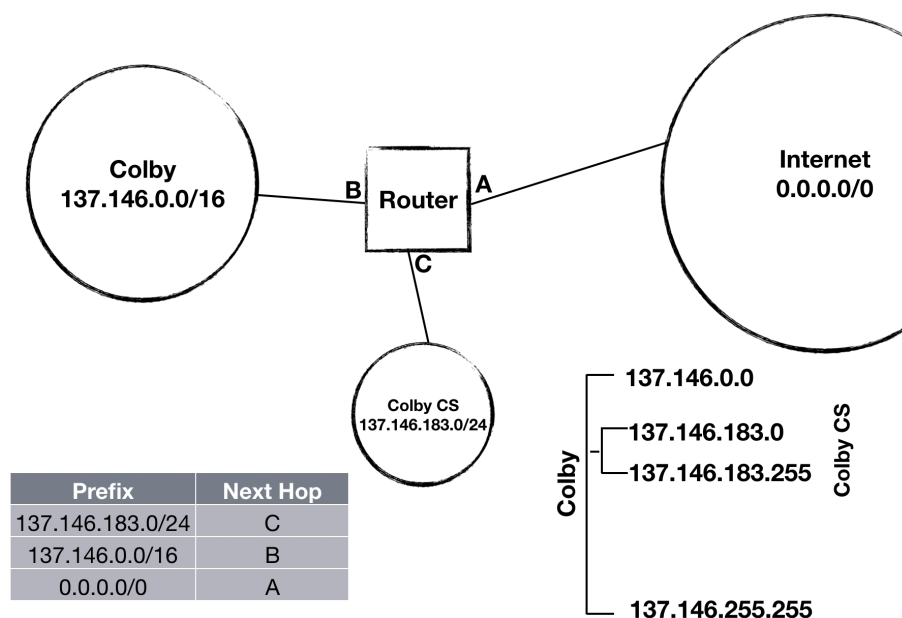


Networking Fundamentals (III)

Longest Prefix Match

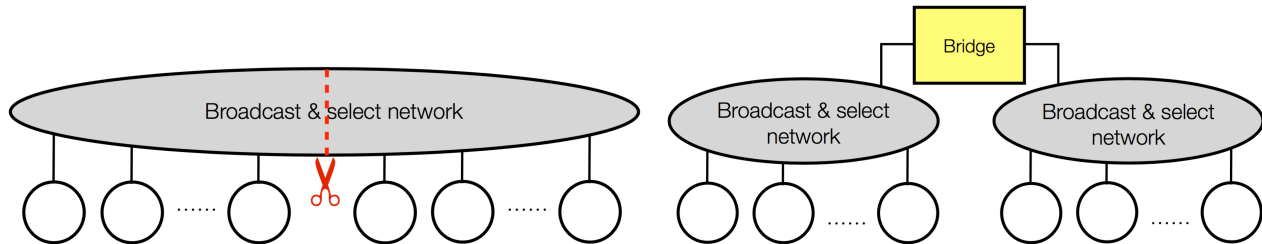
- We know that if the leftmost N bits of an IP address are the same as those in the subnet ID, the IP address belongs to the subnet specified by the prefix.
- However, the IP range of subnets are nested usually. For example, as show in the figure below, the IP range for CS department is nested in the range for Colby.
- So, if the destination of a packet is an IP of CS department, how does the router route the packet to the appropriate subnet?
- It uses the **longest prefix match**, forwarding the packet to the hop that connects a subnet whose prefix is the most specific matching (aka **matching entry with the longest prefix length**).



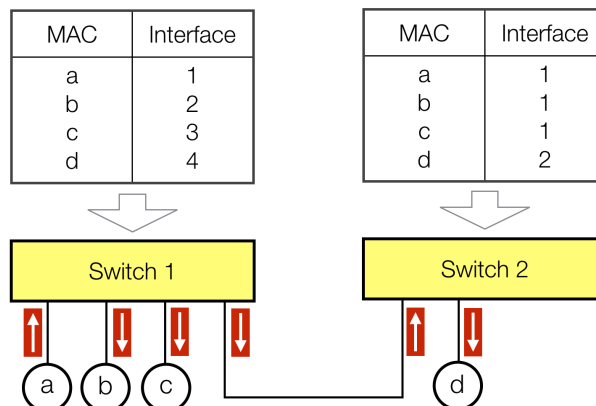
Dest Address	Matches	Used
137.146.3.15	B, A	B
137.146.183.35	C, B, A	C
200.100.0.15	A	A

Bridging

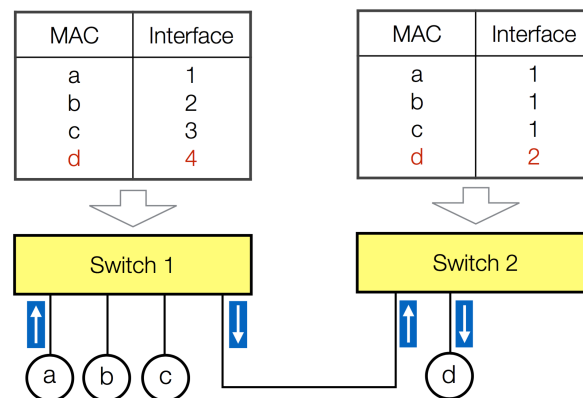
- Due to the broadcast nature of the underlying medium of L2 networks, it is difficult to scale up the L2 networks. The signal attenuates as the distance between two nodes increases, so as for the interference. No to mention the limited number of ports on a L2 devices (e.g., hub and switch).
- However, introducing more routers are expensive in terms of monetary cost and labor cost.
- Therefore, bridging is introduced to limit the scope of broadcasting and extend the reach of L2 networks.



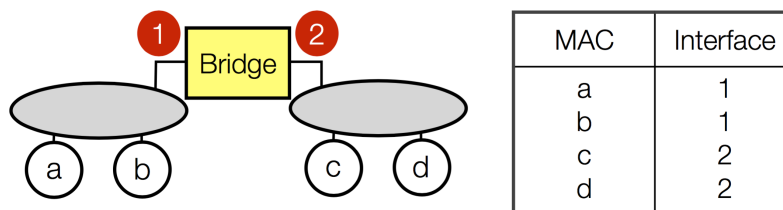
- The bridge sits between the sections of a subnet.
- In a simple subnet, it can be a wire connecting two sections of a subnet. In a complex subnet, it can be a switch connecting different sections.
- Please note that each **section** of the subnet **can** be a L2 network **connecting hosts via a switch**. Different from the L2 broadcast and selected networks that connect hosts via hubs, unicast packets can be forwarded to the destination by a switch without broadcasting to every host in that section. Each **switch maintains** a **switching table**, mapping MAC addresses to appropriate interfaces.
- Let's use a simple scenario to explain how the broadcast and unicast will work.
- The simple scenario is that a subnet is divided into two sections. Nodes in a section are connected via a switch. The two sections are bridged by a wire connecting two switches.
- If a node a in section 1 wants to broadcast a packet, all nodes in the subnet, including the nodes in a different section, will receive the packet.



- In the above example, all nodes in section 1 receive the packet, and the packet is also forwarded to section 2 via the cable connecting between these two sections. Switch 2 delivers the packets to all nodes in section 2.
- In this broadcast case, the bridging table maintained by both switches are not used. As the dest address of the packet is a broadcast address. So, the packet is forwarded to every node in the subnet.
- Let's use the same scenario to explain how the unicast works.
- If a node a in section 1 wants to send a packet to a node d in section 2, switch 1 will use its switching table to forward the packet.



- Once switches build up the switching table, they can tell the interface to the desired node. When node a pass the packet to switch 1, switch 1 will look up the table and forward it to interface 4, as that interface can direct the packet to d. Once the packet arrives at switch 2, switch 2 will look up its table and forward the packet to interface 2, as that interface connects node d.
- In a more complex scenario, a bridging switch connects two sections of the same subnet. It **learns** node locations from passing traffic and stores them in its switching table.



- As shown in the above figure, the bridge connects two subnet sections and its switching table maps the MAC addresses of hosts in different sections to the interface that directly connects to that section.

Special Use IPv4 Addresses

- **10.0.0.0/8**, **172.16.0.0/12**, **192.168.0.0/16** - Private network
 - Range: 10.0.0.0 ~ 10.255.255.255, 172.16.0.0 ~ 172.31.255.255, 192.168.0.0 ~ 192.168.255.255
 - Scope: Private network
 - Purpose: Used for **local communications within a private network**
 - Commonly used for home, office, and enterprise networks
 - To **delay IPv4 address exhaustion**
 - May **use without approval from regional Internet registry**
 - Are **not allocated to any specific organization**
 - IP **packets addressed from these** addresses **cannot be transmitted through the public Internet**, and so if such a private network needs to connect to the Internet, it must do so via a network address translator (NAT) gateway, or a proxy server.
- **127.0.0.0/8** - Loopback
 - Range: 127.0.0.0 ~ 127.255.255.255
 - Scope: Host
 - Purpose: Used for **loopback address** to the local host
- REF: https://en.wikipedia.org/wiki/Reserved_IP_addresses
- A complete lists from RFC 5735