and subnet mask example (IPV4)

Example #1

IP Address: 192.168.1.**144**

Subnet Mask: 255.255.255.0

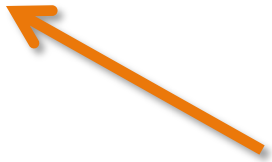


IP address and subnet mask example (IPV4)

Example #2

IP Address: **192.168**.1.144

Subnet Mask: **255.255**.0.0



The subnet mask 255.255.0.0

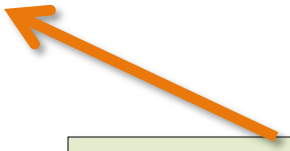
Indicates that all of the bits of the first 2 bytes of the IP address indicate the **local network ID** 192.168

IP address and subnet mask example (IPV4)

Example #2

IP Address: 192.168.**1.144**

Subnet Mask: 255.255.0.0



This unique local address of the device is **1.144**

The local address now is 2 bytes long

Did you know?

The subnet mask allows you to control the number of devices that can be a part of the local network

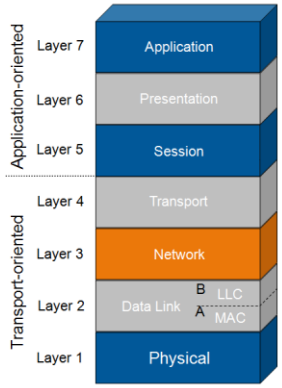
What is IPV6

Internet Protocol version 6

- Newest version of the IP address specification
- Addresses future issue where we would run out of IPV4 addresses
- Uses 128 bit addressing
  - This allows for 2^{128} or $3.4 * 10^{38}$ addresses

IPV6 Example:

- **2001:0db8:85a3:0042:1000:8a2e:0370:7334**

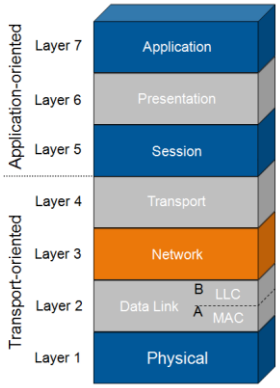


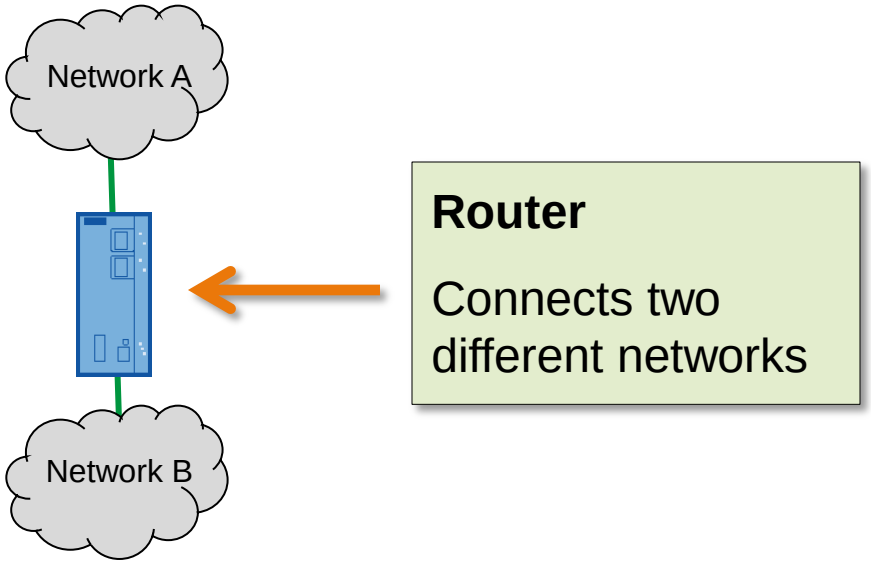
Did you know?

Most local networks will not need to change to use IPV6 addresses in the near future

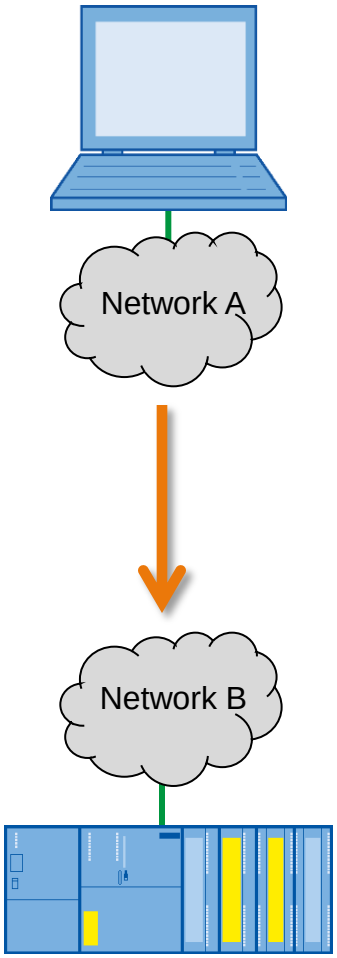
Routers

- Used to connects two different networks or subnet together





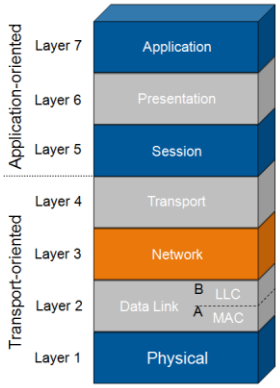
Router example



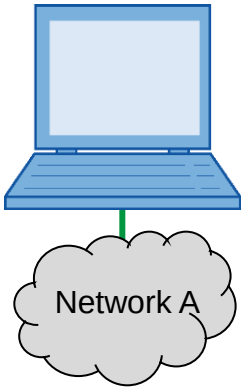
192. 168. 1. 144
255. 255. 255. 0

192. 200. 1. 28
255. 255. 255. 0

A laptop in network A wants to talk to a PLC in network B

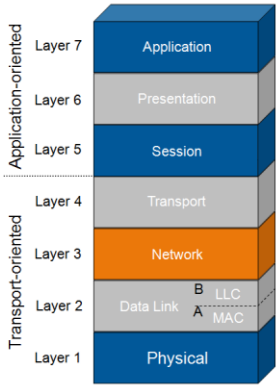


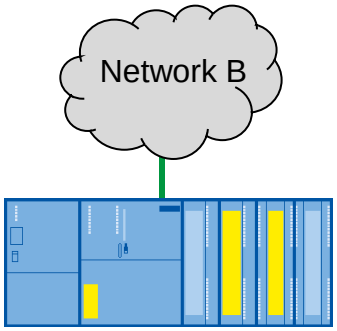
Router example



192. 168. 1. 144
255. 255. 255. 0

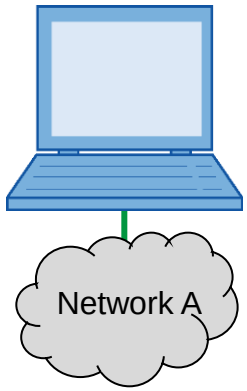
The laptop is a member of the 192.168.1.xxx subnet



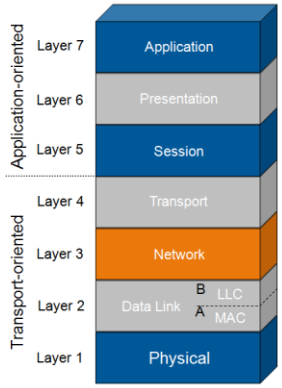


192. 200. 1. 28
255. 255. 255. 0

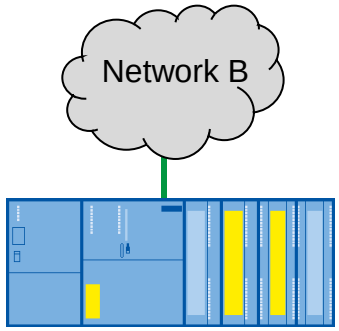
Router example



192. 168. 1. 144
255. 255. 255. 0

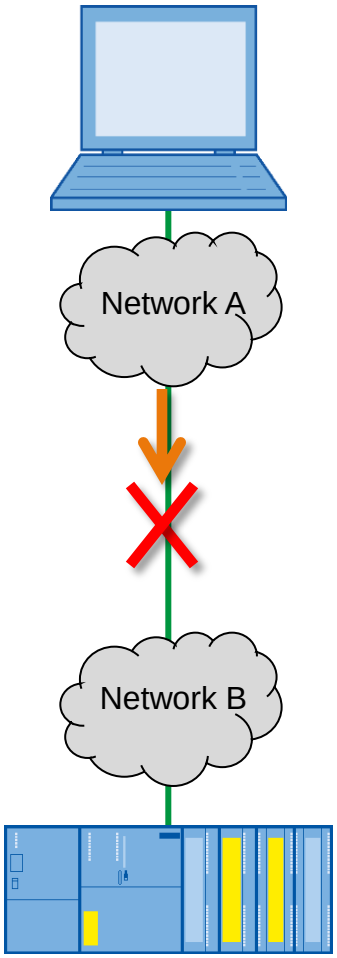


The PLC is a member of the 192.200.1.xxx subnet



192. 200. 1. 28
255. 255. 255. 0

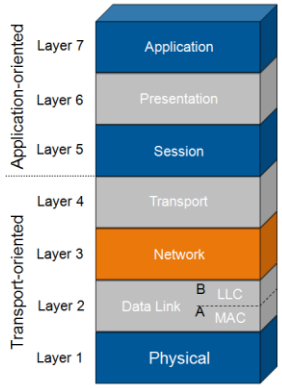
Router example



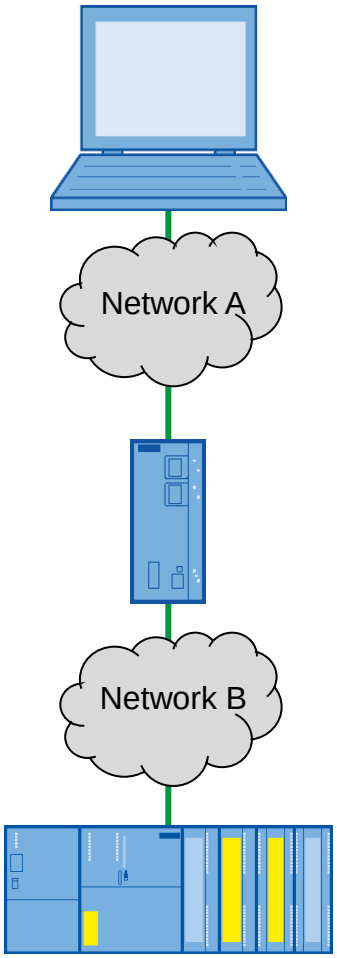
192. 168. 1. 144
255. 255. 255. 0

192. 200. 1. 28
255. 255. 255. 0

Connecting the two networks together does not solve the problem. The device addresses and subnet masks still separate the network traffic



Router example



192. 168. 1. 144
255. 255. 255. 0

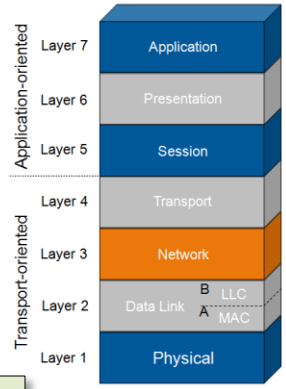
192. 168. 1. 1 (Gateway)

192. 168. 1. 1
255. 255. 255. 0

192. 200. 1. 1
255.255. 255. 0

192. 200. 1. 28
255. 255. 255. 0

192. 200. 1. 1 (Router)



Adding a router and configuring it properly will allow the device in network A and network B to talk

SIEMENS

Why Ethernet for Automation networks?

- Ethernet's proven track record make it a sounds choice for Automation field buses now and for the future

- Due to its open specifications it is
  - Widely available and understood
  - Reliable
  - Cost Effective
  - Will be around for a long time

- Multiple transmission mediums available for different applications
  - Copper
  - Fiber
  - Wireless

Nathan Schiavo – Wesco Portland

Nathan Schiavo

Wesco Portland

Application Specialist

503-734-5062

nschiavo@wesco.com

Answers for industry.