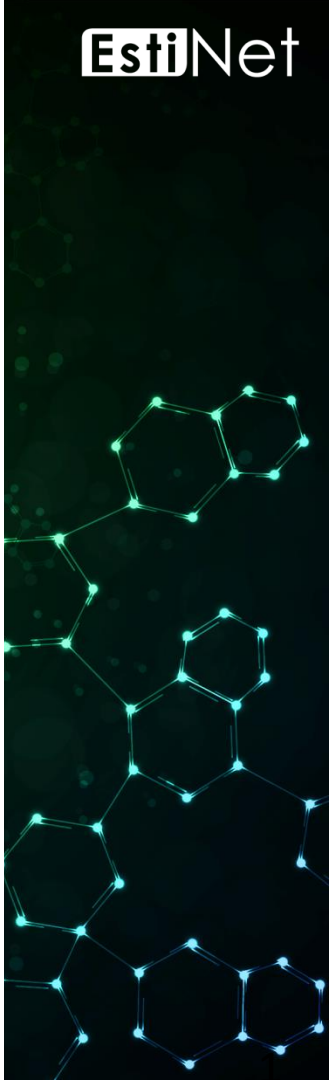
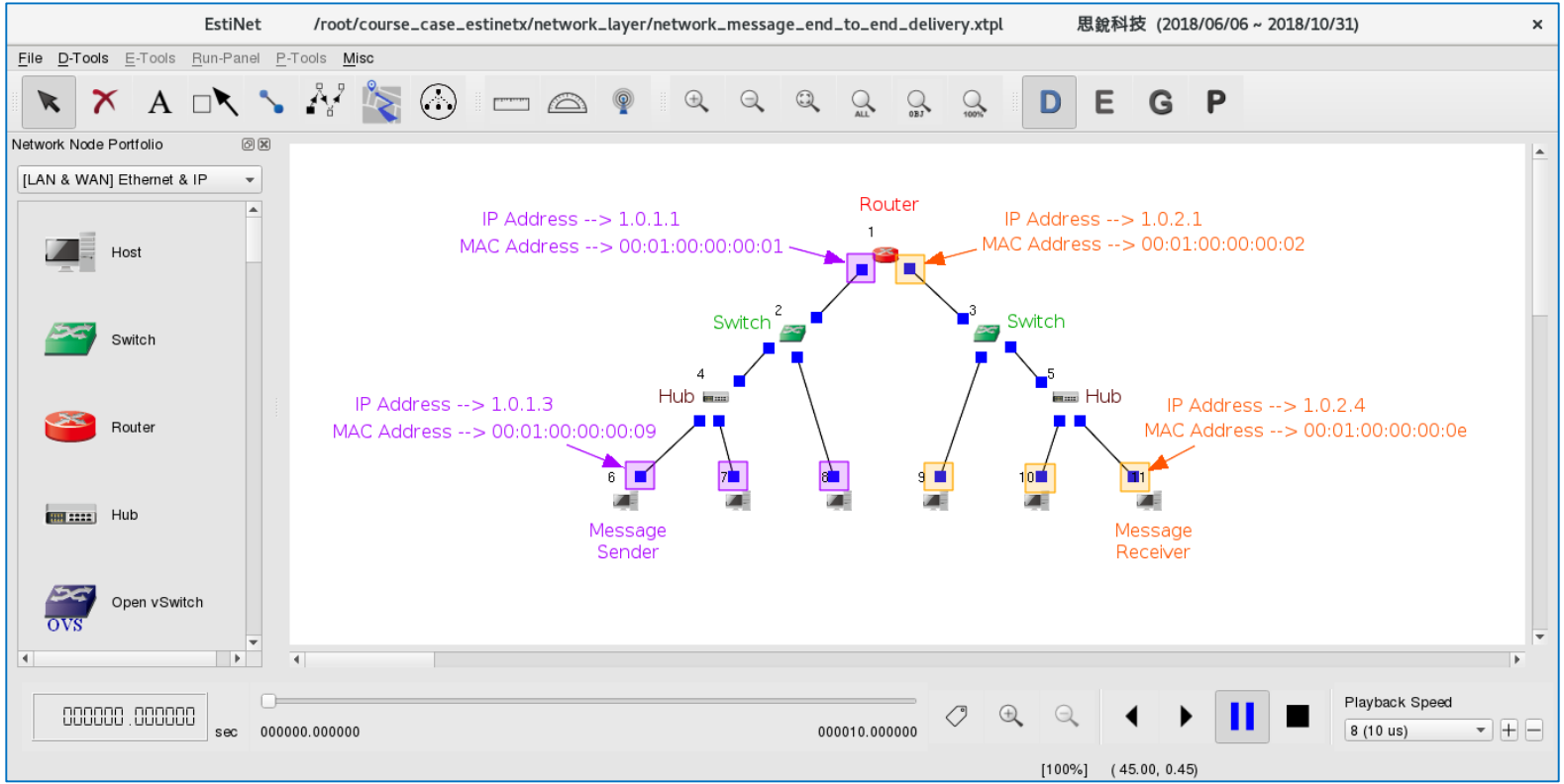
Network Messages' Encapsulation, Addressing and End-to-end Delivery Process



Outline

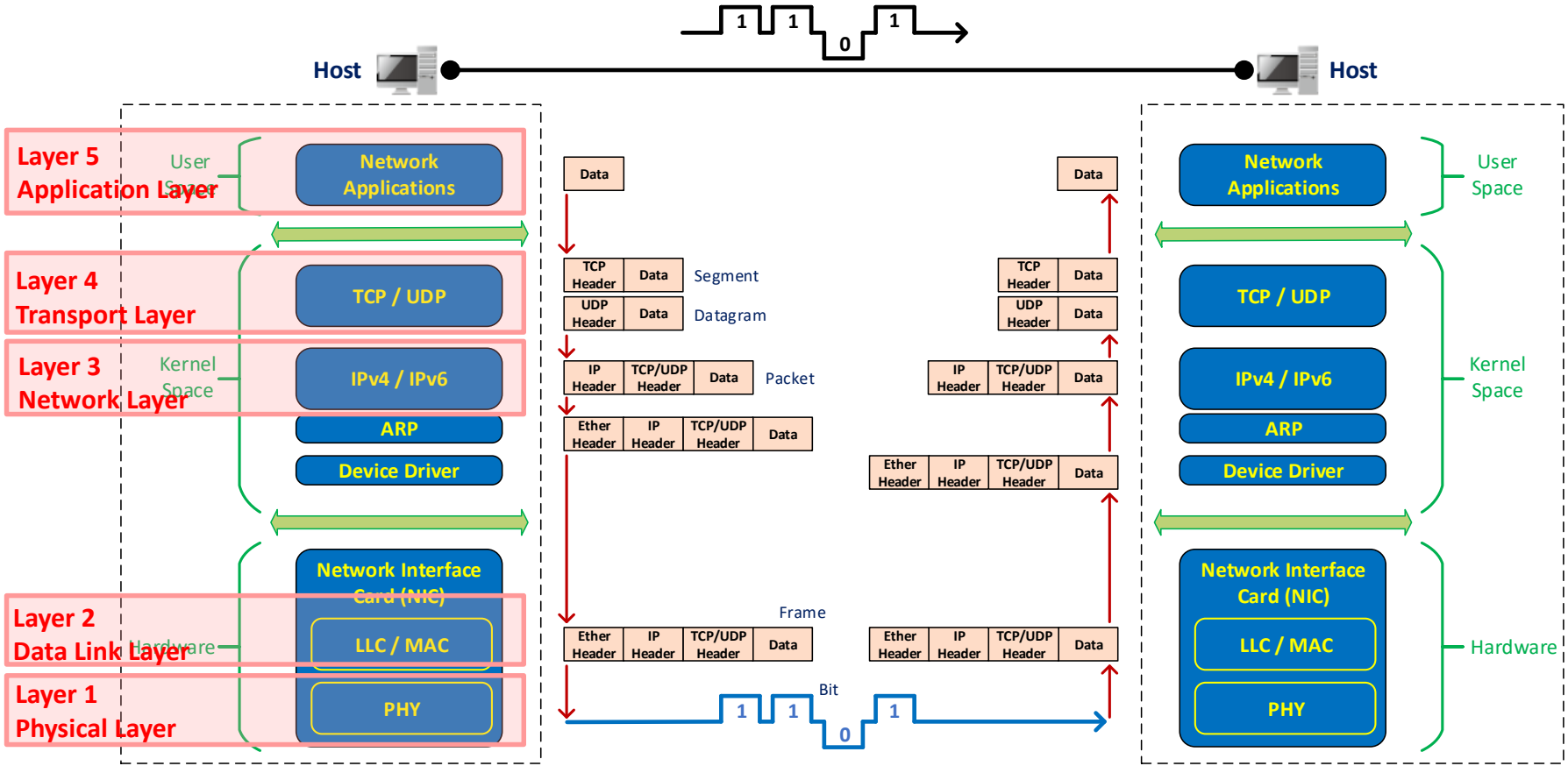
- The Header Encapsulation and Addressing of Network Messages
- The End-to-end Delivery Process of Network Messages
- Summary

<Simulation Case>
network_message_end_to_end_delivery.xtpl



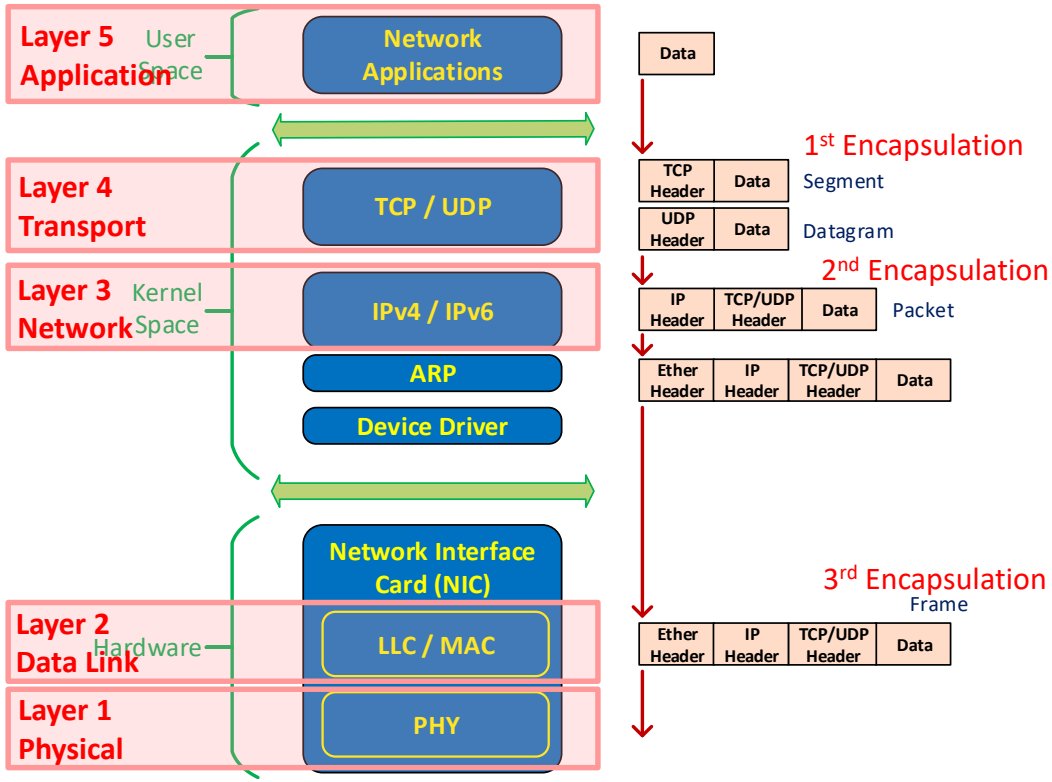
The Header Encapsulation and Addressing of Network Messages

The Encapsulation and Decapsulation of Network Messages



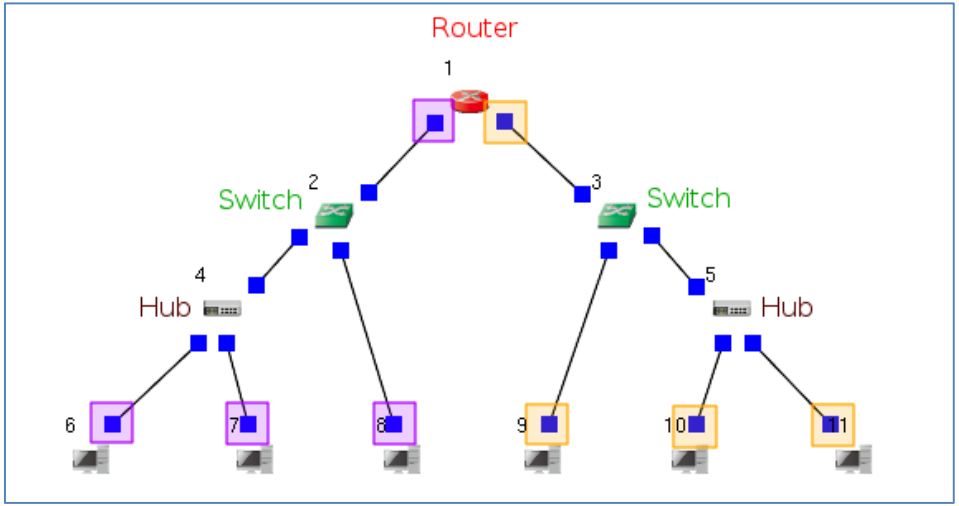
A Network Message's Encapsulation at the Sending Site

- On an Internet device, network application programs are executed to send network messages to the network. Before being sent out, network messages are usually encapsulated three times.
  - The 1st one occurs at layer 4 (transport layer) and common cases are TCP or UDP encapsulation.
  - The 2nd one occurs at layer 3 (network layer and common cases are IPv4 or IPv6 encapsulation.
  - The 3rd one occurs at layer 2 (data link layer). Different network interface cards have different encapsulation methods, such as Ethernet, Wi-Fi, Bluetooth, LTE, etc.



During the encapsulation process at the 2nd layer, a MAC header is prepended to a network message. The MAC header is filled with a destination MAC address to achieve MAC addressing.

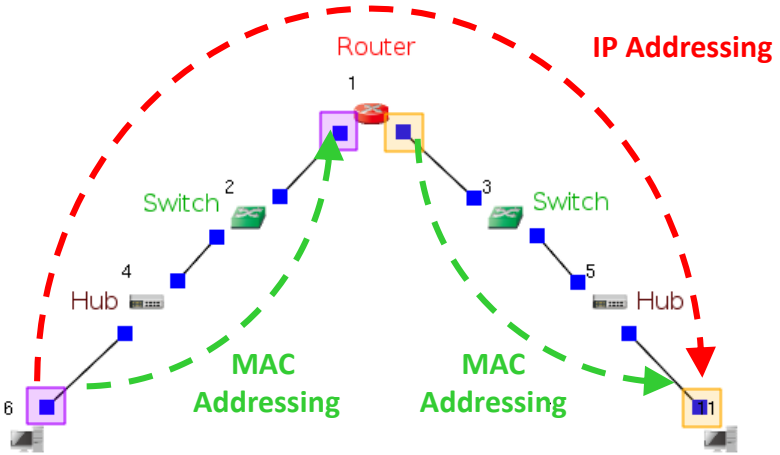
- In short, MAC address is the address of a network interface card (NIC). When a network message is going to be sent to a network from a NIC, filling destination MAC address in the message's MAC header can address a single or multiple NICs on the network.
- Generally speaking, if two network hosts are directly connected or connected through layer-1 or layer-2 devices (such as hub or switch), they are considered MAC-addressable to each other. If they are connected through layer-3 devices (such as router), they are not considered MAC-addressable to each other.



- In the graph above, two subnets are separated by the router. In the left subnet, four NIC's marked with purple squares are MAC-addressable to each other. Similarly, in the right subnet, four NIC's marked with orange squares are MAC-addressable to each other.
- However, a purple-square NIC and a orange-square NIC are not MAC-addressable to each other. That means the addressable range of MAC address is limited within a subnet.

During the encapsulation process at the 3rd layer, an IP header is prepended to a network message. The IP header is filled with a destination IP address to achieve IP addressing.

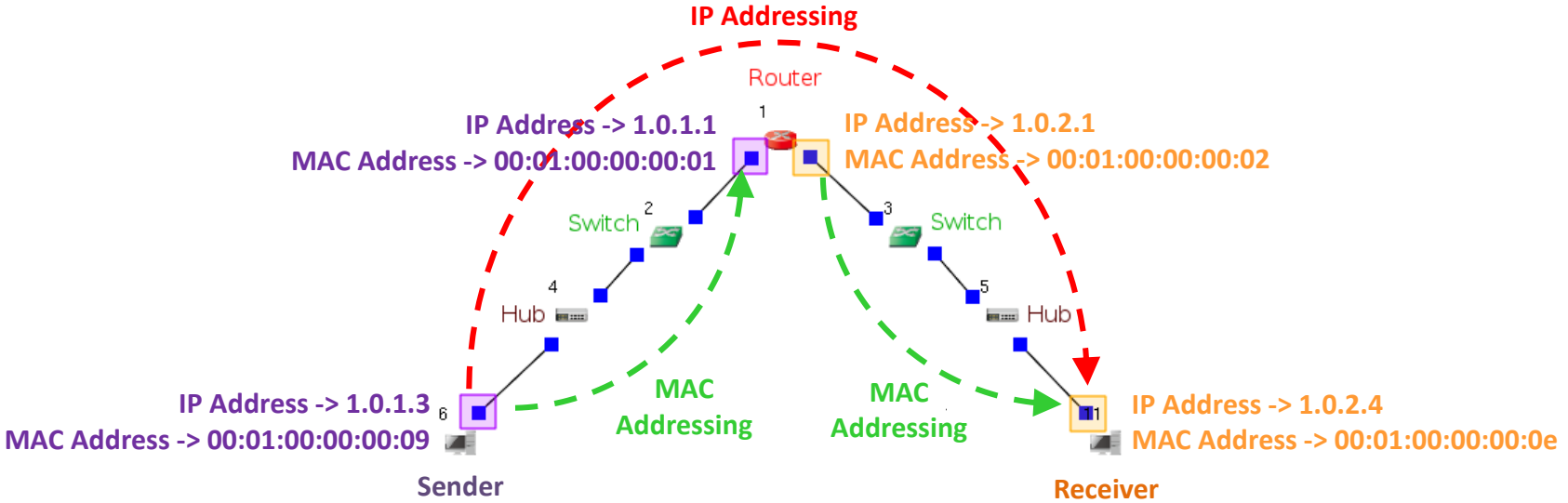
- Because the addressable range of MAC address is limited within a subnet, a network message requires IP addressing if its destination is located beyond a subnet.
- A router, which divides subnets, forwards network messages according to the destination IP address of network messages.
- During the encapsulation process of a network message, both IP addressing and MAC addressing are involved.
- During the delivery process of a network message, the message, in general, experiences one IP addressing and more than one MAC addressing (if across a subnet).

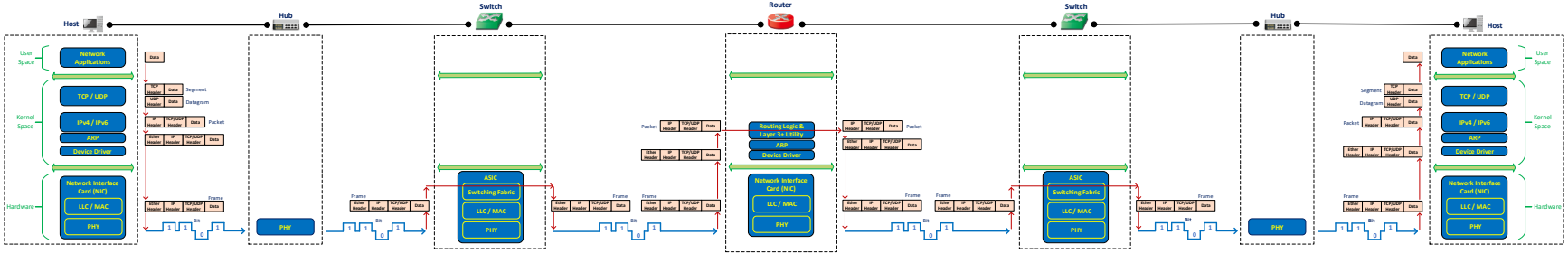


- In the graph above, the host at the left-down corner wants to send a message to the host at the right-down corner. During the delivery process of the message, it experiences one IP addressing the two MAC addressing.

The End-to-end Delivery Process of Network Messages

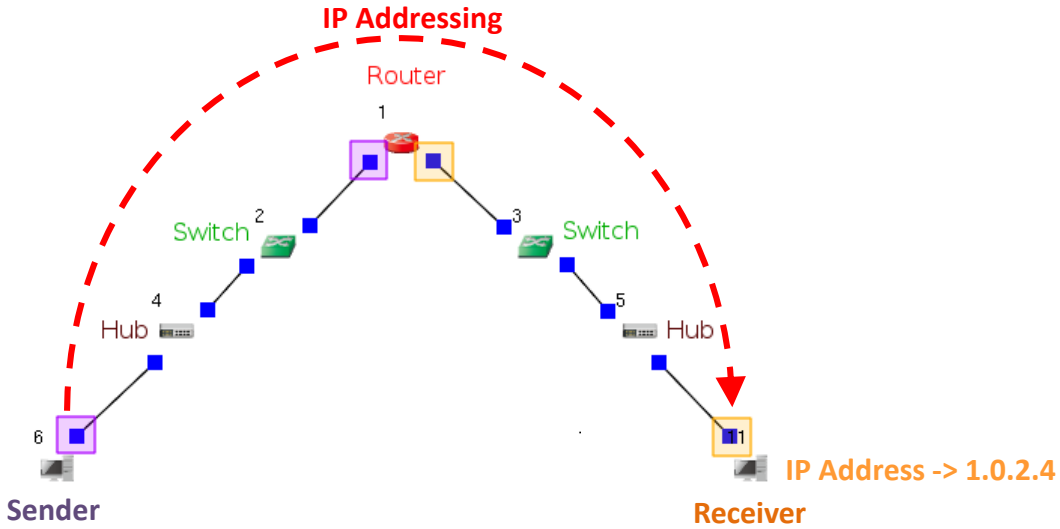
An Example of End-to-end Network Message Delivery Process



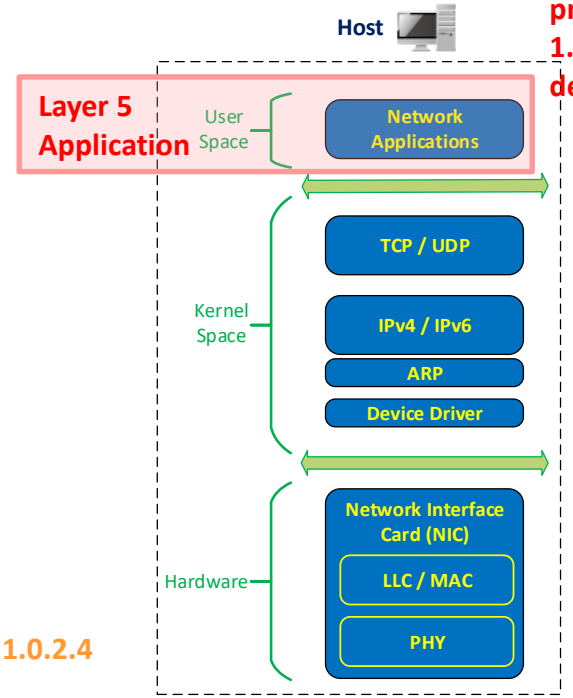


(1) A network application program (layer 5, application layer) running on the sender host has a message to be sent to the receiver host.

- The sender host takes the NIC's IP address of the receiver host as the message's destination.

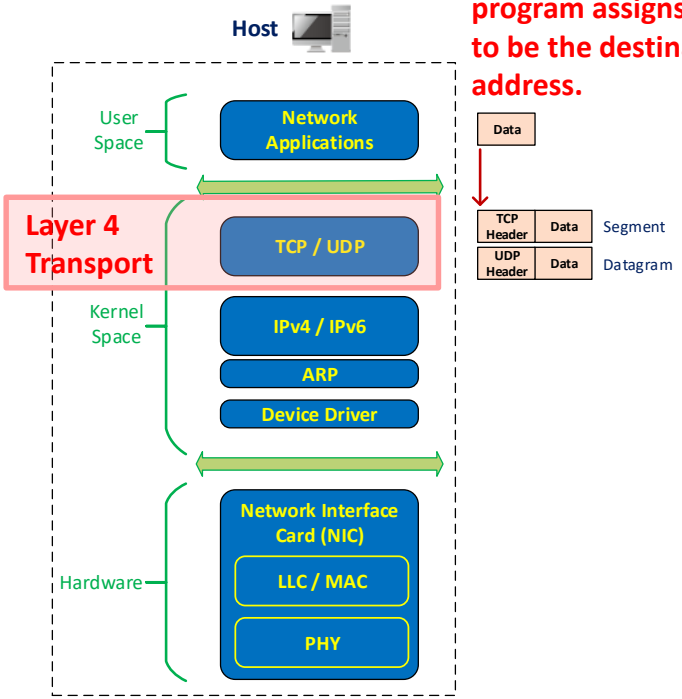


A network application program assigns 1.0.2.4 to be the destination IP address.



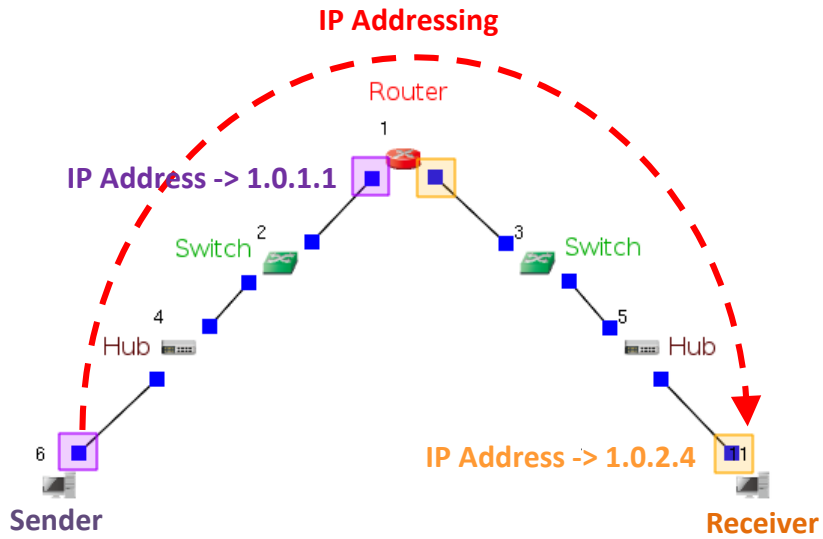
(2) If a network message has to be sent by TCP or UDP protocol (layer 4, transport layer), it has to be encapsulated with a TCP or UDP header.

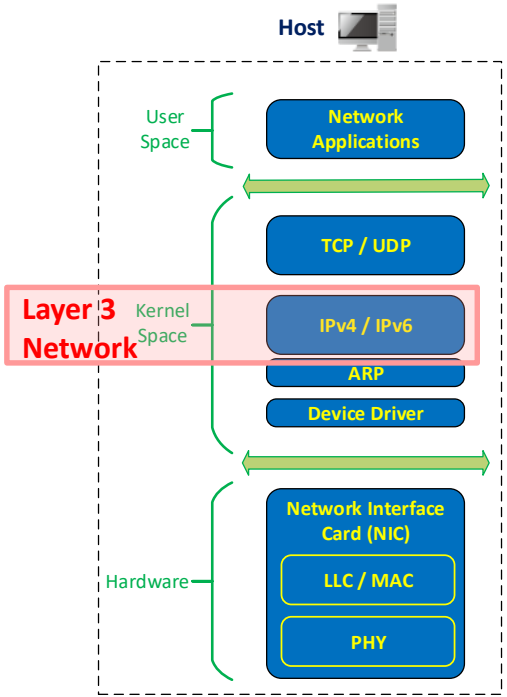
- After being encapsulated with a TCP header, a network message is also called a TCP segment.
- After being encapsulated with a UDP header, a network message is also called a UDP datagram.



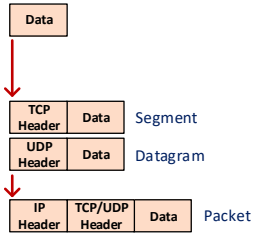
(3) When a network message reaches layer 3 (network layer), it is encapsulated with an IP header.

- After being encapsulated with an IP header, a network message is also called a packet.
- The destination's IP address is filled in the IP header.





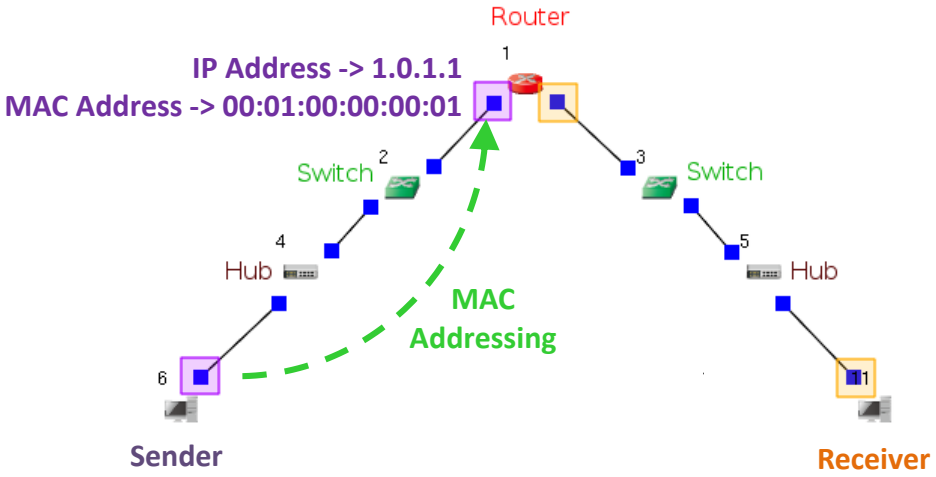
A network application program assigns 1.0.2.4 to be the destination IP address.

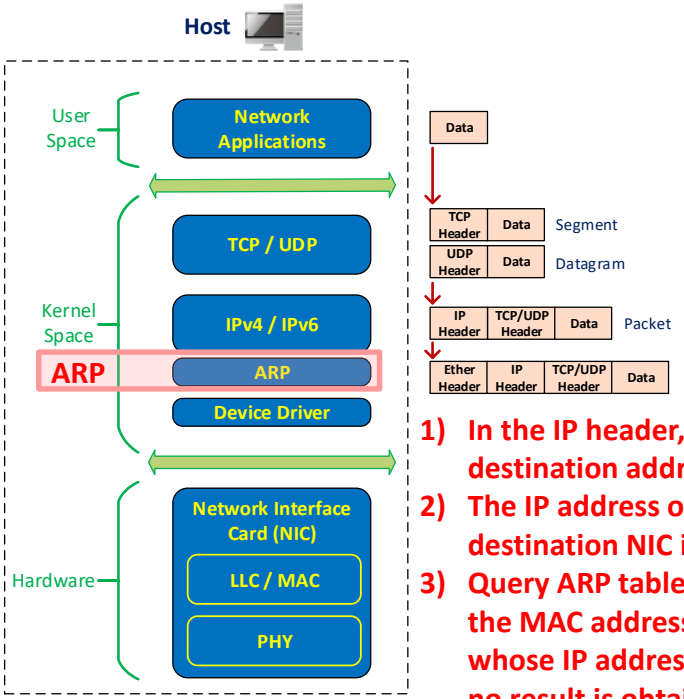


1) **The destination's IP address 1.0.2.4 is filled in the IP header.**
2) **Query the network-layer routing table to know that a message has to be forwarded by the router if its destination address is 1.0.2.4, that is located beyond the current subnet. Thus, the message has to be sent to the router's NIC first whose address is 1.0.1.1.**

(4) Get the MAC address of a message's next destination NIC by Address Resolution Protocol (ARP).

- The ARP turns the next destination NIC's IP address into the NIC's MAC address. The MAC address is filled in the MAC header of the message.
- Because the NIC used in this simulation case is an Ethernet NIC, the layer-2 MAC header is called Ether header.

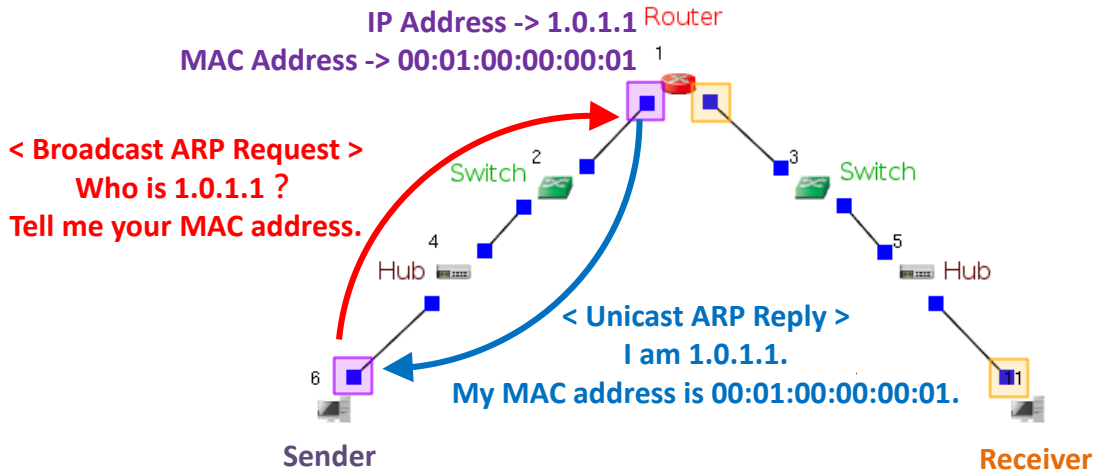




1) In the IP header, the IP destination address is 1.0.2.4.
2) The IP address of the next destination NIC is 1.0.1.1.
3) Query ARP table to try to get the MAC address of the NIC whose IP address is 1.0.1.1. If no result is obtained, an ARP request is sent to the network to ask the answer.

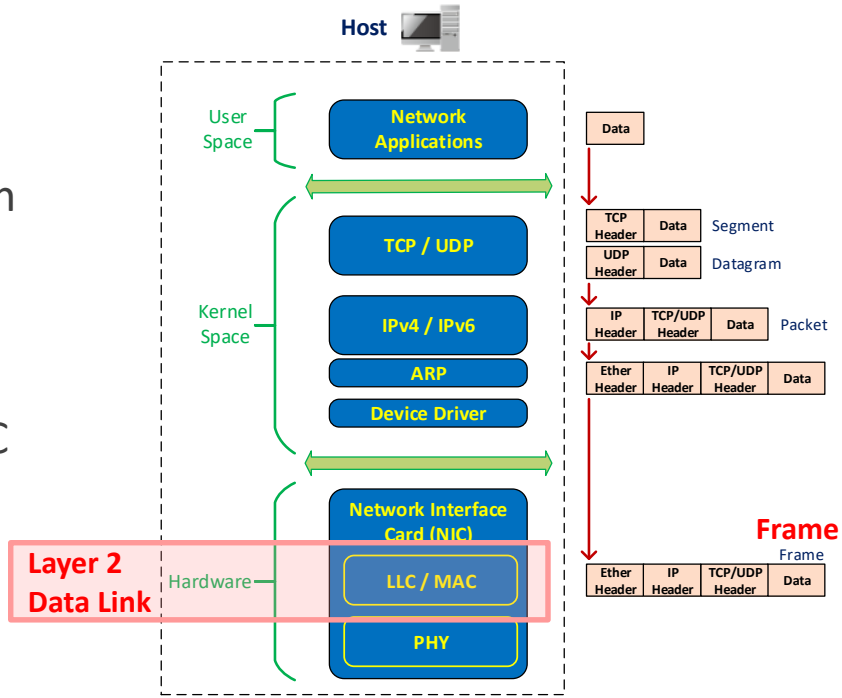
(4-1) ARP Request and ARP Reply

- At the sender site, if no IP-to-MAC address mapping entry is found in the ARP table, the ARP sends a broadcast message to network to ask the answer. This message is called ARP request.
- When a NIC receives an ARP request and finds that it is the asking target of the ARP request, it sends back an ARP reply that carries its MAC address.



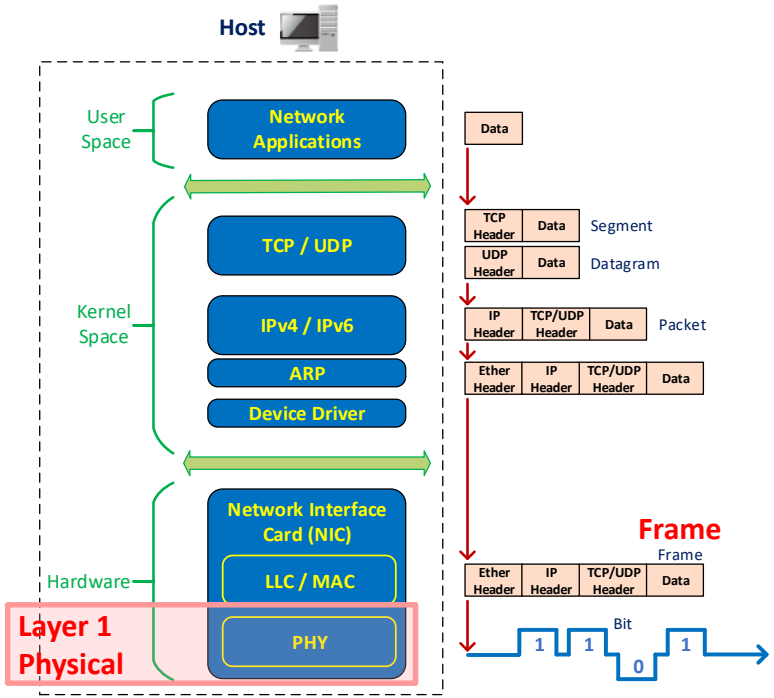
(5) When a network message reaches layer 2 (data link layer), it is encapsulated with a MAC header.

- When a message is processed by the ARP, a MAC header is prepended to the message and the destination MAC address is filled in the header. In general, the whole MAC header processing is finished at data link layer (layer 2).
- After being encapsulated with a MAC header, a network message is also called a frame.



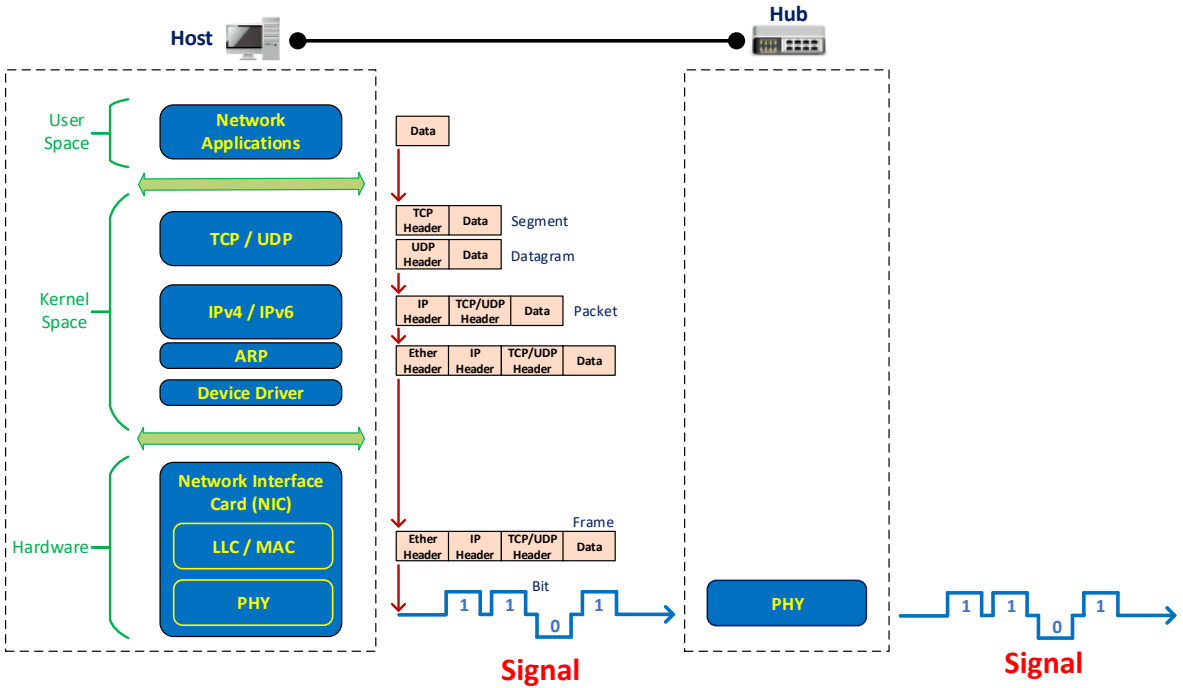
(6) When a network message reaches layer 1 (physical layer), it is transformed into signals and transmitted through media.

- In short, the main procedure at physical layer is signal processing, including signal encoding (transform a frame into signals), signal decoding (transform signals into a frame), and signal amplification, etc.



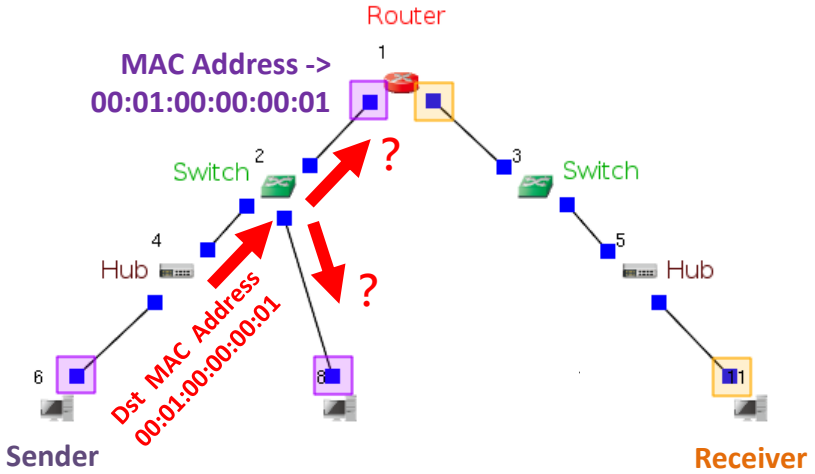
(7) When signals reach a layer-1 hub, the hub forwards the signals directly.

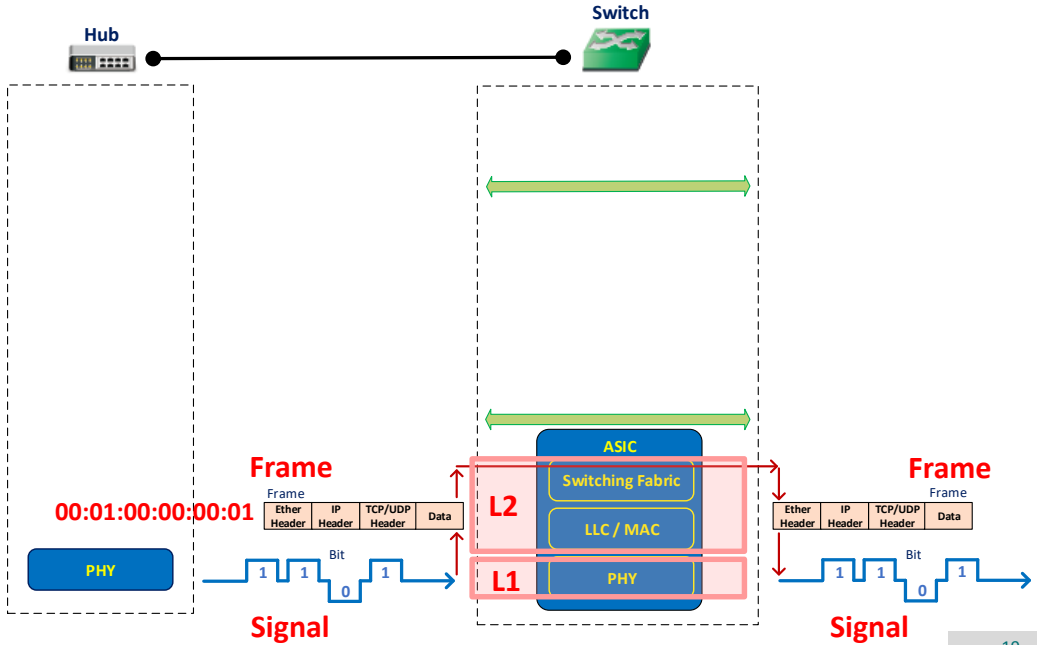
- On a hub, signals are not transformed into a frame for checking the frame's MAC header.
- A hub amplifies signals' power and forwards them out. Doing this extends the signal transmission range and increases the rate of successful signal decoding at receiver sites.



(8) When signals reach a layer-2 switch, the signals are transformed into a frame for checking the frame's MAC header.

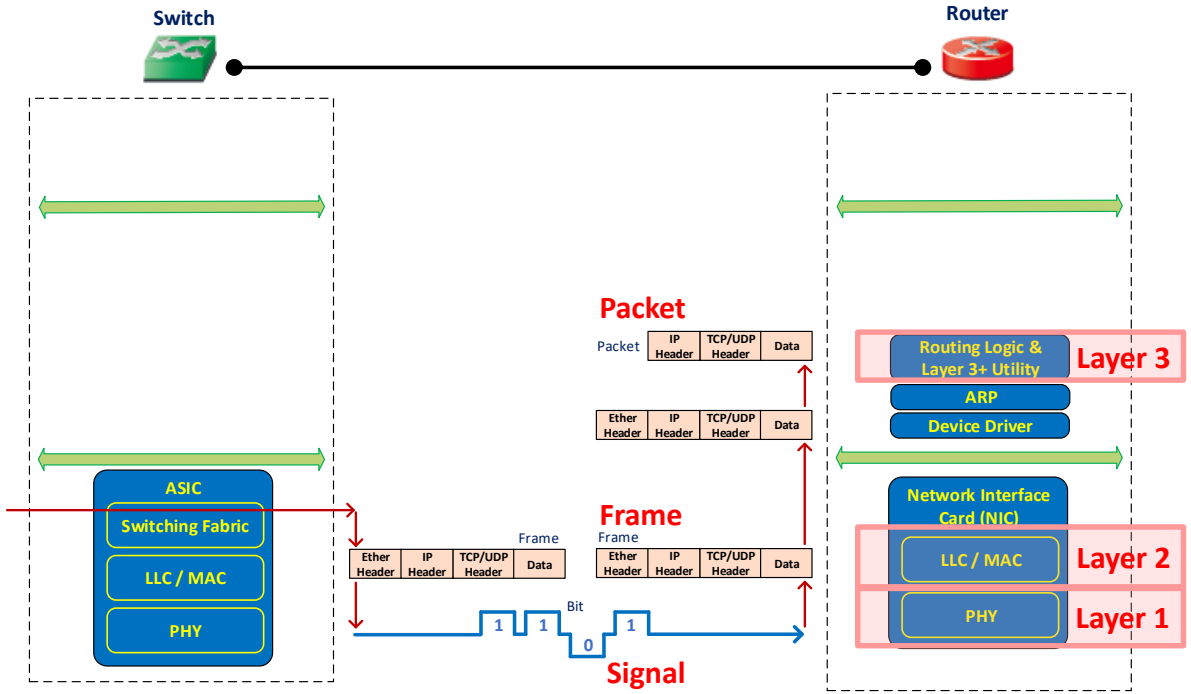
- The switch retrieves the destination MAC address from a MAC header. The address is used to query the switch's forwarding table to determine to which port(s) this frame should be forwarded. If no answer is obtained from the table, the switch forwards the frame to all ports except the input port.
- After the output port(s) is determined, the layer-2 frame is again transformed into layer-1 signals and the signals are transmitted.





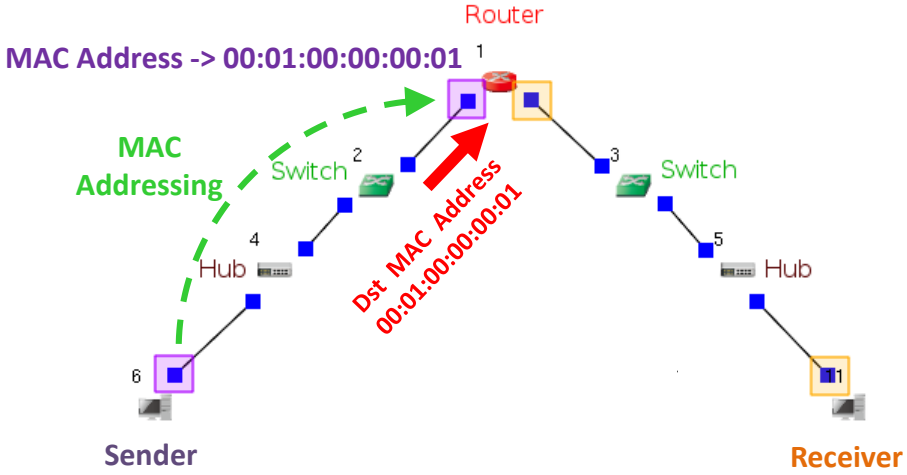
(9) When signals reach a layer-3 router, the signals are first transformed into a frame for checking MAC header. Next, the frame's MAC header is removed so that the frame becomes a packet. Finally, the IP header of the packet is checked for routing.

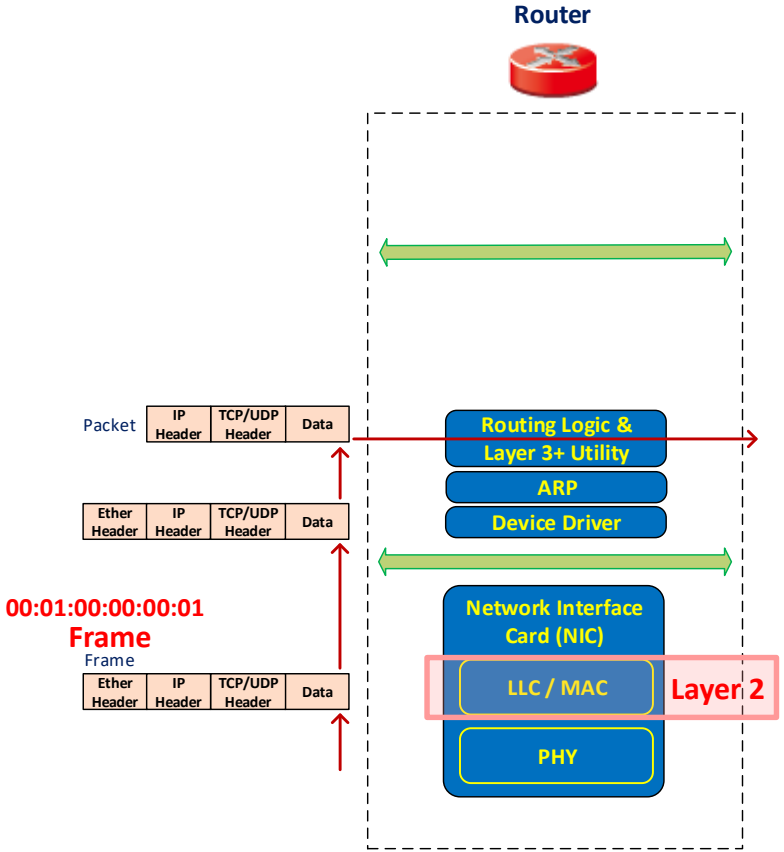
- After the signals are transformed into a frame, the destination MAC address retrieved from the frame's MAC header is checked to determine if this frame reaches the MAC-addressing destination or not. If the answer is yes, the MAC header of the frame is removed so that the frame becomes a packet. The packet is passed to layer 3 and the IP header of the packet is checked for routing.



(9-1) MAC Address Checking

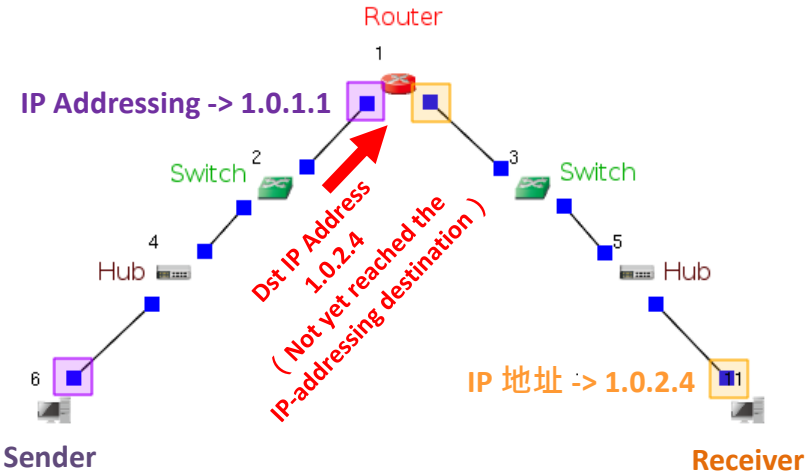
- The network message travels from the sender host to the left NIC of the router.
- First, the destination MAC address of the MAC header is compared with the NIC's MAC address to confirm that the message reaches the MAC-addressing destination.
- Next, the MAC header is removed and the message is passed to layer 3.

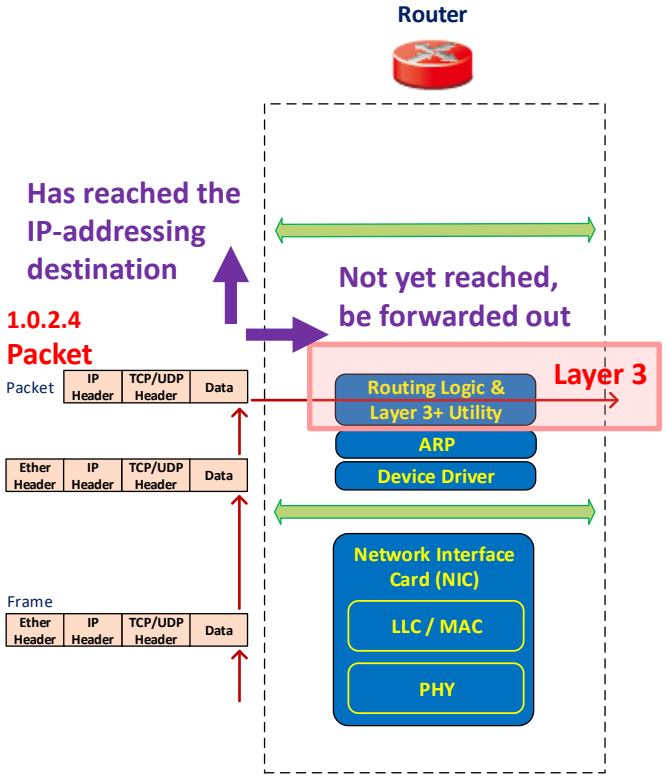




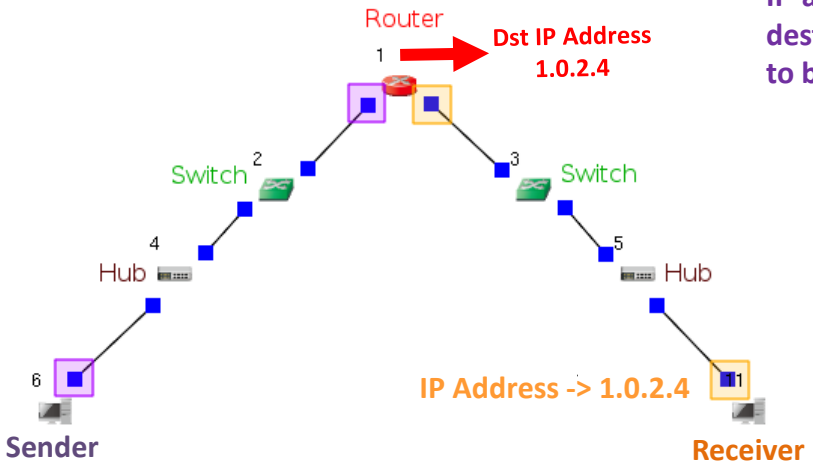
(9-2) IP Address Checking and Routing

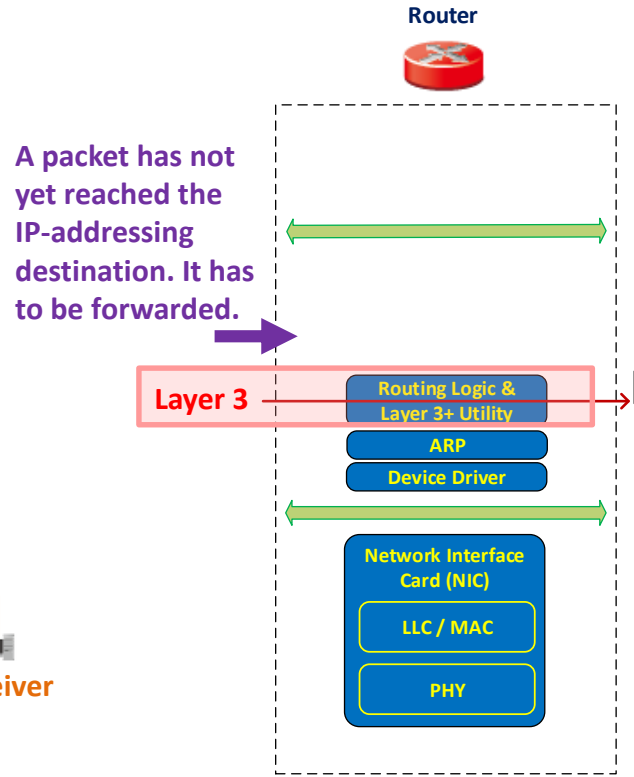
- If the prefix of a message is an IP header, the message is called a packet.
- When a packet reaches layer 3, the destination IP address of the IP header is checked to determine if this packet reaches its IP-addressing destination or not. If yes, the message is passed to layer 4. If no, the destination IP address is used to query the routing table to determine to which interface(s) this packet should be forwarded.





(10) When a packet/message is being routed at layer 3, its destination IP address is used to query the routing table.

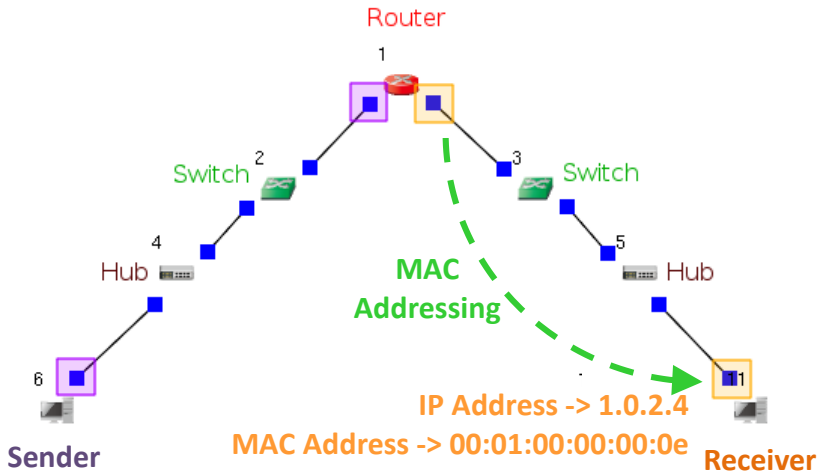


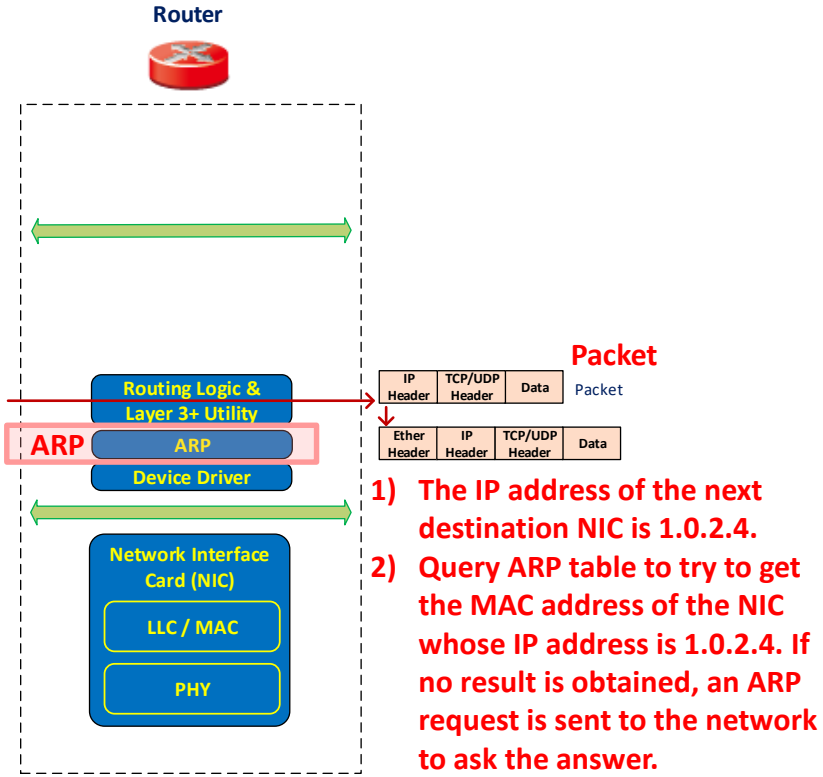


1) Dst IP address is 1.0.2.4.
2) Query the routing table and know that the destination IP address is located at the same subnet where the router's right NIC is located. That means the destination NIC and the router's right NIC are MAC-addressable to each other.

(11) Get the MAC address of a message's next destination NIC by Address Resolution Protocol (ARP).

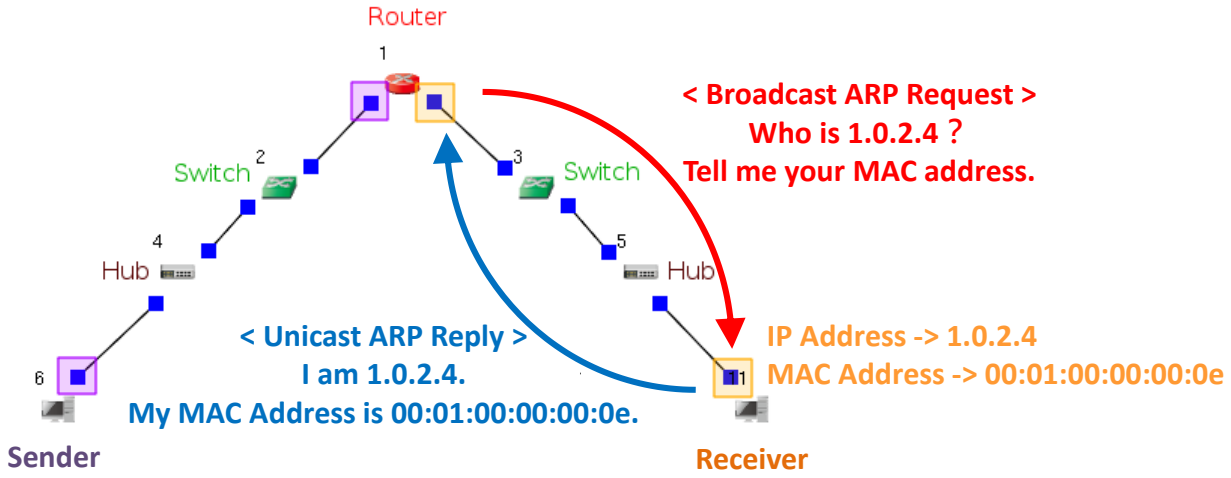
- The ARP turns the next destination NIC's IP address into the NIC's MAC address. The MAC address is filled in the MAC header of the message.
- Because the NIC used in this simulation case is an Ethernet NIC, the layer-2 MAC header is called Ether header.





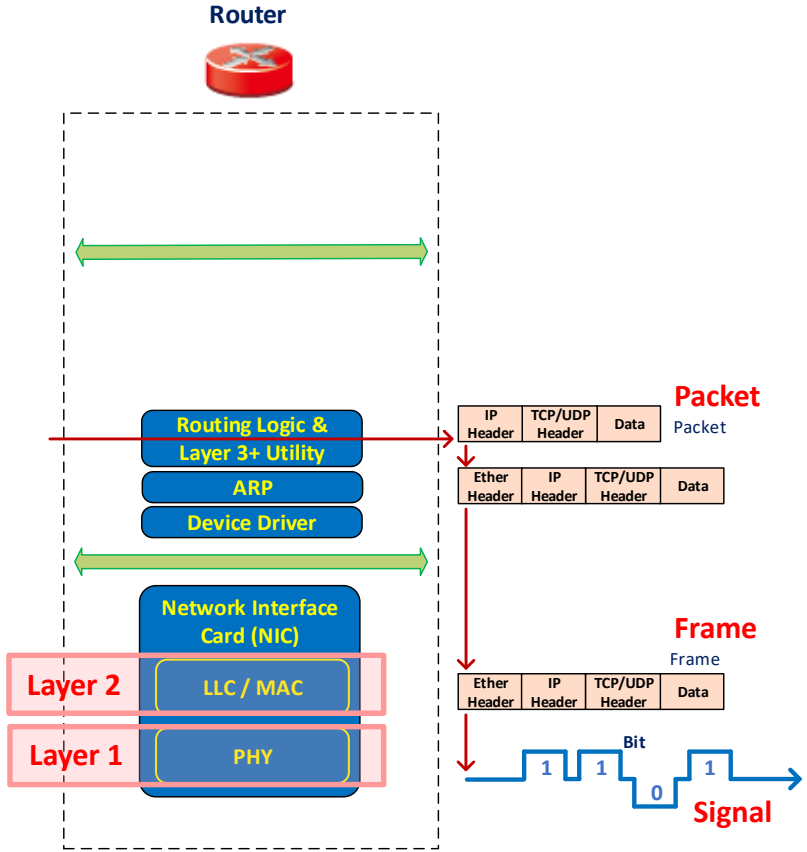
(11-1) ARP Request and ARP Reply

- At the sender site, if no IP-to-MAC address mapping entry is found in the ARP table, the ARP sends a broadcast message to network to ask the answer. This message is called ARP request.
- When a NIC receives an ARP request and finds that it is the asking target of the ARP request, it sends back an ARP reply that carries its MAC address.



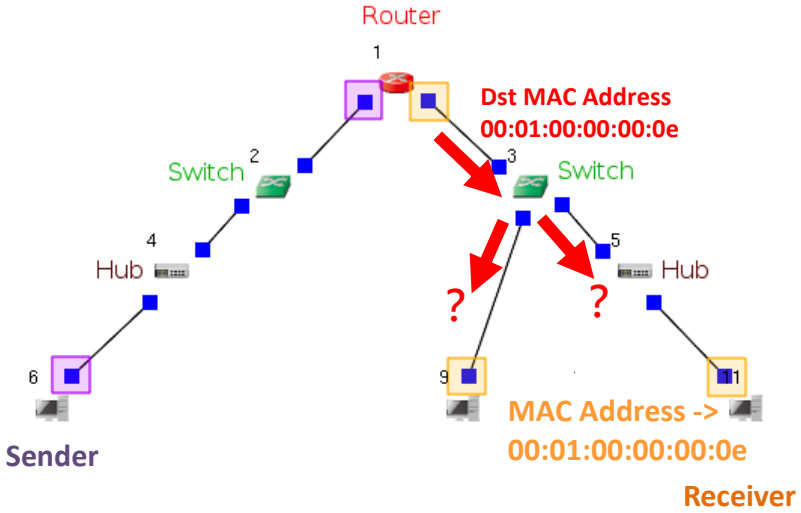
(12) The message is passed down to layer 2 (data link layer) and layer 1 (physical layer). Finally, it is transformed into signals and the signals are transmitted.

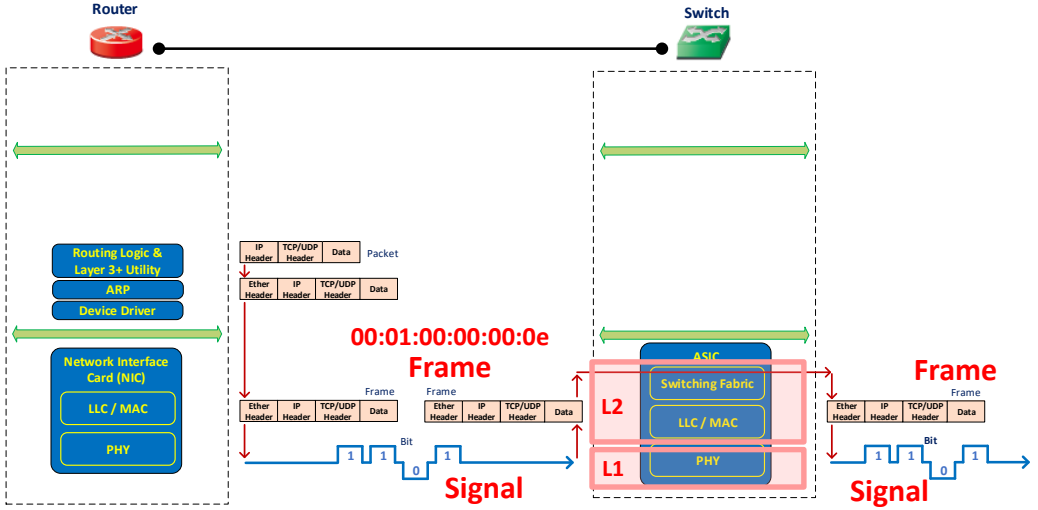
- The ways that address resolution protocol, layer 2 protocol, and layer 1 protocol process the message are the same as the ways used on the sender host.



(13) When signals reach a layer-2 switch, the signals are transformed into a frame for checking the frame's MAC header.

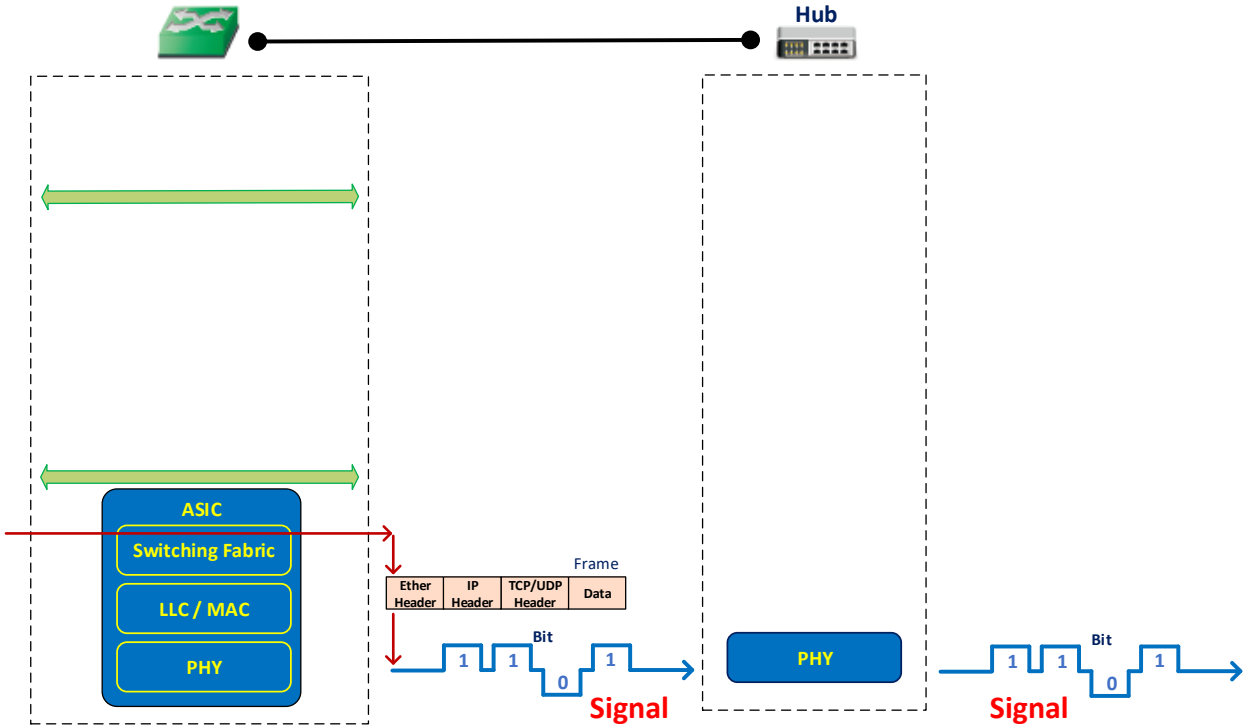
- The switch retrieves the destination MAC address from a MAC header. The address is used to query the switch's forwarding table to determine to which port(s) this frame should be forwarded. If no answer is obtained from the table, the switch forwards the frame to all ports except the input port.
- After the output port(s) is determined, the layer-2 frame is again transformed into layer-1 signals and the signals are transmitted out.





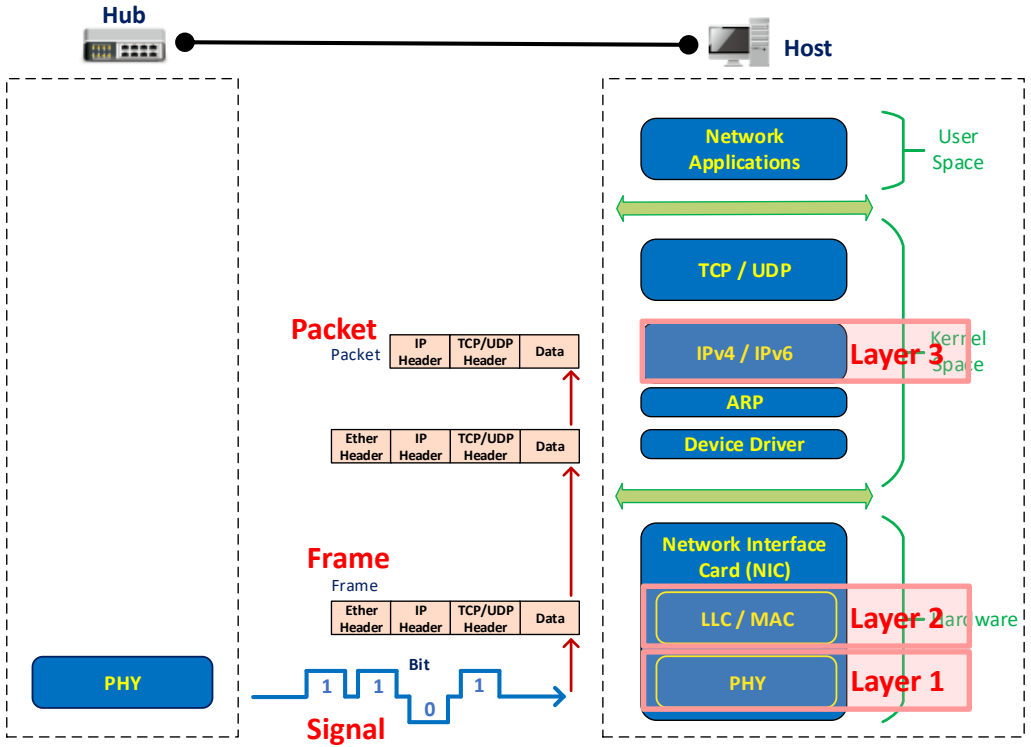
(14) When signals reach a layer-1 hub, the hub forwards the signals directly.

- On a hub, signals are not transformed into a frame for checking the frame's MAC header.
- A hub amplifies signals' power and forwards them out. Doing this extends the signal transmission range and increases the success rate of signal decoding at receiver sites.



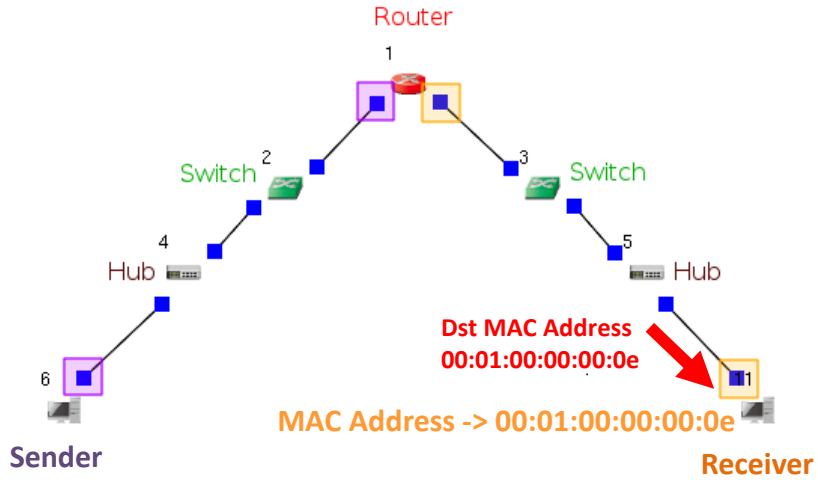
(15) When signals reach the receiver host, the signals are first transformed into a frame for checking MAC header. Next, the frame's MAC header is removed so that the frame becomes a packet. Finally, the destination IP address of the packet is checked.

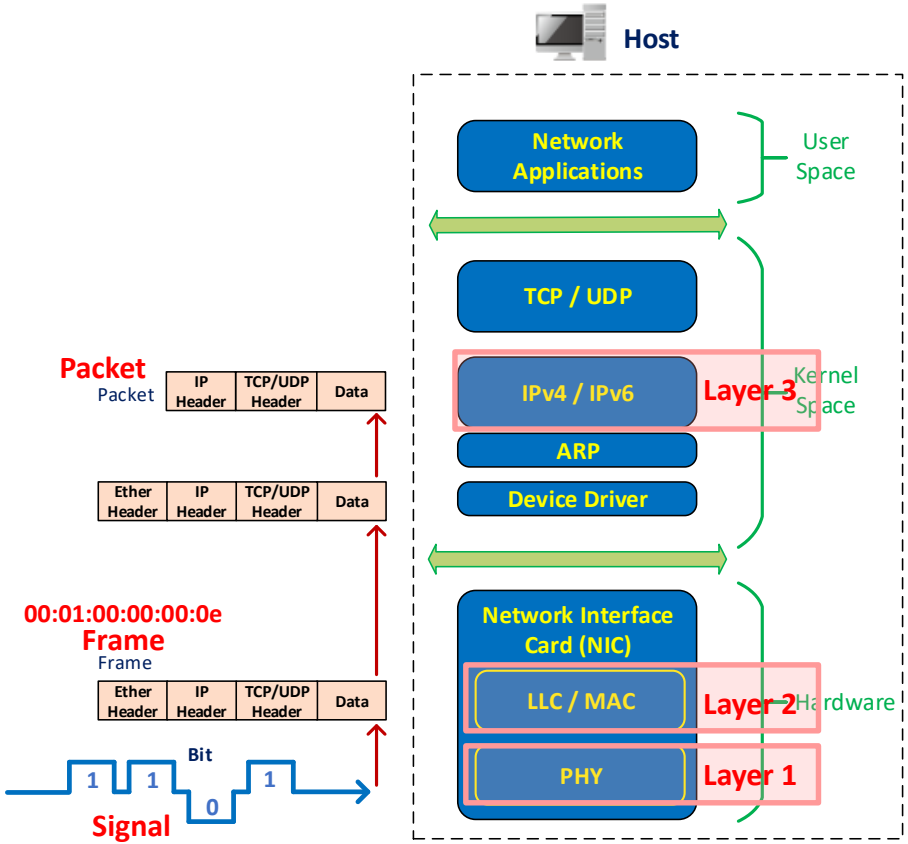
- After the signals are transformed into a frame, the destination MAC address retrieved from the frame's MAC header is checked to determine if this frame reaches the MAC-addressing destination or not. If the answer is yes, the MAC header of the frame is removed so that the frame becomes a packet. The packet is passed to layer 3 and the destination IP address in the IP header is checked to determine if this packet reaches the IP-addressing destination or not.



(15-1) MAC Addressing Checking

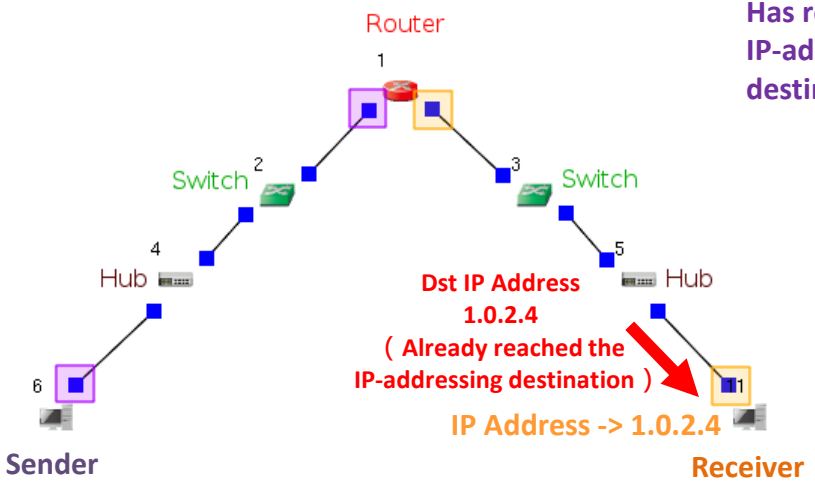
- The network message travels from the right NIC of the router to the receiver host.
- First, the destination MAC address of the MAC header is compared with the NIC's MAC address to confirm that the message reaches the MAC-addressing destination.
- Next, the MAC header is removed and the message is passed to layer 3.

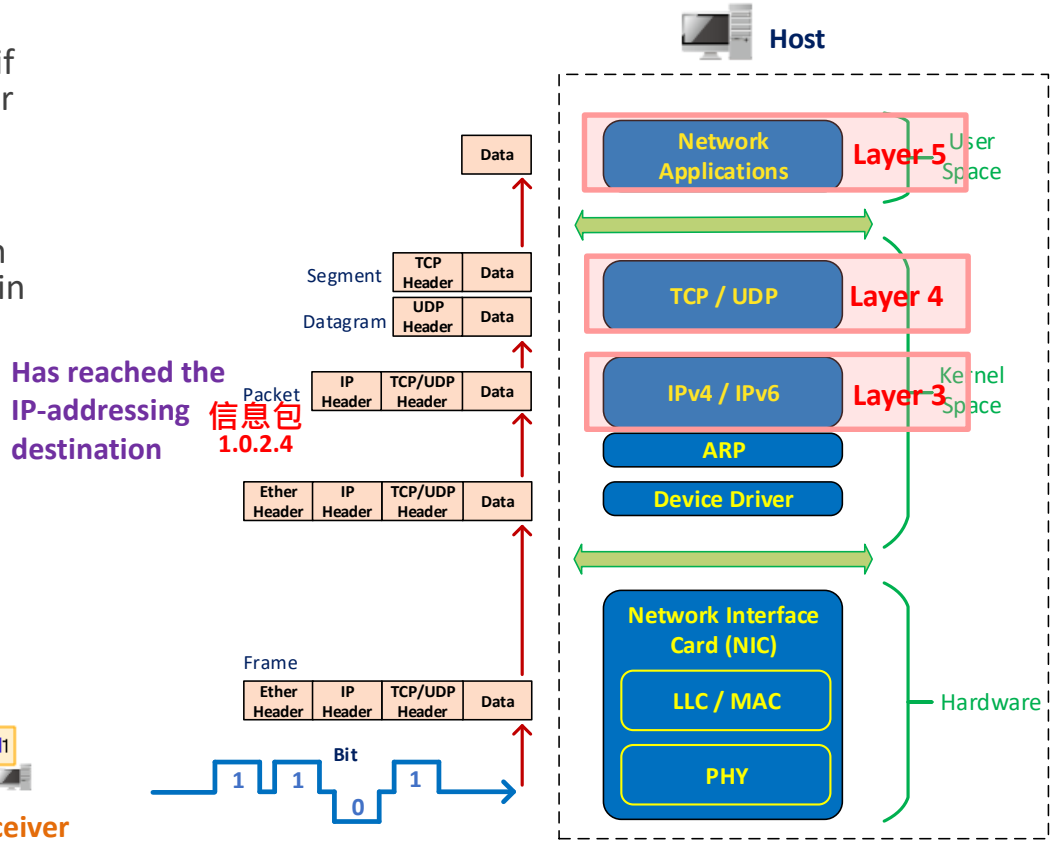




(15-2) IP Addressing Checking and Port Number Checking

- If the prefix of a message is an IP header, the message is called a packet.
- When a packet reaches layer 3, the destination IP address of the IP header is checked to determine if this packet reaches its IP-addressing destination or not. If yes, the IP header of the packet is removed and the rest of the message is passed to layer 4.
- The layer-4 TCP or UDP protocol dispatches the message to a layer-5 network application program according to the destination port number carried in the TCP or UDP header.





Summary

Review of Points

- In a network, how far is the addressable range of MAC address? How far is the addressable range of IP address?
- During the encapsulation process of a network message, both IP addressing and MAC addressing are involved. Describe 1) how the network layer (layer 3) queries the next destination NIC's IP address according to the final destination NIC's IP address? 2) how to translate the next destination NIC's IP address to its MAC address by ARP?