## Introduction To IP Routing

IP routing, the fundamental mechanism for directing IP packets, facilitates the transmission of data across extensive TCP/IP networks, bridging the gap from the originating device that assembles the IP packet to the intended recipient device. In essence, IP routing serves as the conduit for IP packets from the sending host to the target host. This end-to-end routing process hinges on the network layer's intelligence, which resides within both hosts and routers.

The sending host leverages Layer 3 principles to construct an IP packet, subsequently forwarding it to its default gateway, often referred to as the default router. This procedure mandates the utilization of Layer 3 logic within the routers as well.

These routers scrutinize the destination address contained within the packet against their routing tables, thereby determining the optimal path for forwarding the IP packet. Moreover, the routing process heavily relies on the intricacies of **data-link and physical** attributes at each network link. IP routing seamlessly traverses various network types, including serial WAN links, Ethernet WAN links, Ethernet LANs, wireless LANs, and countless others, all of which adhere to specific data-link and physical layer standards.

These underlying devices and protocols facilitate the movement of IP packets throughout the TCP/IP network by encapsulating and transmitting these packets within data-link layer frames.

## IP Routing Process

The routing process begins with the host creating the IP packet. The host must first determine if the destination IP address is within its local subnet. It does this by using its own IP address and subnet mask to define the range of local addresses.

### Forwarding the IP Packet to the Default Gateway

Consider a scenario where Host A wants to send data to Host B (172.16.2.9). Host A, with IP address 172.16.1.9/24, identifies its local subnet as 172.16.1.0–172.16.1.255. Since Host B's IP address (172.16.2.9) is outside this range, Host A forwards the packet to its default gateway (172.16.1.1). To do this, Host A encapsulates the IP packet in an Ethernet frame, setting the destination MAC address to that of the default gateway's G0/0 interface.

### Routing Step 1: Frame Processing Decision

Upon receiving a data-link frame, the network device decides whether to process it. It checks the frame's destination MAC address against its own. If the frame is intended for the device, it proceeds to the next step; otherwise, it considers routing the frame.

### Routing Step 2: De-encapsulation of the IP Packet

If the device processes the incoming frame, it de-encapsulates it, removing the data-link layer header and trailer to reveal the IP packet. This step allows access to the packet's source and destination IP addresses.

### Routing Step 3: Determining the Next Hop

The device consults its routing table to determine the next hop for the IP packet. It matches the destination IP address with entries in the table to identify the appropriate next-hop router or interface, essential for proper forwarding.

### Routing Step 4: Creating a New Data-Link Frame

With next-hop information determined, the device prepares a new data-link frame to encapsulate the IP packet. The frame's destination MAC address is set to the next-hop router's MAC address or the MAC address of the outgoing interface on the device. The source MAC address is the device’s own MAC address, along with other necessary control information.

### Routing Step 5: Transmitting the Data-Link Frame

Finally, the device transmits the newly encapsulated data-link frame onto the network. The transmission adheres to the data-link layer protocols and standards, such as Ethernet or Wi-Fi. The frame traverses the network towards the next-hop router or the final destination, repeating the process until the packet arrives at its intended endpoint.

Association For
Cyber Security

Association for Cyber Security looks forward towards your success!
Contact us: +91 7938001181 | Email: info@acs.albussec.com