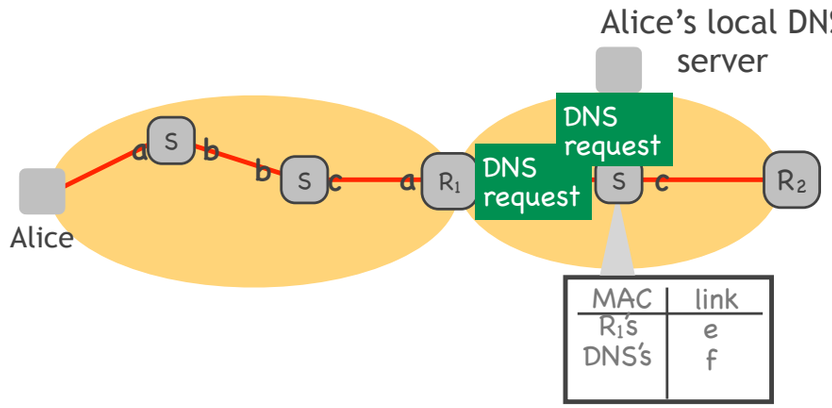
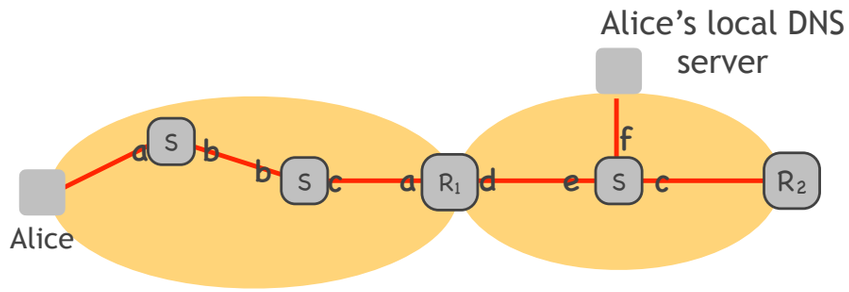
9. R_1's network layer forwards DNS request
   - it now knows what dst MAC address to use

src MAC: R_1's
dst MAC: DNS server's

src IP: Alice's
dst IP: DNS server's



The switches forward traffic within local IP subnets between end-systems and routers



End-systems and routers need MAC addresses

Switches do not (*)

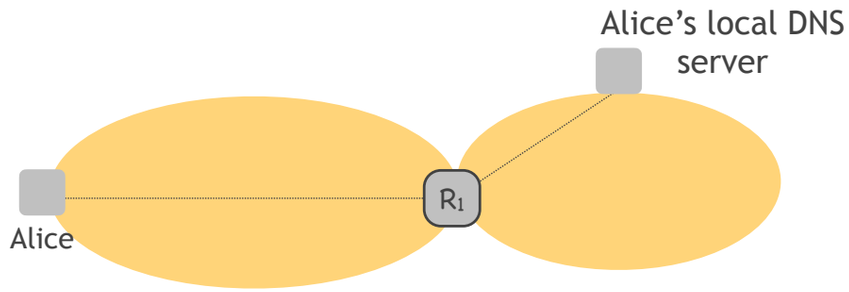
So:

In an Ethernet IP subnet, there are end-systems and routers, and there are Ethernet switches, which forward packets between end-systems and routers.

End-systems and routers need MAC addresses (otherwise how would the Ethernet switches know where to forward each packet?)
However, Ethernet switches do NOT need MAC addresses in order to forward packets.

(*) But, as we will see, switches do have MAC addresses for practical reasons.

The routers forward traffic end-to-end between source and destination end-systems



End-systems need IP addresses

Routers do not (*)

Similarly, in the Internet, there are end-systems, and there are routers, which forward packets between end-systems.

End-systems need IP addresses (otherwise how would the routers know where to forward each packet?)
However, routers do NOT need IP addresses in order to forward packets.

(*) But, as we will see, routers do have IP addresses for practical reasons (and also to do NAT, which we have already seen).

Switch and router addresses

- Yet both switches and routers have both MAC and IP addresses
  - *1 MAC address + >= 1 IP address per network interface*
- For various practical reasons
  - *to be reachable by an administrator (*)*
  - *for link testing (*)*
  - *a router needs an IP address to respond to ARP requests*
  - *a router that acts as a NAT gateway needs an IP address for NAT*

(*) A network administrator often needs to log into a network device and inspect or configure it. For this reason, network devices also act as standard computers, i.e., one can login to them and run processes. To be reachable as a standard computer, a network device must have at least one MAC address and one IP address (though not necessarily 1 MAC address and 1 IP address **per network interface**).

(**) About link testing: Imagine that an administrator wants to test a specific physical link (does it lose or corrupt packets? what is its latency?) One way to do this is to put packets on one end of the link and count/inspect the packets that arrive at the other end. One way to implement such a simple test, is to have sender and receiver processes (e.g., a simple UDP sender and receiver) running on the devices that are at the two ends of the link. In order for these processes to exchange packets over the specific link, each of the two network interfaces at the two ends of the link must have 1 MAC and at least 1 IP address.

Three network “levels”

- IP subnet
  - *L2 forwarding, L2 learning*
- Autonomous System (AS)
  - *IP (L3) forwarding, intra-domain routing*
- Internet
  - *IP (L3) forwarding, inter-domain routing (BGP)*

Informally speaking, there are three “levels” of networks:

1. IP subnets. Inside each IP subnet, there are link-layer switches, which do L2 forwarding and populate their forwarding tables through L2 learning.
2. Autonomous Systems (ASes). Inside each AS, there are many IP subnets, interconnected by routers. These routers do IP forwarding and populate their forwarding tables through the AS’s intra-domain routing protocol.
3. The Internet. Inside the Internet, there are many ASes, interconnected by their border routers. These also do IP forwarding, and they participate both in their AS’s intra-domain routing protocol AND the inter-domain routing protocol (BGP).