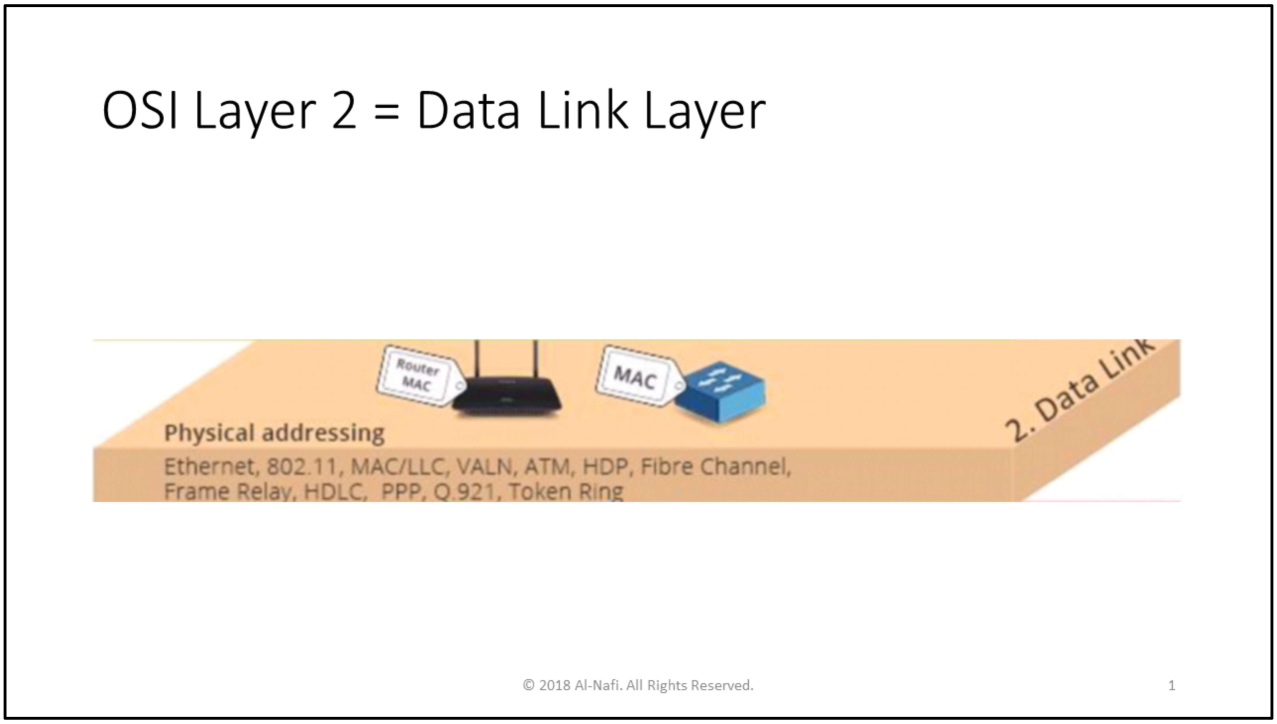


OSI Layer 2 = Data Link Layer

Router
MAC
MAC
2. Data Link

Physical addressing

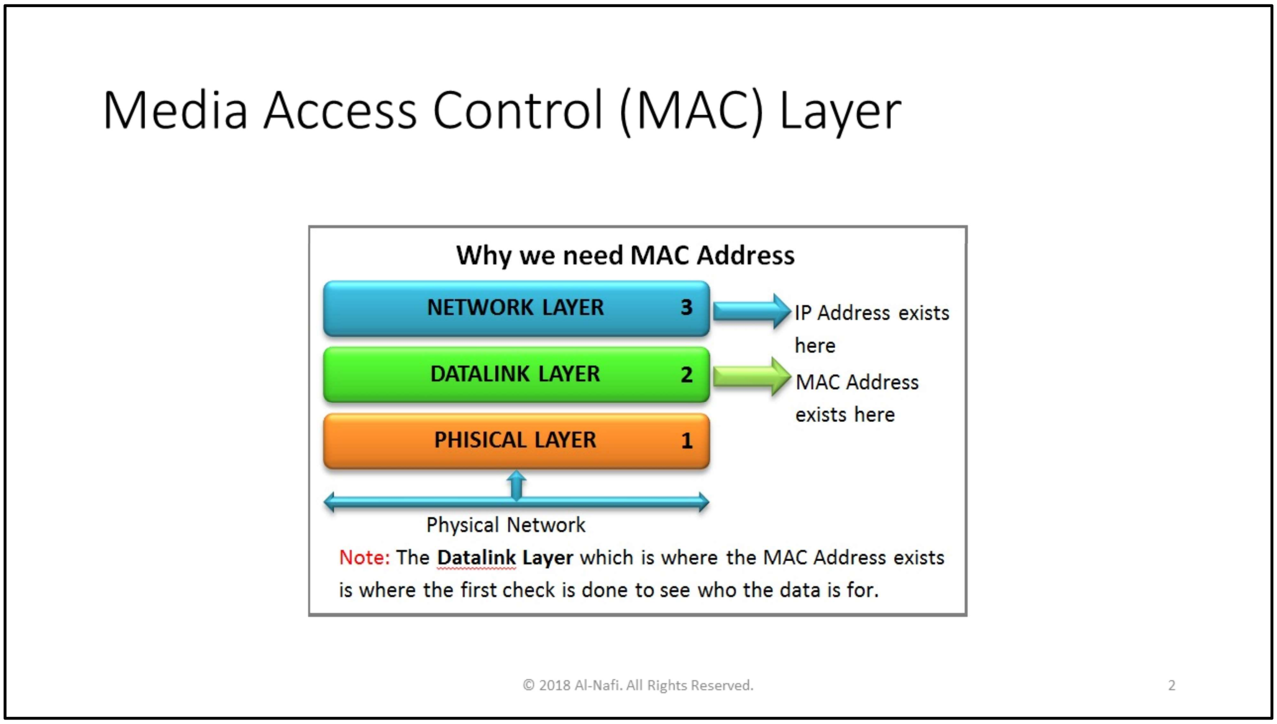
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring

The data-link layer prepares the packet that it receives from the network layer to be transmitted as frames on the network. This layer ensures that the information that it exchanges with its peers is error-free. If the data-link layer detects an error in a frame, it will request that its peer resend that frame. The data-link layer converts information from

the higher layers into bits in the format that is expected for each networking technology, such as Ethernet, Token Ring, etc. Using hardware addresses, this layer transmits frames to devices that are physically connected only.

There are two sub layers within the data-link layer:

- Media Access Control (MAC) Layer
- Logical Link Control (LLC) Layer



Media Access Control (MAC) Layer

Why we need MAC Address

NETWORK LAYER **3** → IP Address exists here

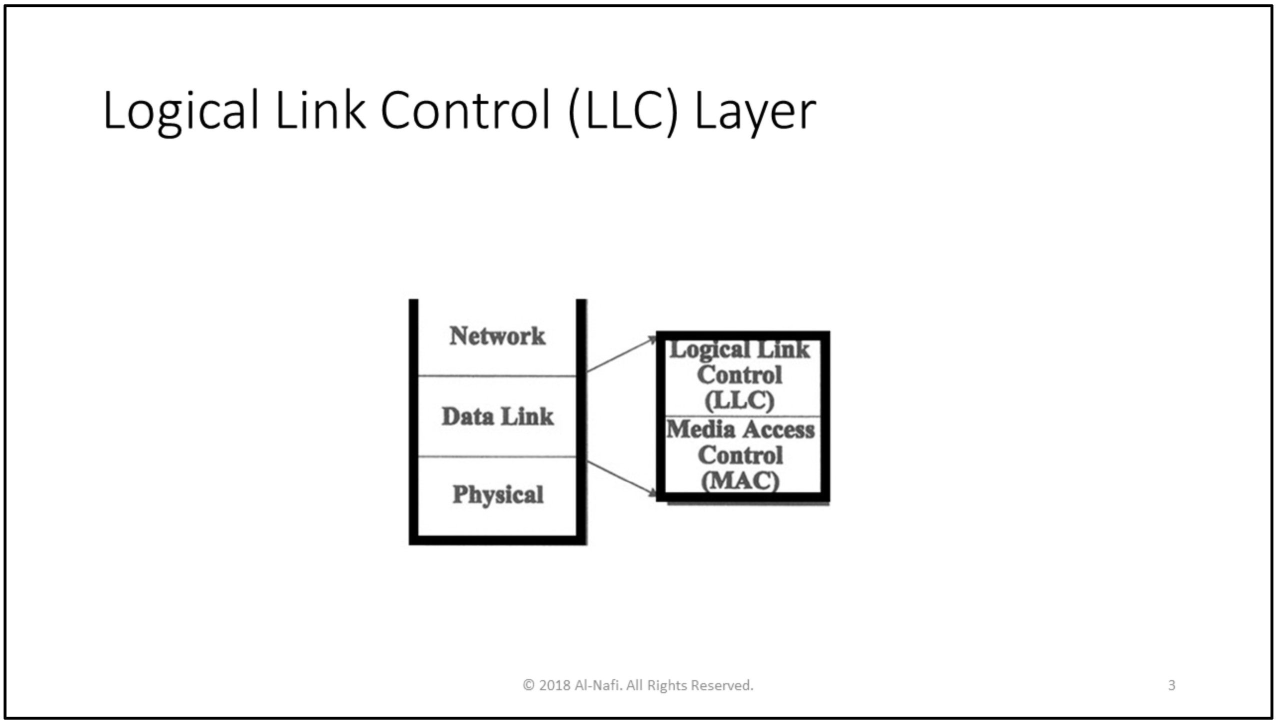
DATALINK LAYER **2** → MAC Address exists here

PHISICAL LAYER **1**

Physical Network

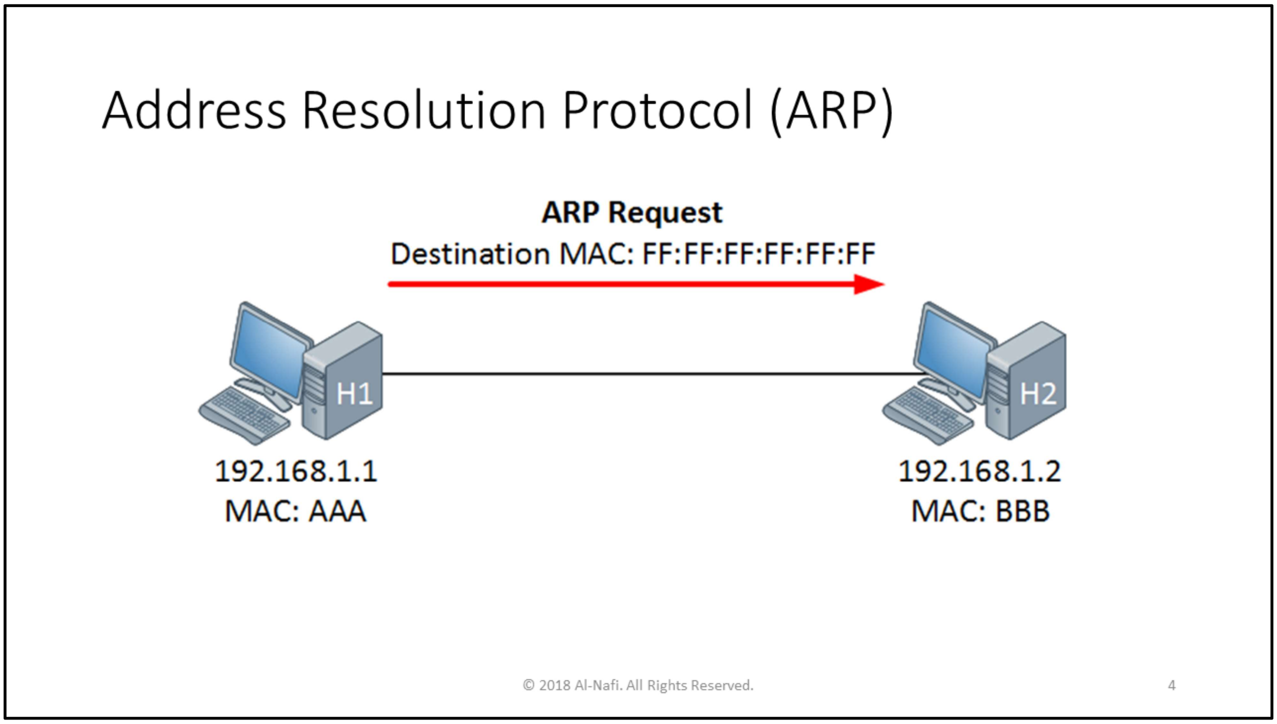
Note: The **Datalink Layer** which is where the MAC Address exists is where the first check is done to see who the data is for.

At this layer, a 48-bit (12-digit hexadecimal) address is defined that represents the physical address “burned-in” or chemically etched into each Network Interface Card (NIC). The first three
octets (MM:MM:MM or MM-MM-MM) are the ID number of the hardware manufacturer. Manufacturer ID numbers are assigned by the Institute of Electrical and Electronics Engineers (IEEE). The last three octets (SS:SS:SS or SS-SS-SS) make up the serial number for the device that is assigned by the manufacturer. The Ethernet and ATM technologies supported on devices use the MAC-48 address space. IPv6 uses the EUI-64 address space.



Logical Link Control (LLC) Layer

This layer is concerned with sending frames to the next link on a local area network.



Address Resolution Protocol (ARP)

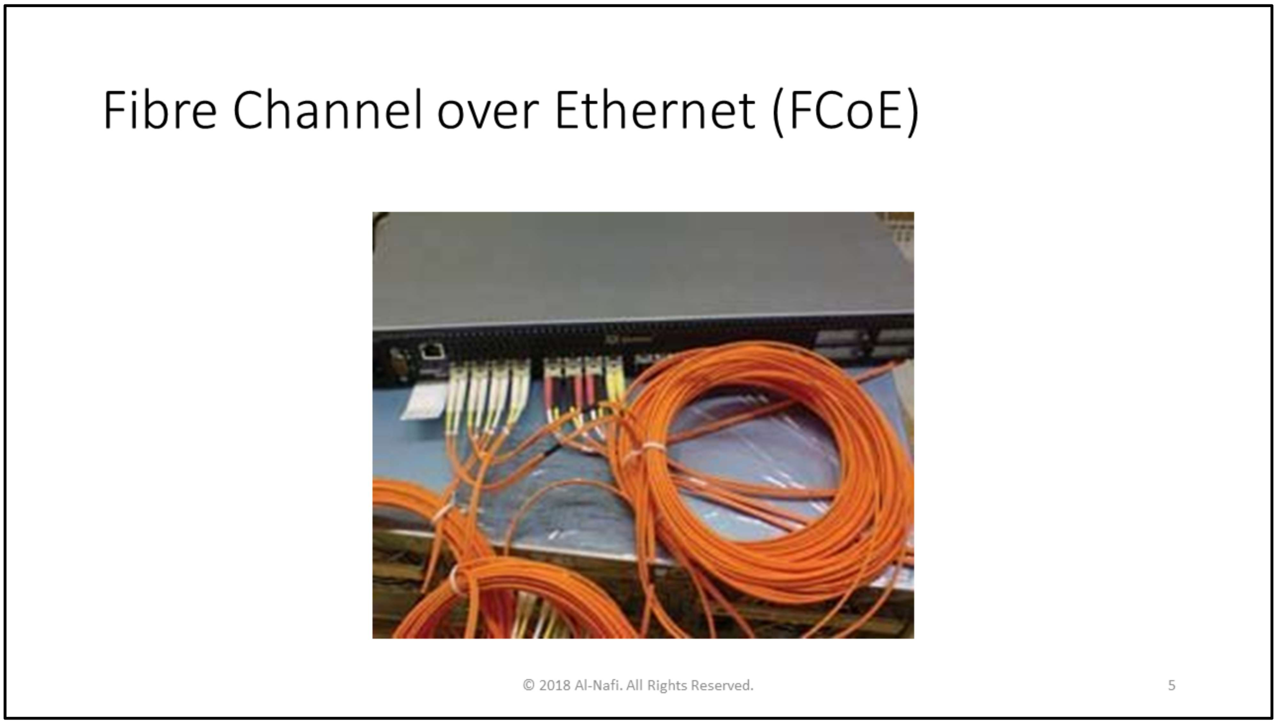
ARP Request

Destination MAC: FF:FF:FF:FF:FF:FF

192.168.1.1
MAC: AAA

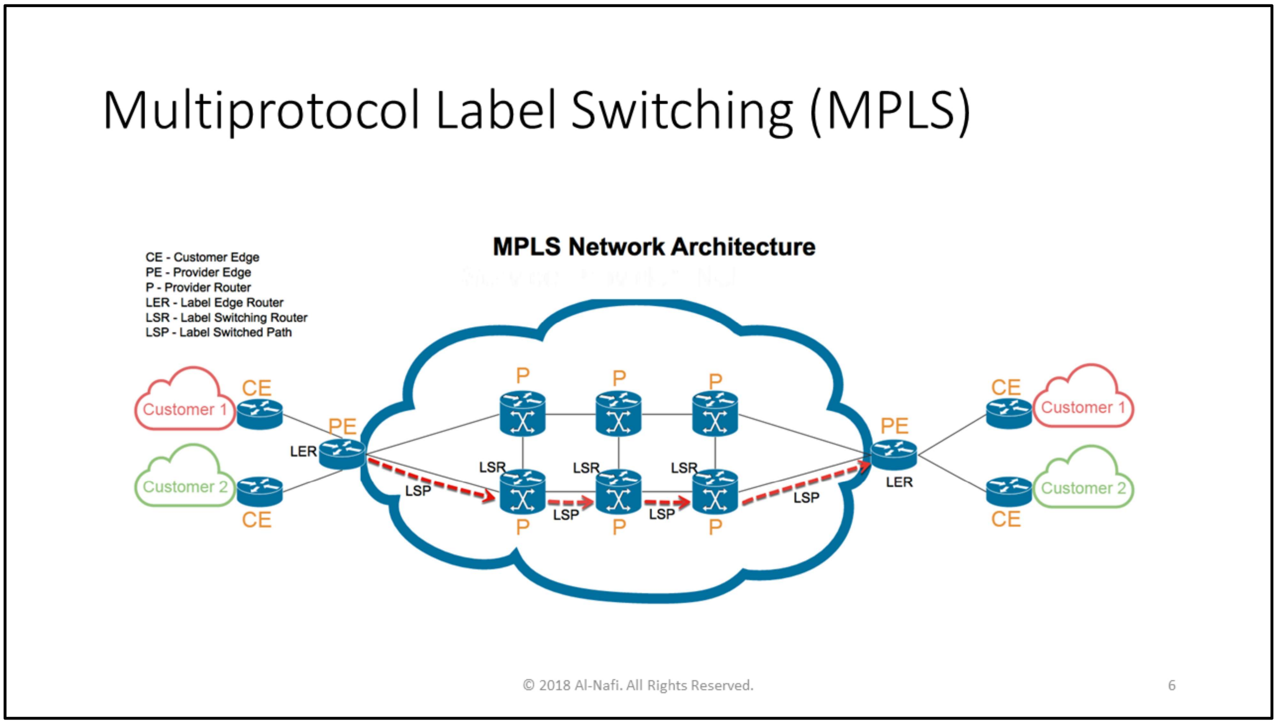
192.168.1.2
MAC: BBB

Address Resolution Protocol (ARP) is used at the MAC layer to provide for direct communication between two devices within the same LAN segment. Sending devices will resolve IP addresses to MAC addresses of target devices to communicate.



Fibre Channel over Ethernet (FCoE)

Fibre Channel is a high-speed serial interface using either optical or electrical connections (i.e., the physical layer) at data rates currently up to 2Gbits/s with a growth path to 10Gbits/s. FCoE is a lightweight encapsulation protocol and lacks the reliable data transport of the TCP layer. Therefore, FCoE must operate on DCB-enabled Ethernet and use lossless traffic classes to prevent Ethernet frame loss under congested network conditions. FCoE on a DCB network mimics the lightweight nature of native FC protocols and media. It does not incorporate TCP or even IP protocols. This means that FCoE is a layer 2 (non-routable) protocol just like FC. FCoE is only for short-haul communication within a data center.



Multiprotocol Label Switching (MPLS)

MPLS Network Architecture

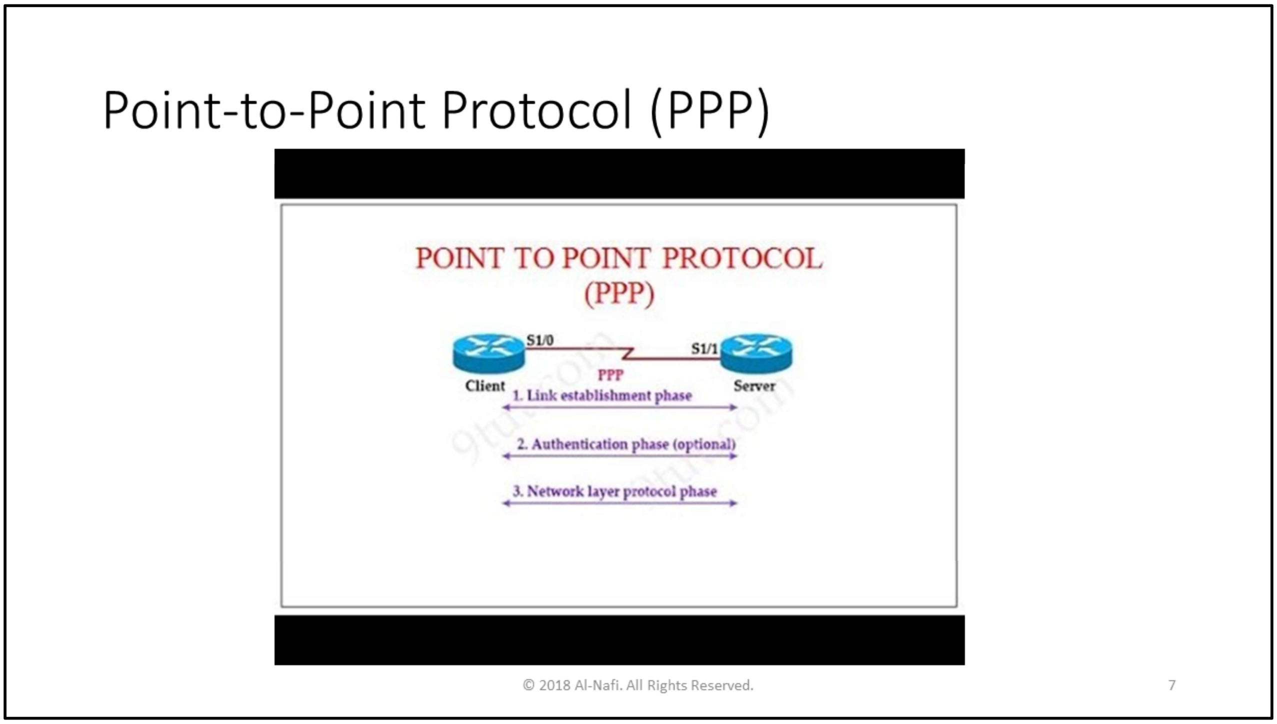
CE - Customer Edge
PE - Provider Edge
P - Provider Router
LER - Label Edge Router
LSR - Label Switching Router
LSP - Label Switched Path

Multiprotocol Label Switching (MPLS) is a wide area networking protocol that operates at both layer 2 and 3 and does “label switching.” The first device does a routing lookup, just like before, but instead of finding a next-hop, it finds the final destination router. And it finds a predetermined path from “here” to that final router. The router applies a “label” based on this information. Future routers use the label to route the traffic without needing to perform any additional IP lookups. At the final destination router, the label is removed, and the packet is delivered via normal IP routing. RFC 3031 defines the MPLS label switching architecture.

Why MPLS is used:

- Implementing Traffic Engineering which provides an ability to control where and how the traffic is routed on your network.
- Implementing Multiple Service Networks, which provides the ability to deliver data transport services as well as IP routing services across the same packets switched network architecture.
- Improving Network Resiliency with MPLS fast Reroute, which provides the

ability to organizations which are choosing Software Defined Wide area network or SD WAN. We will cover this later inshAllah.

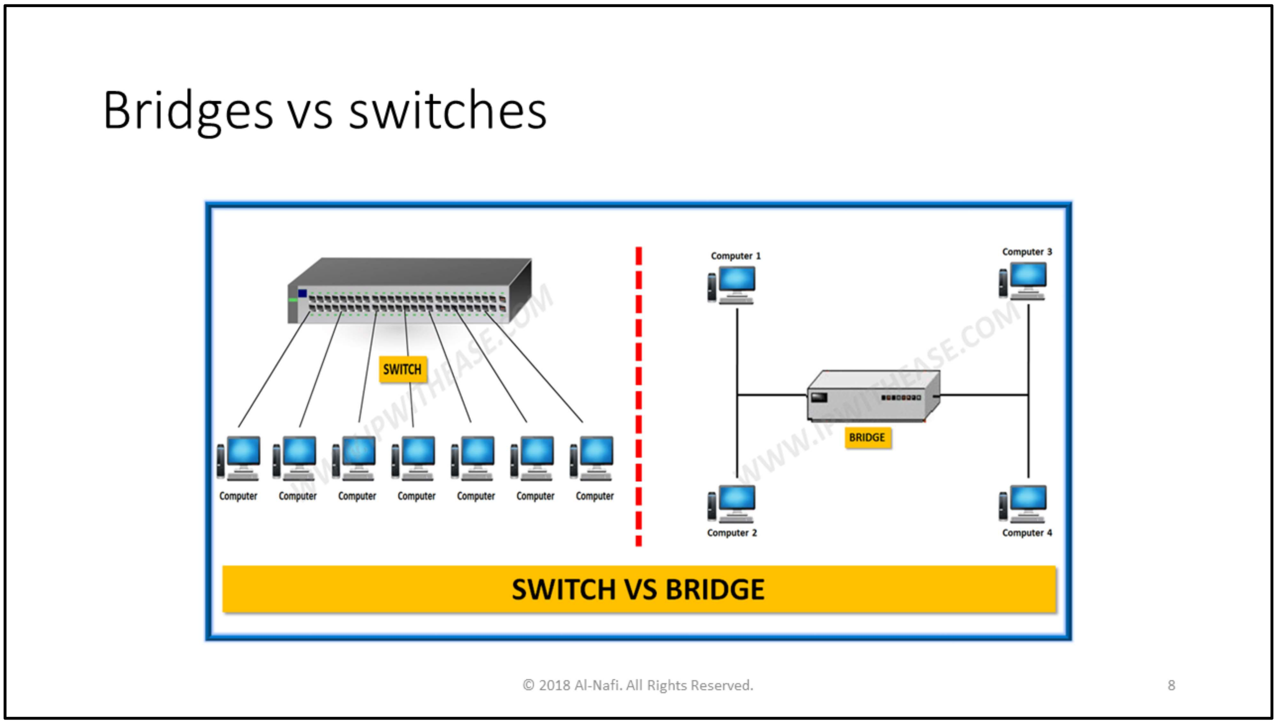


Point-to-Point Protocol (PPP)

POINT TO POINT PROTOCOL (PPP)
S1/0
S1/1
PPP
Client
Server
1. Link establishment phase
2. Authentication phase (optional)
3. Network layer protocol phase

The Point-to-Point Protocol (PPP) provides a standard method for transporting multiprotocol datagrams over point-to-point links. PPP is
comprised of three main components:

1. A method for encapsulating multiprotocol datagrams
2. A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection
3. A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols



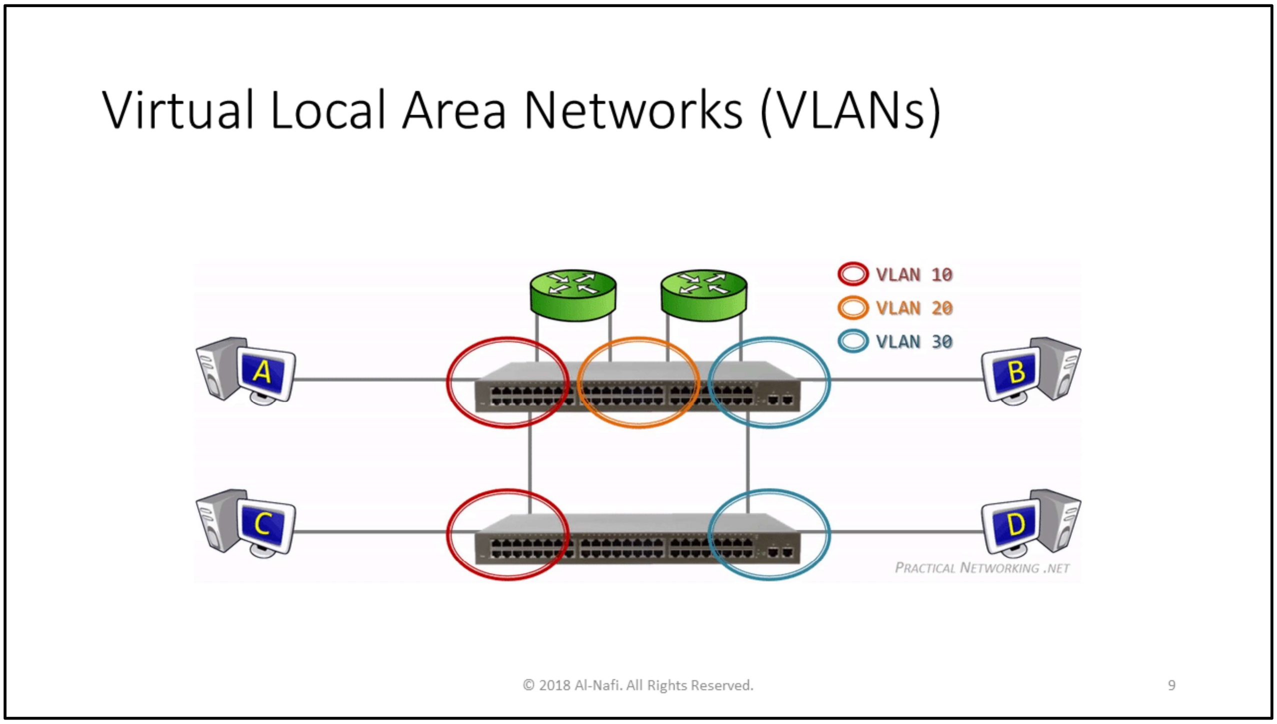
Bridges vs switches

Bridges are layer 2 devices that filter traffic between segments based on MAC addresses. In addition, they amplify signals to facilitate physically larger networks. A basic bridge filters out frames that are destined for another segment. Bridges can connect LANs with unlike media types, such as connecting an Unshielded Twisted Pair (UTP) segment with a segment that uses coaxial cable. Bridges do not reformat frames, such as converting a Token Ring frame to Ethernet. This means that only identical layer 2 architectures can relate to a simple bridge (e.g., Ethernet to Ethernet, etc.).

Network administrators can use translator bridges to connect dissimilar layer 2 architectures, such as Ethernet to Token Ring. Other specialized bridges filter outgoing traffic based on the destination MAC address. Bridges do not prevent an intruder from intercepting traffic on the local segment. A common type of bridge for many organizations is a wireless bridge based upon one of the IEEE 802.11 standards. While wireless bridges offer compelling efficiencies, they can pose devastating security issues

to organizations by effectively making all traffic crossing the
bridge visible to anyone connected to the LAN.

Switches The most common type of switches used today in the LAN operate at layer 2. A switch establishes a collision domain per port, enabling more efficient transmissions with CSMA/CD logic within Ethernet. Switches are the core device used today to build LANs. There are many security features offered within switches today, such as port blocking, port authentication, MAC filtering, and virtual local area networks (VLAN), to name a few. Layer 3 switches are switch, router combinations and are capable of making “switching decisions” based on either the MAC or IP address.

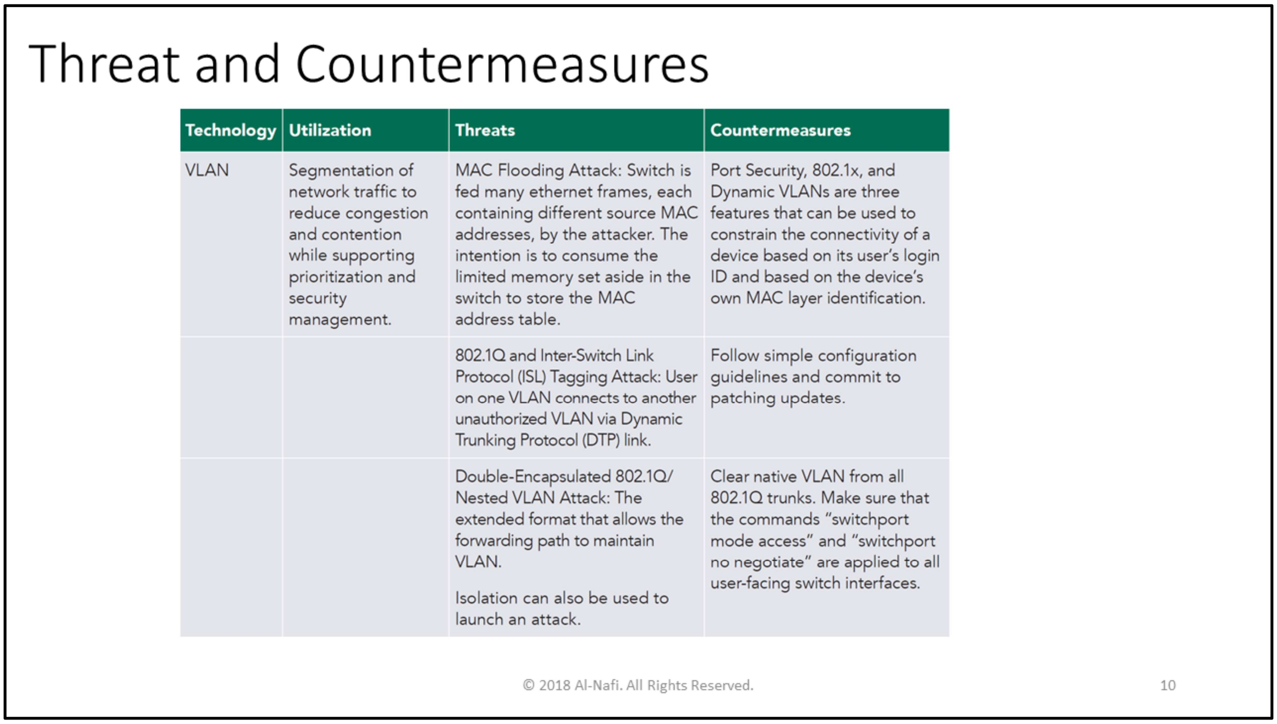


Virtual Local Area Networks (VLANs)

Virtual local area networks (VLANs) allow network administrators to use switches to create software-based LAN segments that can be defined based on factors other than physical location. Devices that share a VLAN communicate through switches, without being routed to other sub-networks, which reduces overhead due to router latency (as routers become faster, this is less of an advantage).

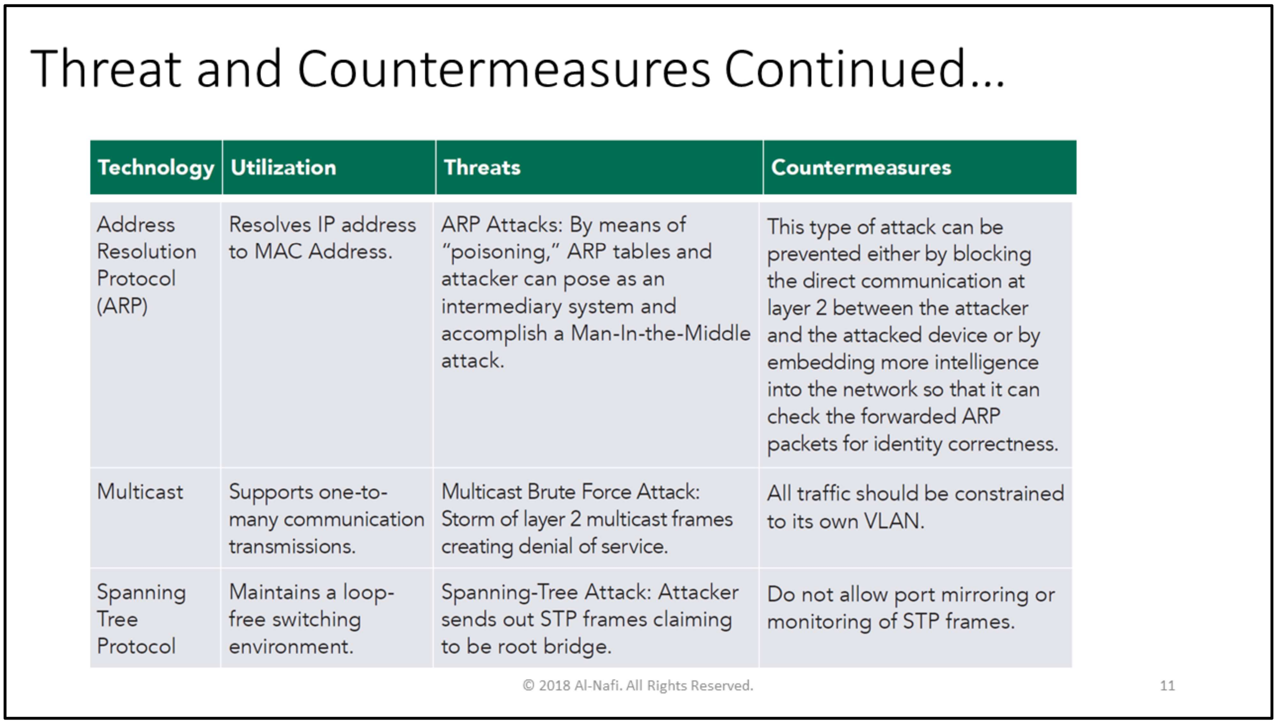
Furthermore, broadcasts are not forwarded outside of a VLAN, which reduces congestion due to broadcasts. Because VLANs are not restricted to the physical location of devices, they help make networks easier to manage. When a user or group of users changes their physical location, network administrators can simply change the membership of ports within a VLAN. Likewise, when additional devices must communicate with members of a VLAN, it is easy to add new ports to a VLAN. VLANs can be configured based on switch port, IP subnet, MAC address, and protocols. It is important to remember that VLANs do not guarantee a network's security. At first glance, it may seem that traffic cannot be intercepted because communication within a VLAN is restricted to member devices. However, there are attacks that allow a malicious user to see traffic from other VLANs (so-called VLAN hopping). Therefore, a VLAN can be created so that engineers can efficiently share confidential documents,

but the VLAN does not significantly protect the documents from unauthorized access.



Threat and Countermeasures

Technology	Utilization	Threats	Countermeasures
VLAN	Segmentation of network traffic to reduce congestion and contention while supporting prioritization and security management.	MAC Flooding Attack: Switch is fed many ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC address table.	Port Security, 802.1x, and Dynamic VLANs are three features that can be used to constrain the connectivity of a device based on its user's login ID and based on the device's own MAC layer identification.
		802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack: User on one VLAN connects to another unauthorized VLAN via Dynamic Trunking Protocol (DTP) link.	Follow simple configuration guidelines and commit to patching updates.
		Double-Encapsulated 802.1Q/ Nested VLAN Attack: The extended format that allows the forwarding path to maintain VLAN. Isolation can also be used to launch an attack.	Clear native VLAN from all 802.1Q trunks. Make sure that the commands "switchport mode access" and "switchport no negotiate" are applied to all user-facing switch interfaces.



Threat and Countermeasures Continued…

Technology	Utilization	Threats	Countermeasures
Address Resolution Protocol (ARP)	Resolves IP address to MAC Address.	ARP Attacks: By means of "poisoning," ARP tables and attacker can pose as an intermediary system and accomplish a Man-In-the-Middle attack.	This type of attack can be prevented either by blocking the direct communication at layer 2 between the attacker and the attacked device or by embedding more intelligence into the network so that it can check the forwarded ARP packets for identity correctness.
Multicast	Supports one-to-many communication transmissions.	Multicast Brute Force Attack: Storm of layer 2 multicast frames creating denial of service.	All traffic should be constrained to its own VLAN.
Spanning Tree Protocol	Maintains a loop-free switching environment.	Spanning-Tree Attack: Attacker sends out STP frames claiming to be root bridge.	Do not allow port mirroring or monitoring of STP frames.