

Computación en Internet I

Andrés A. Aristizábal P.
aaaristizabal@icesi.edu.co

Departamento de Tecnologías de Información y Comunicaciones



2023-1

1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

What is the basic service provided by the link layer?

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).
- Passes through a series of packet switches (switches and routers).

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).
- Passes through a series of packet switches (switches and routers).

What are the possible services that can be offered by a link-layer protocol?

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).
- Passes through a series of packet switches (switches and routers).

What are the possible services that can be offered by a link-layer protocol?

- Framing.

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).
- Passes through a series of packet switches (switches and routers).

What are the possible services that can be offered by a link-layer protocol?

- Framing.
- Link access.

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).
- Passes through a series of packet switches (switches and routers).

What are the possible services that can be offered by a link-layer protocol?

- Framing.
- Link access.
- Reliable delivery.

What is the basic service provided by the link layer?

- Provides a communication service between any two network hosts.
- Datagrams travel over a series of communication links (wired or wireless).
- Passes through a series of packet switches (switches and routers).

What are the possible services that can be offered by a link-layer protocol?

- Framing.
- Link access.
- Reliable delivery.
- Error detection and correction.

Framing?

Framing?

- Link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link.

Framing?

- Link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link.
- A frame consists of:

Framing?

- Link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link.
- A frame consists of:
 - ▶ A data field (where the network-layer datagram is inserted).

Framing?

- Link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link.
- A frame consists of:
 - ▶ A data field (where the network-layer datagram is inserted).
 - ▶ A number of header fields.

Link access?

Link access?

- A MAC protocol specifies the rules by which a frame is transmitted onto the link.

Link access?

- A MAC protocol specifies the rules by which a frame is transmitted onto the link.
 - ▶ For point-to-point links with a single sender and a single receiver at the other end of the link, the protocol is simple (or nonexistent).

Link access?

- A MAC protocol specifies the rules by which a frame is transmitted onto the link.
 - ▶ For point-to-point links with a single sender and a single receiver at the other end of the link, the protocol is simple (or nonexistent).
 - ▶ The sender can send a frame whenever the link is idle.

Link access?

- A MAC protocol specifies the rules by which a frame is transmitted onto the link.
 - ▶ For point-to-point links with a single sender and a single receiver at the other end of the link, the protocol is simple (or nonexistent).
 - ▶ The sender can send a frame whenever the link is idle.
 - ▶ When multiple nodes share a single broadcast link the MAC protocol serves to coordinate the frame transmissions of the many nodes.

Reliable delivery?

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.
- Can be achieved with acknowledgments and retransmissions.

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.
- Can be achieved with acknowledgments and retransmissions.
- Is often used for links that are prone to high error rates.

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.
- Can be achieved with acknowledgments and retransmissions.
- Is often used for links that are prone to high error rates.
 - ▶ Such as a wireless link.

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.
- Can be achieved with acknowledgments and retransmissions.
- Is often used for links that are prone to high error rates.
 - ▶ Such as a wireless link.
 - ▶ Correcting an error locally rather than forcing an end-to-end retransmission of the data by a transport or application-layer protocol.

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.
- Can be achieved with acknowledgments and retransmissions.
- Is often used for links that are prone to high error rates.
 - ▶ Such as a wireless link.
 - ▶ Correcting an error locally rather than forcing an end-to-end retransmission of the data by a transport or application-layer protocol.
- Can be considered an unnecessary overhead for low bit-error links (fiber, coax, and many twisted-pair copper links).

Reliable delivery?

- Guarantees to move each network-layer datagram across the link without error.
- Can be achieved with acknowledgments and retransmissions.
- Is often used for links that are prone to high error rates.
 - ▶ Such as a wireless link.
 - ▶ Correcting an error locally rather than forcing an end-to-end retransmission of the data by a transport or application-layer protocol.
- Can be considered an unnecessary overhead for low bit-error links (fiber, coax, and many twisted-pair copper links).
- Many wired link-layer protocols do not provide a reliable delivery service.

Error detection and correction?

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.
- Many link-layer protocols provide a mechanism to detect such bit errors.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.
- Many link-layer protocols provide a mechanism to detect such bit errors.
- The transmitting node includes error-detection bits in the frame.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.
- Many link-layer protocols provide a mechanism to detect such bit errors.
- The transmitting node includes error-detection bits in the frame.
- The receiving node performs an error check.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.
- Many link-layer protocols provide a mechanism to detect such bit errors.
- The transmitting node includes error-detection bits in the frame.
- The receiving node performs an error check.
- It is implemented in hardware.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.
- Many link-layer protocols provide a mechanism to detect such bit errors.
- The transmitting node includes error-detection bits in the frame.
- The receiving node performs an error check.
- It is implemented in hardware.
- Error correction is similar to error detection.

Error detection and correction?

- Bit errors are introduced by signal attenuation and electromagnetic noise.
- There is no need to forward a datagram that has an error.
- Many link-layer protocols provide a mechanism to detect such bit errors.
- The transmitting node includes error-detection bits in the frame.
- The receiving node performs an error check.
- It is implemented in hardware.
- Error correction is similar to error detection.
 - ▶ Determines exactly where in the frame the errors have occurred (and then corrects these errors).

Where is the Link Layer Implemented?

Where is the Link Layer Implemented?

- Mainly implemented on a chip called the network adapter (NIC).

Where is the Link Layer Implemented?

- Mainly implemented on a chip called the network adapter (NIC).
- Much of a link-layer controller's functionality is implemented in hardware.

Where is the Link Layer Implemented?

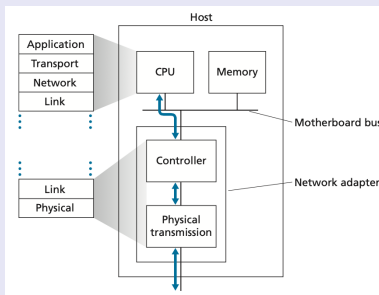
- Mainly implemented on a chip called the network adapter (NIC).
- Much of a link-layer controller's functionality is implemented in hardware.
- Part of the link layer is implemented in software that runs on the host's CPU.

Where is the Link Layer Implemented?

- Mainly implemented on a chip called the network adapter (NIC).
- Much of a link-layer controller's functionality is implemented in hardware.
- Part of the link layer is implemented in software that runs on the host's CPU.
- It is the place in the protocol stack where software meets hardware.

Where is the Link Layer Implemented?

- Mainly implemented on a chip called the network adapter (NIC).
- Much of a link-layer controller's functionality is implemented in hardware.
- Part of the link layer is implemented in software that runs on the host's CPU.
- It is the place in the protocol stack where software meets hardware.



Hardware

Hardware

- At the heart of the network adapter is the link-layer controller.

Hardware

- At the heart of the network adapter is the link-layer controller.
- Usually a single, special purpose chip that implements many of the link-layer services.

Hardware

- At the heart of the network adapter is the link-layer controller.
- Usually a single, special purpose chip that implements many of the link-layer services.
- Previously network adapters were physically separate cards.

Hardware

- At the heart of the network adapter is the link-layer controller.
- Usually a single, special purpose chip that implements many of the link-layer services.
- Previously network adapters were physically separate cards.
- Increasingly being integrated onto the host's motherboard.

What does the controller do?

What does the controller do?

- On the sending side:

What does the controller do?

- On the sending side:
 - ▶ Takes a datagram created and stored in host memory.

What does the controller do?

- On the sending side:
 - ▶ Takes a datagram created and stored in host memory.
 - ▶ Encapsulates the datagram in a link-layer frame.

What does the controller do?

- On the sending side:
 - ▶ Takes a datagram created and stored in host memory.
 - ▶ Encapsulates the datagram in a link-layer frame.
 - ▶ Transmits the frame into the communication link.

What does the controller do?

- On the sending side:
 - ▶ Takes a datagram created and stored in host memory.
 - ▶ Encapsulates the datagram in a link-layer frame.
 - ▶ Transmits the frame into the communication link.
- On the receiving side:

What does the controller do?

- On the sending side:
 - ▶ Takes a datagram created and stored in host memory.
 - ▶ Encapsulates the datagram in a link-layer frame.
 - ▶ Transmits the frame into the communication link.
- On the receiving side:
 - ▶ Receives the entire frame.

What does the controller do?

- On the sending side:
 - ▶ Takes a datagram created and stored in host memory.
 - ▶ Encapsulates the datagram in a link-layer frame.
 - ▶ Transmits the frame into the communication link.
- On the receiving side:
 - ▶ Receives the entire frame.
 - ▶ Extracts the network-layer datagram.

Software

Software

- Implements higher-level link layer functionality:

Software

- Implements higher-level link layer functionality:
 - ▶ Assembling link-layer addressing information.

Software

- Implements higher-level link layer functionality:
 - ▶ Assembling link-layer addressing information.
 - ▶ Activating the controller hardware.

Software

- Implements higher-level link layer functionality:
 - ▶ Assembling link-layer addressing information.
 - ▶ Activating the controller hardware.
 - ▶ Responding to controller interrupts.

Software

- Implements higher-level link layer functionality:
 - ▶ Assembling link-layer addressing information.
 - ▶ Activating the controller hardware.
 - ▶ Responding to controller interrupts.
 - ▶ Handles error conditions.

Software

- Implements higher-level link layer functionality:
 - ▶ Assembling link-layer addressing information.
 - ▶ Activating the controller hardware.
 - ▶ Responding to controller interrupts.
 - ▶ Handles error conditions.
 - ▶ Passes a datagram up to the network layer.

1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

What is a MAC address?

What is a MAC address?

- It is a means of identifying a device on the local network.

What is a MAC address?

- It is a means of identifying a device on the local network.
- An address that has many names.

What is a MAC address?

- It is a means of identifying a device on the local network.
- An address that has many names.
- Also referred to as a physical address, a hardware address, or a burnt-in address (BIA).

What is a MAC address?

- It is a means of identifying a device on the local network.
- An address that has many names.
- Also referred to as a physical address, a hardware address, or a burnt-in address (BIA).
- Represented as a 48-bit hexadecimal number.

What is a MAC address?

- It is comprised of 12 characters broken into 6 pairs.

What is a MAC address?

- It is comprised of 12 characters broken into 6 pairs.
- Globally unique.

What is a MAC address?

- It is comprised of 12 characters broken into 6 pairs.
- Globally unique.
- Each network card manufacturer is issued an Organizationally Unique Identifier (OUI).

What is a MAC address?

- It is comprised of 12 characters broken into 6 pairs.
- Globally unique.
- Each network card manufacturer is issued an Organizationally Unique Identifier (OUI).
- The OUI is the first six characters of the MAC address.

What is a MAC address?

- It is comprised of 12 characters broken into 6 pairs.
- Globally unique.
- Each network card manufacturer is issued an Organizationally Unique Identifier (OUI).
- The OUI is the first six characters of the MAC address.
- It is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place.

What is a MAC address?

- It is comprised of 12 characters broken into 6 pairs.
- Globally unique.
- Each network card manufacturer is issued an Organizationally Unique Identifier (OUI).
- The OUI is the first six characters of the MAC address.
- It is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place.
- Meanwhile, the IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers.

1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

What is the Address Resolution Protocol (ARP)?

What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.

What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.
- It works between the data link layer and the network layer.

What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.
- It works between the data link layer and the network layer.
- By using this protocol, a computer can find a MAC address related to a particular IP address.

What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.
- It works between the data link layer and the network layer.
- By using this protocol, a computer can find a MAC address related to a particular IP address.
 - ▶ The computer broadcasts who has the IP address used to communicate.

What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.
- It works between the data link layer and the network layer.
- By using this protocol, a computer can find a MAC address related to a particular IP address.
 - ▶ The computer broadcasts who has the IP address used to communicate.
 - ▶ All the devices on the network will receive that ARP request and will look at the IP address that was requested.

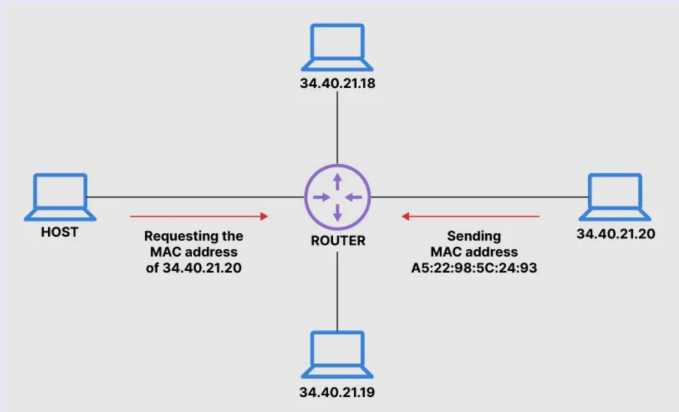
What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.
- It works between the data link layer and the network layer.
- By using this protocol, a computer can find a MAC address related to a particular IP address.
 - ▶ The computer broadcasts who has the IP address used to communicate.
 - ▶ All the devices on the network will receive that ARP request and will look at the IP address that was requested.
 - ▶ If the IP address doesn't belong to that device, it will ignore the request.

What is the Address Resolution Protocol (ARP)?

- A protocol that connects an ever-changing IP address to a MAC address, in a LAN.
- It works between the data link layer and the network layer.
- By using this protocol, a computer can find a MAC address related to a particular IP address.
 - ▶ The computer broadcasts who has the IP address used to communicate.
 - ▶ All the devices on the network will receive that ARP request and will look at the IP address that was requested.
 - ▶ If the IP address doesn't belong to that device, it will ignore the request.
 - ▶ If the IP address does belong to the device, it will send an ARP reply saying that that particular IP address belongs to a specific MAC address.

What is the Address Resolution Protocol (ARP)?



1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

What is a switch?

What is a switch?

- It is a device that's used to forward traffic from one device to the next within a local network.

What is a switch?

- It is a device that's used to forward traffic from one device to the next within a local network.

What is the purpose of switches?

What is a switch?

- It is a device that's used to forward traffic from one device to the next within a local network.

What is the purpose of switches?

- By introducing a switch to a network, it provides a means of segmenting the network into smaller, more manageable, and more efficient areas.

What is a switch?

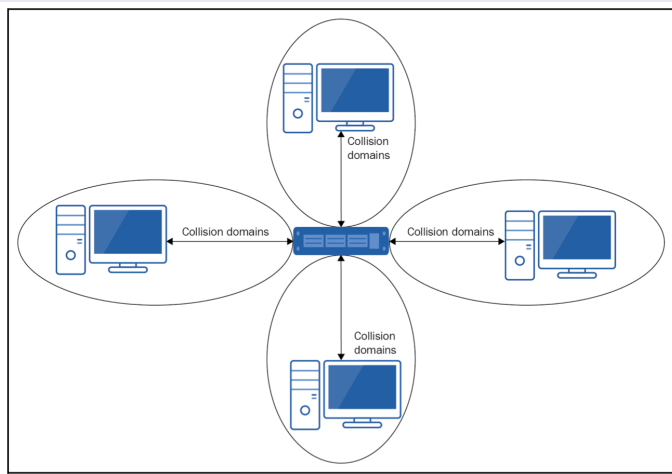
- It is a device that's used to forward traffic from one device to the next within a local network.

What is the purpose of switches?

- By introducing a switch to a network, it provides a means of segmenting the network into smaller, more manageable, and more efficient areas.
- This segmentation leads to a reduction in collisions since each port on a switch is classed as its own collision domain.

Understanding switches

What is the purpose of switches?



1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- **Frame forwarding**
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

What is frame forwarding?

What is frame forwarding?

- Frames contain a source MAC address and a destination MAC address.

What is frame forwarding?

- Frames contain a source MAC address and a destination MAC address.
- Switches receive a frame from the source device and quickly forward it toward the destination device.

What is frame forwarding?

- Frames contain a source MAC address and a destination MAC address.
- Switches receive a frame from the source device and quickly forward it toward the destination device.

Which are the two methods of forwarding data?

What is frame forwarding?

- Frames contain a source MAC address and a destination MAC address.
- Switches receive a frame from the source device and quickly forward it toward the destination device.

Which are the two methods of forwarding data?

- Cut-through.

What is frame forwarding?

- Frames contain a source MAC address and a destination MAC address.
- Switches receive a frame from the source device and quickly forward it toward the destination device.

Which are the two methods of forwarding data?

- Cut-through.
- Store and forward.

How does the cut-through method work?

How does the cut-through method work?

- The switch forwards the data almost immediately.

How does the cut-through method work?

- The switch forwards the data almost immediately.
- Just needs to know the source and destination MAC addresses.

How does the cut-through method work?

- The switch forwards the data almost immediately.
- Just needs to know the source and destination MAC addresses.
- As soon as it has this information, it will forward the data, even if the whole frame hasn't been received by the switch.

How does the cut-through method work?

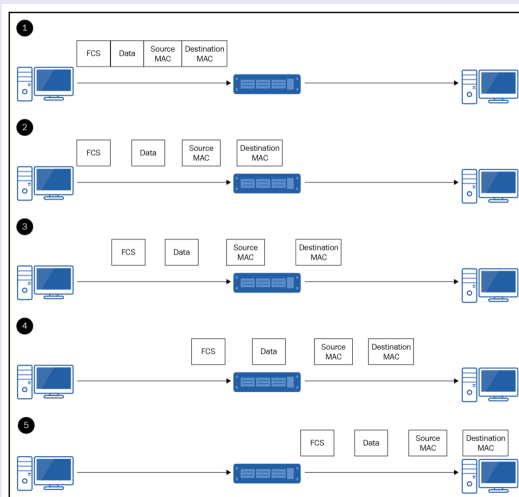
- The switch forwards the data almost immediately.
- Just needs to know the source and destination MAC addresses.
- As soon as it has this information, it will forward the data, even if the whole frame hasn't been received by the switch.
- It is a fast method.

How does the cut-through method work?

- The switch forwards the data almost immediately.
- Just needs to know the source and destination MAC addresses.
- As soon as it has this information, it will forward the data, even if the whole frame hasn't been received by the switch.
- It is a fast method.
- But it means that frames containing errors may be forwarded.

Frame forwarding

How does the cut-through method work?



How does the store and forward method work?

How does the store and forward method work?

- The switch will store the frame data in its memory buffer until the completely received.

How does the store and forward method work?

- The switch will store the frame data in its memory buffer until the completely received.
- Then it will perform error checking before forwarding the data.

How does the store and forward method work?

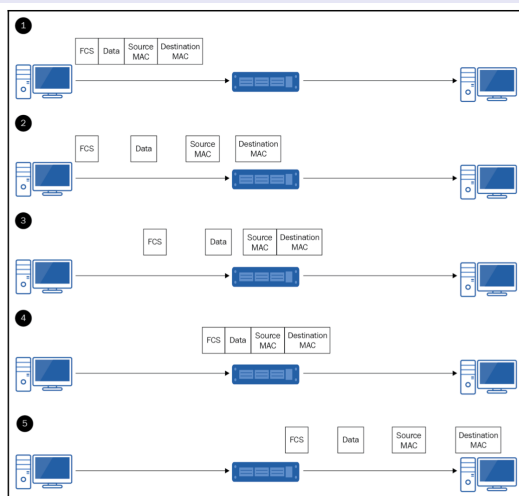
- The switch will store the frame data in its memory buffer until the completely received.
- Then it will perform error checking before forwarding the data.
- Any corrupt frames are discarded.

How does the store and forward method work?

- The switch will store the frame data in its memory buffer until the completely received.
- Then it will perform error checking before forwarding the data.
- Any corrupt frames are discarded.
- Allows data to be prioritized through Quality of Service (QoS).

Frame forwarding

How does the cut-through method work?



How could we summarize the frame forwarding process?

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).
- If it isn't, the switch updates the table with the interface.

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).
- If it isn't, the switch updates the table with the interface.
- Checks if there is an entry for the destination MAC address.

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).
- If it isn't, the switch updates the table with the interface.
- Checks if there is an entry for the destination MAC address.
- If there is, the frame is forwarded internally to the listed interface which transmits it to the destination device.

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).
- If it isn't, the switch updates the table with the interface.
- Checks if there is an entry for the destination MAC address.
- If there is, the frame is forwarded internally to the listed interface which transmits it to the destination device.
- If there is no entry for the destination MAC address, the switch broadcasts the frame from all its interfaces, except the interface the frame came in on.

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).
- If it isn't, the switch updates the table with the interface.
- Checks if there is an entry for the destination MAC address.
- If there is, the frame is forwarded internally to the listed interface which transmits it to the destination device.
- If there is no entry for the destination MAC address, the switch broadcasts the frame from all its interfaces, except the interface the frame came in on.
- The intended recipient will receive the frame and respond.

How could we summarize the frame forwarding process?

- Checks if the source MAC address is in its MAC table (CAM).
- If it isn't, the switch updates the table with the interface.
- Checks if there is an entry for the destination MAC address.
- If there is, the frame is forwarded internally to the listed interface which transmits it to the destination device.
- If there is no entry for the destination MAC address, the switch broadcasts the frame from all its interfaces, except the interface the frame came in on.
- The intended recipient will receive the frame and respond.
- The switch repeats this process for the response.

1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

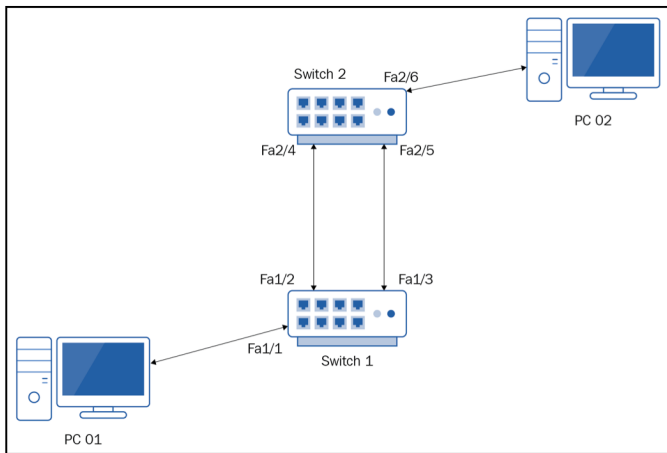
- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

What is data looping?

Spanning Tree Protocol

What is data looping?



What is the Spanning Tree Protocol?

What is the Spanning Tree Protocol?

- The purpose of STP is to prevent looping between switches when redundant links are implemented.

What is the Spanning Tree Protocol?

- The purpose of STP is to prevent looping between switches when redundant links are implemented.
- A switch is elected as the root bridge.

What is the Spanning Tree Protocol?

- The purpose of STP is to prevent looping between switches when redundant links are implemented.
- A switch is elected as the root bridge.
- The switches identify which of their interfaces are the closest to the root bridge and dub them root ports (RP).

What is the Spanning Tree Protocol?

- The purpose of STP is to prevent looping between switches when redundant links are implemented.
- A switch is elected as the root bridge.
- The switches identify which of their interfaces are the closest to the root bridge and dub them root ports (RP).
- These ports will always be available.

What is the Spanning Tree Protocol?

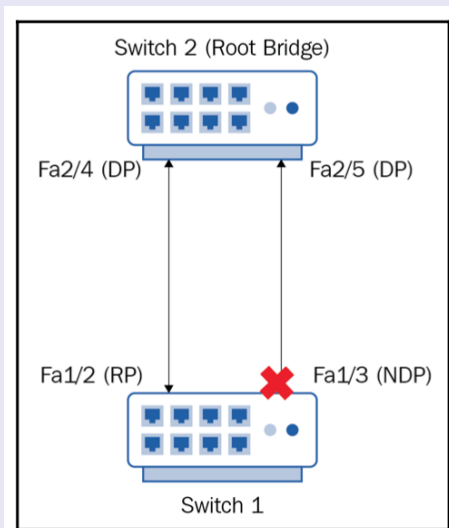
- The purpose of STP is to prevent looping between switches when redundant links are implemented.
- A switch is elected as the root bridge.
- The switches identify which of their interfaces are the closest to the root bridge and dub them root ports (RP).
- These ports will always be available.
- The other ports are referred to as designated ports (DPs) and non-designated ports (NDPs).

What is the Spanning Tree Protocol?

- The purpose of STP is to prevent looping between switches when redundant links are implemented.
- A switch is elected as the root bridge.
- The switches identify which of their interfaces are the closest to the root bridge and dub them root ports (RP).
- These ports will always be available.
- The other ports are referred to as designated ports (DPs) and non-designated ports (NDPs).
- Non-designated ports are prevented from sending data unless something fails on the network that requires them to assume the role of sending data.

Spanning Tree Protocol

What is the Spanning Tree Protocol?



1 Introduction to the link layer

- Services

2 MAC addresses

- Understanding MAC addresses
- ARP

3 Switches

- Understanding switches
- Frame forwarding
- Spanning Tree Protocol
- Switch characteristics

4 Workshop

How can switches be classified?

How can switches be classified?

- Managed.

How can switches be classified?

- Managed.
- Unmanaged.

How can switches be classified?

- Managed.
- Unmanaged.

What is an unmanaged switch?

How can switches be classified?

- Managed.
- Unmanaged.

What is an unmanaged switch?

- Network device that ships with a preloaded configuration that cannot be changed.

How can switches be classified?

- Managed.
- Unmanaged.

What is an unmanaged switch?

- Network device that ships with a preloaded configuration that cannot be changed.
- Used purely to allow endpoint devices to communicate with each other.

How can switches be classified?

- Managed.
- Unmanaged.

What is an unmanaged switch?

- Network device that ships with a preloaded configuration that cannot be changed.
- Used purely to allow endpoint devices to communicate with each other.
- Physically, it will usually be a small box with a small number of ports.

How can switches be classified?

- Managed.
- Unmanaged.

What is an unmanaged switch?

- Network device that ships with a preloaded configuration that cannot be changed.
- Used purely to allow endpoint devices to communicate with each other.
- Physically, it will usually be a small box with a small number of ports.



What is a managed switch?

What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.

What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.
- To do so, either physically connect to the switch's console port or remotely manage the switch using some form of terminal emulator.

What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.
- To do so, either physically connect to the switch's console port or remotely manage the switch using some form of terminal emulator.
- To connect to the switch remotely, it needs to be configured with an IP address.

What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.
- To do so, either physically connect to the switch's console port or remotely manage the switch using some form of terminal emulator.
- To connect to the switch remotely, it needs to be configured with an IP address.
- Can only be initially configured through a console port.



What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.
- To do so, either physically connect to the switch's console port or remotely manage the switch using some form of terminal emulator.
- To connect to the switch remotely, it needs to be configured with an IP address.
- Can only be initially configured through a console port.



How can it be configured?

What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.
- To do so, either physically connect to the switch's console port or remotely manage the switch using some form of terminal emulator.
- To connect to the switch remotely, it needs to be configured with an IP address.
- Can only be initially configured through a console port.



How can it be configured?

- A laptop or similar device is physically connected to the console port.

What is a managed switch?

- Allows configuration of VLANs, port speeds, security, duplex settings, etc.
- To do so, either physically connect to the switch's console port or remotely manage the switch using some form of terminal emulator.
- To connect to the switch remotely, it needs to be configured with an IP address.
- Can only be initially configured through a console port.

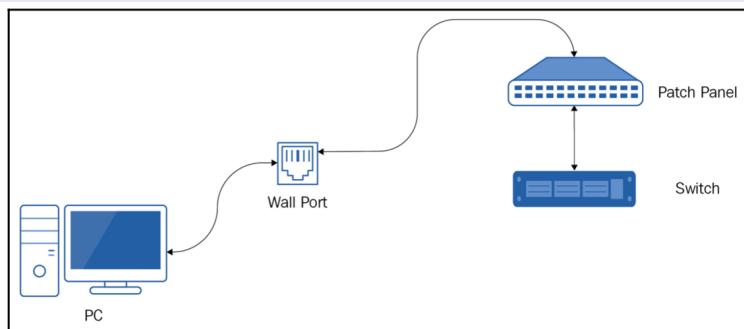


How can it be configured?

- A laptop or similar device is physically connected to the console port.
- A connection is made from the operating system using a terminal emulator, such as PuTTY.

How is the connectivity to the network?

How is the connectivity to the network?



How about the ports?

How about the ports?

- A switch can support 12, 24, or 48 number of interfaces or ports.

How about the ports?

- A switch can support 12, 24, or 48 number of interfaces or ports.
- Can support twisted pair cables, fiber optic cables, or both.

How about the ports?

- A switch can support 12, 24, or 48 number of interfaces or ports.
- Can support twisted pair cables, fiber optic cables, or both.
- Various speeds:

How about the ports?

- A switch can support 12, 24, or 48 number of interfaces or ports.
- Can support twisted pair cables, fiber optic cables, or both.
- Various speeds:
 - ▶ Fast Ethernet (10/100 Mbps).
 - ▶ Gigabit Ethernet (10/100/1,000 Mbps).
 - ▶ Ten Gigabit (10/100/1,000/10,000 Mbps).
 - ▶ 40/100 Gbps speeds.

Workshop

Complete workshop for today's class. To be handed in the next class.