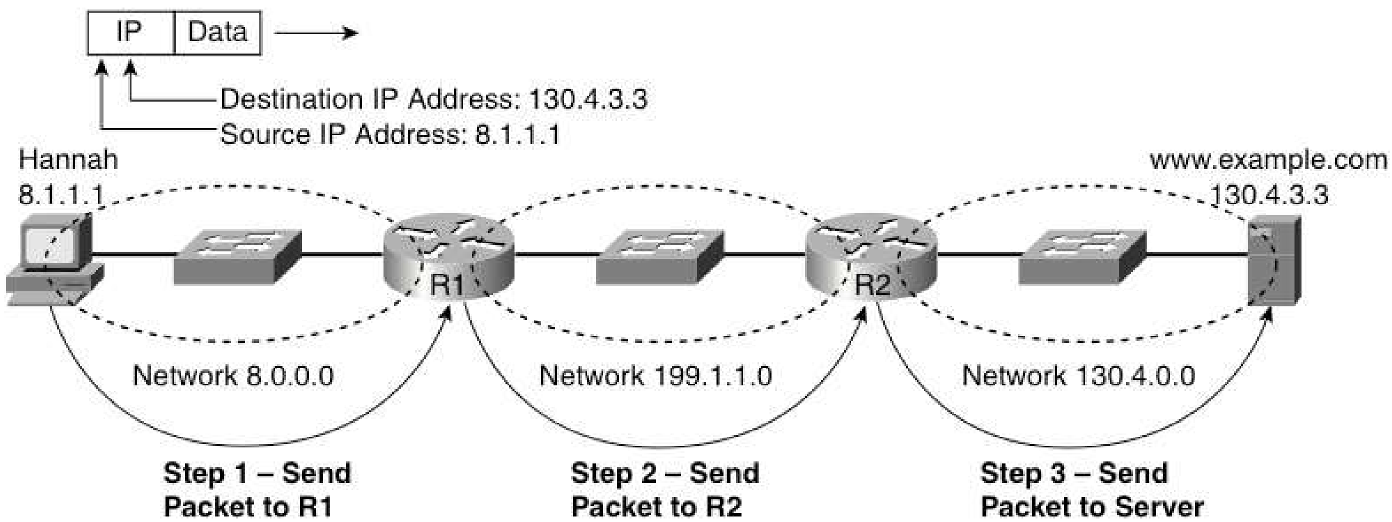
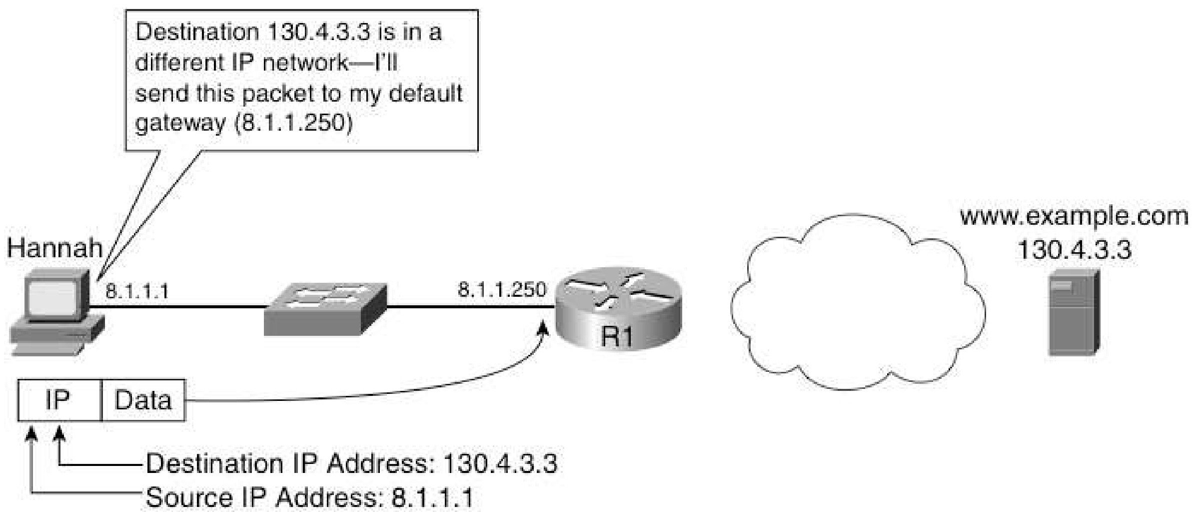
Simplicity in routing

- Routers sit at the intersections within an internet
  - Forward packets from one network to another
    - Some of those packets originated on one of the connected networks
    - Many are simply "passing through"
- Routers may have a huge number of packets to forward
  - Efficiency is key
  - Routing rules are kept as simple as possible



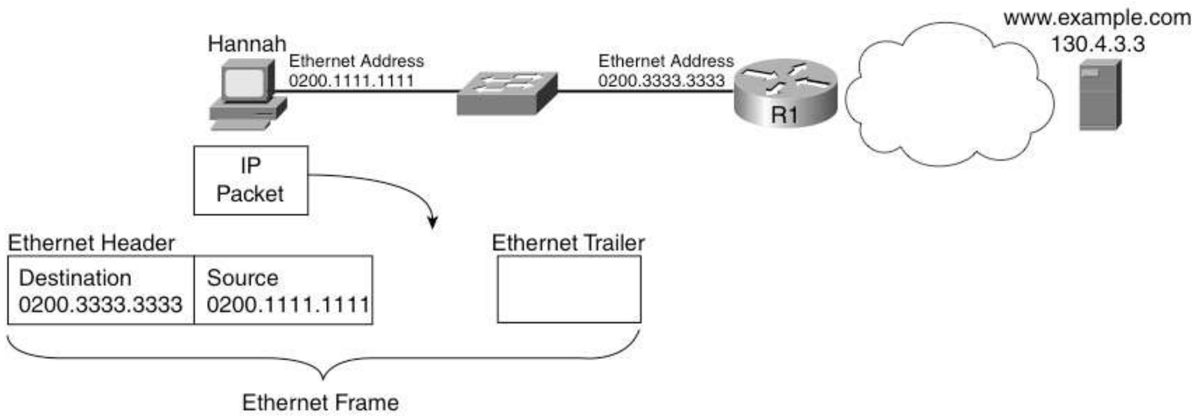
Default routers

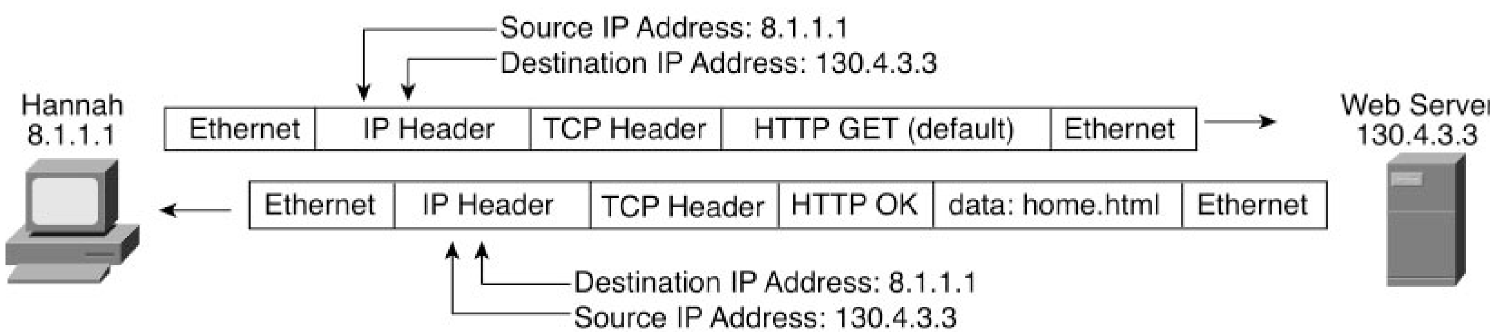
- Every host is configured with the IP address of its network's default router (or gateway)
  - Manually or via Dynamic Host Configuration Protocol (DHCP)
  - Whenever a packet is addressed to a destination on a different network, it is sent to the default router
    - That router examines the packet and decides how to route it
      - If the recipient is on one of its connected networks, it simply delivers it to that host
      - Otherwise, it forwards the packet to another router on one of its connected networks



Encapsulating packets in frames

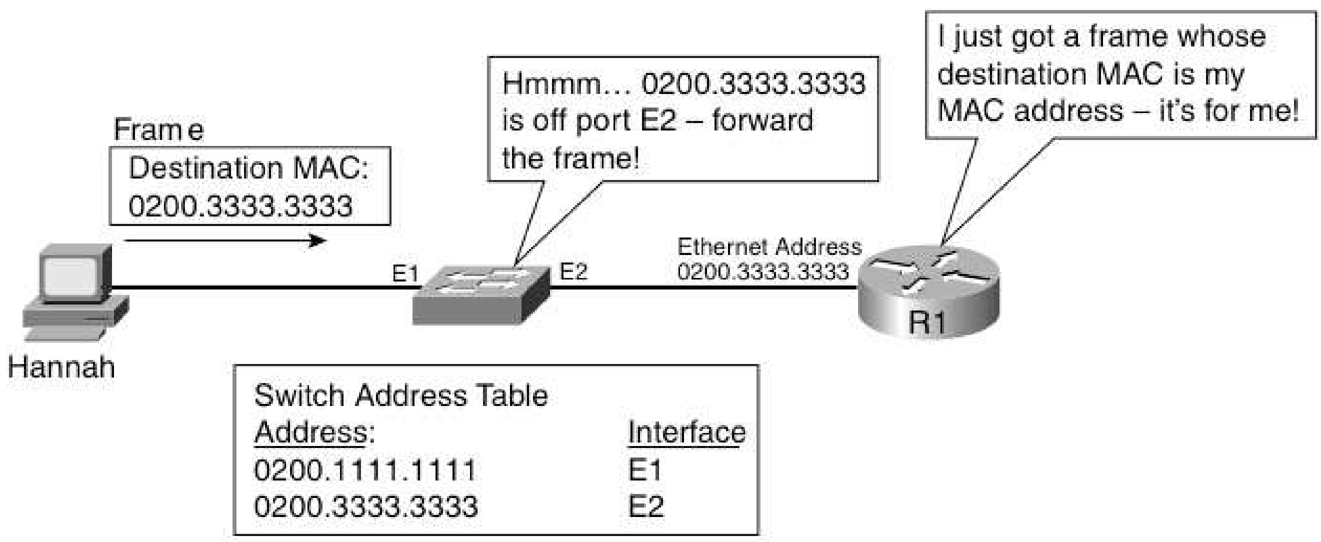
- Only valid Ethernet frames can travel on an Ethernet network
  - IP packets must therefore be encapsulated in Ethernet frames
    - Same is true of other network types as well





Addressing the default router

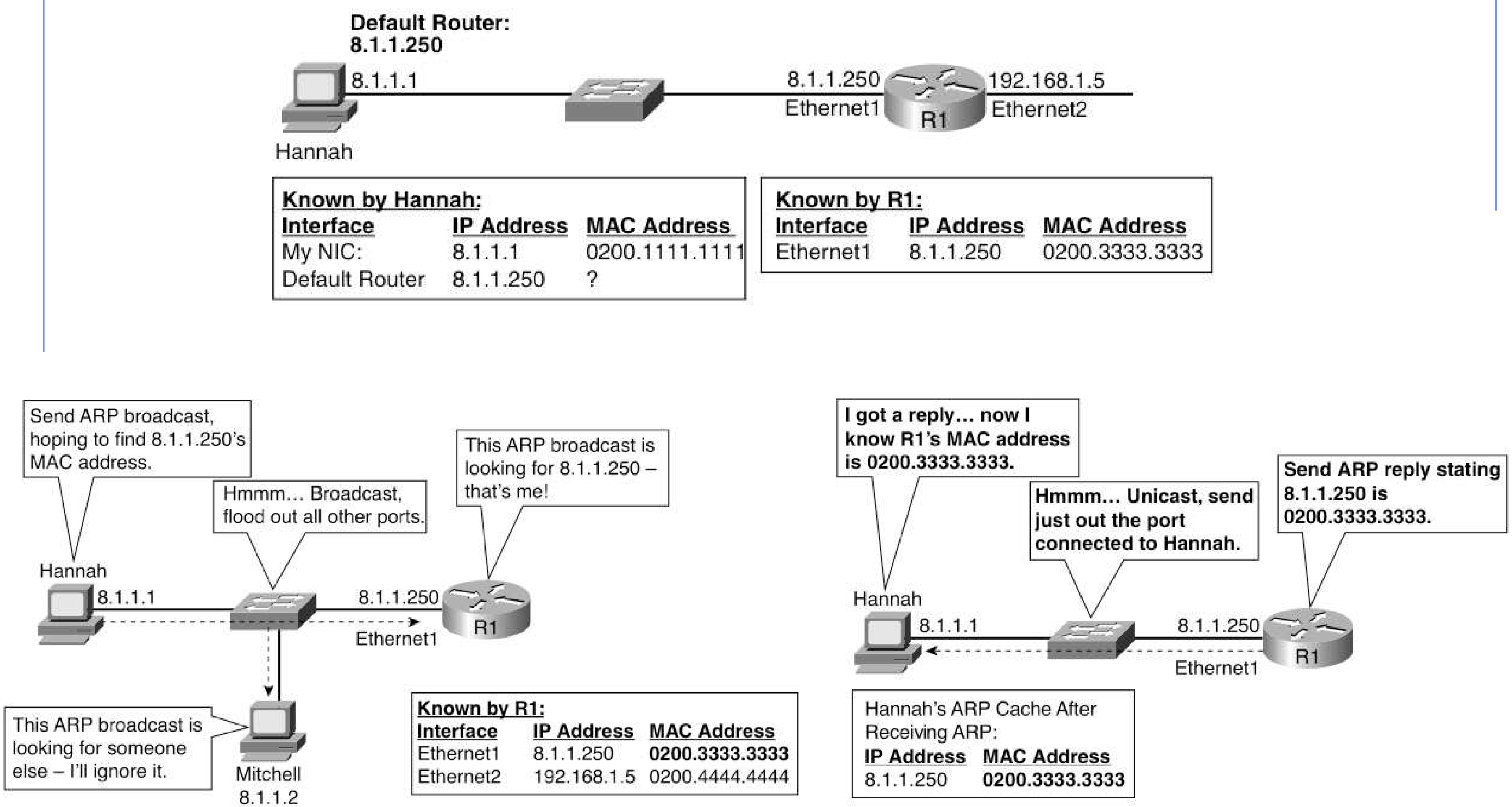
- IP headers only hold the IP address of the packet's ultimate destination
  - There's no field to hold the IP address of the default router
  - But since the packet must be encapsulated in an Ethernet frame, that frame can be addressed to the default router's MAC address
    - But hosts are only configured with default router's IP address
    - Somehow that IP address must be converted to a MAC address



Address Resolution Protocol (ARP)

- Used by sender to learn MAC address of default router
  - Sender sends an ARP request message to the Ethernet broadcast address
    - Request simply asks any host with included IP address to respond with its MAC address
  - Owner of IP address in request sends an ARP response back to the sender's unicast address
    - Response includes responder's MAC address
  - Sender stores answer in ARP cache for subsequent use

ARP illustrated



Intelligent intersections

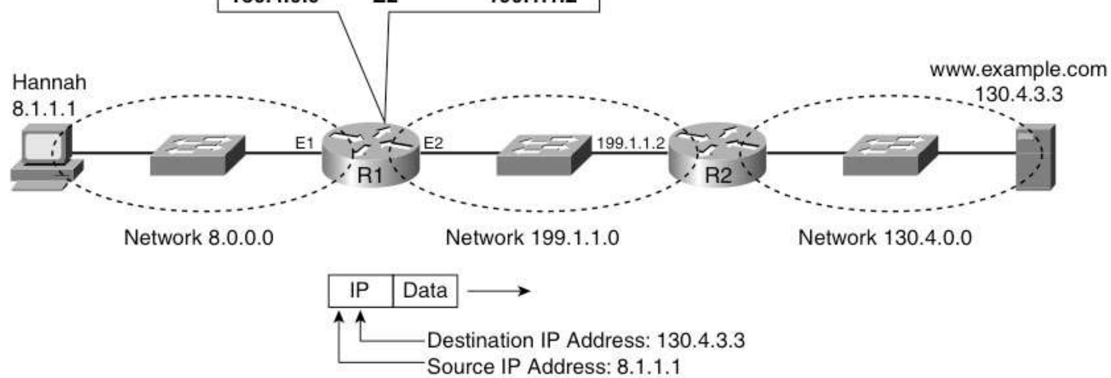
- Routers are like intelligent intersections
  - Packets are entirely passive
  - Routers make all the decisions and move packets closer to their destinations
- The decision making is called routing logic
  - Router checks each incoming frame's FCS and discards erroneous frames
  - For good frames, router decapsulates IP packet from frame
  - Router examines packet and decides where to forward it
  - Having made a forwarding decision, router encapsulates packet in a new frame and sends it

Routing tables

- Each router builds its own routing table
  - Matches network and subnet numbers to forwarding instructions
    - Forwarding instructions include outgoing interface and (if necessary) address of next hop router
      - The next hop router is simply the one that gets the packet closer to its destination

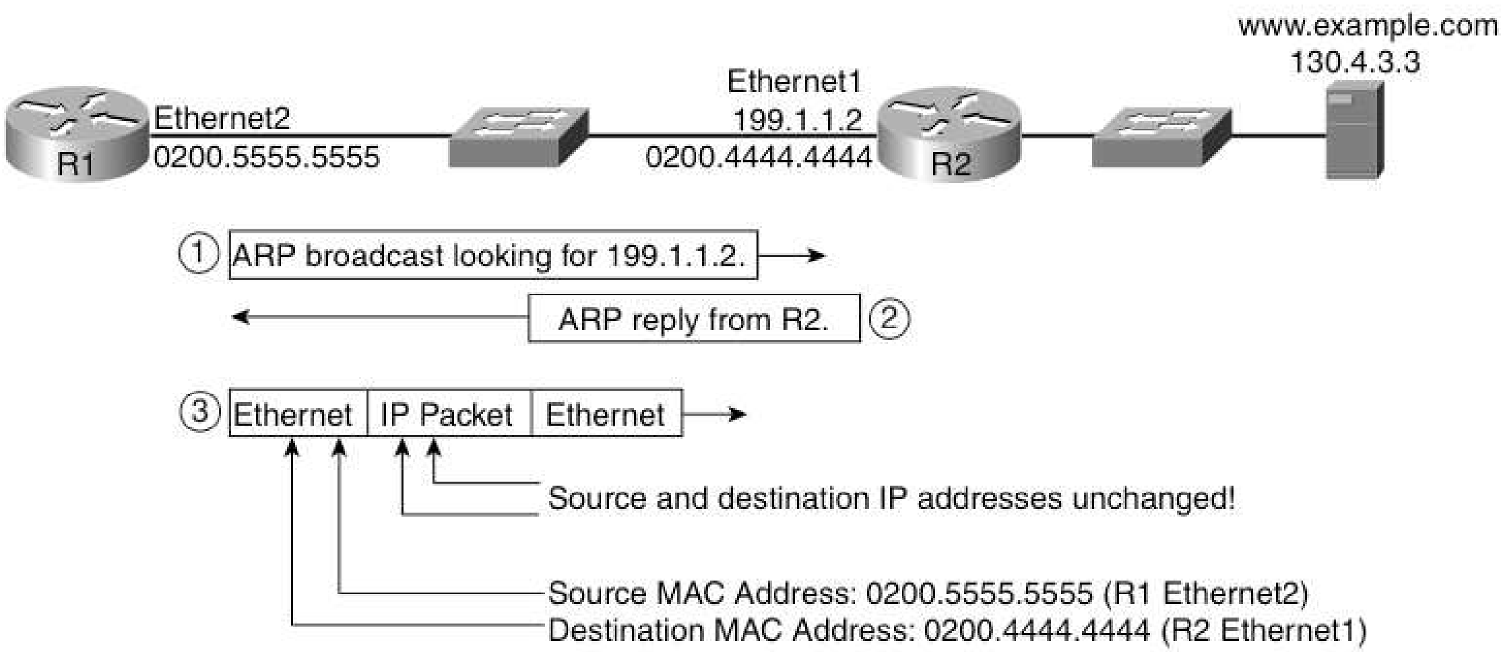
R1 Routing Table

Destination Network	Interface	Next-Hop Router
8.0.0.0	E1	N/A
199.1.1.0	E2	N/A
130.4.0.0	E2	199.1.1.2



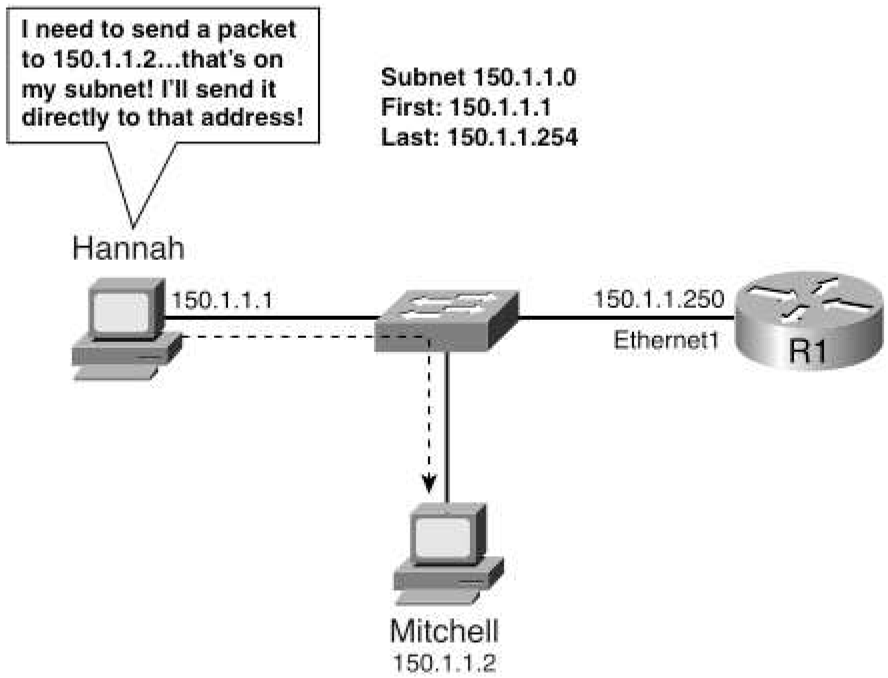
ARP in routing

- The routing table identifies next hop routers by IP address
  - If that IP address is not already in the router's ARP cache, the router broadcasts an ARP request to find the corresponding MAC address
  - Uses that MAC address on outgoing interface in routing table to forward packet to next hop router



The last hop

- In some cases, the destination will be on the same subnet as the source
- If not, the packet eventually gets forwarded to a router on the same subnet as the destination
- In both cases, the packet needs to be encapsulated in a frame addressed to the MAC address of the destination host
  - If necessary, an ARP broadcast is used to find that MAC address



Starting a routing table

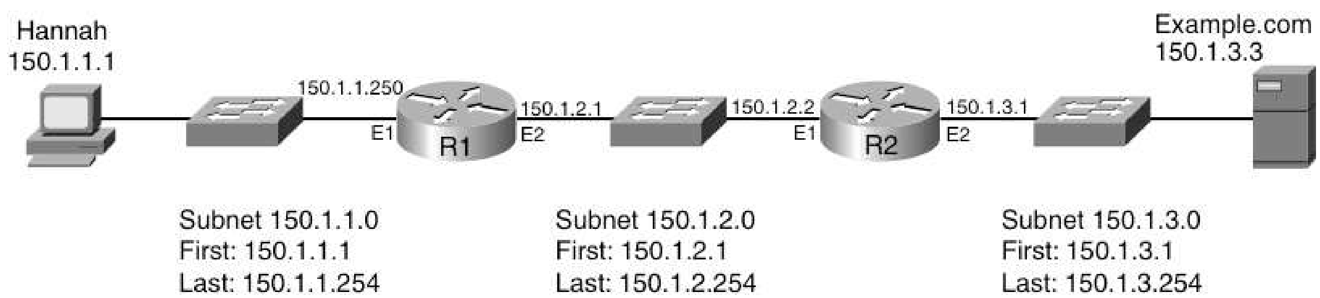
- Routing is only as good as the info in the routing tables
  - Each router must build its own routing table
- Start locally
  - Router is configured with info about its interfaces
    - Has IP address and subnet mask for each interface
    - Can use that info to determine subnet number for each interface
      - So router knows how to route packets for each of those subnets
      - And that no next hop router is necessary to reach them
      - Adds a route for each of these subnets to its routing table

R1 Routing Table

Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A

R2 Routing Table

Destination Subnets	Interface	Next-Hop Router
150.1.2.0	E1	N/A
150.1.3.0	E2	N/A

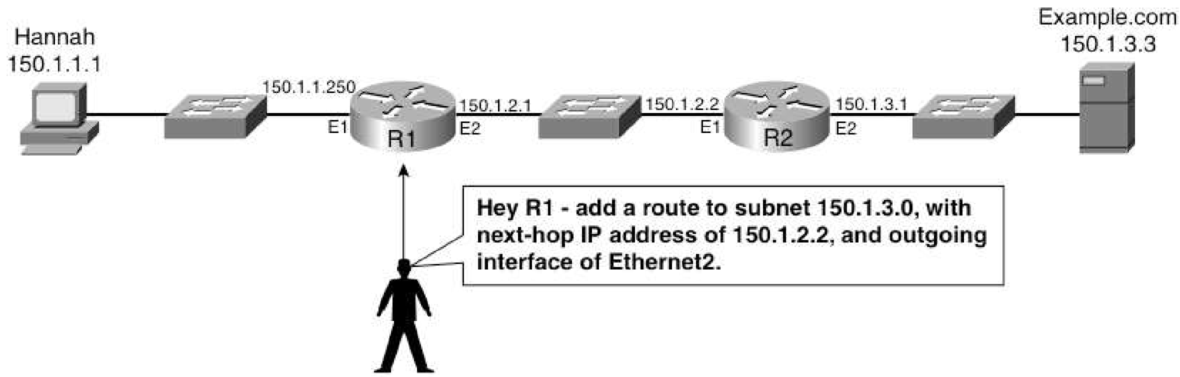


Adding static routes

- Possible to add static routes to a routing table
  - Added to the routing table manually by an administrator
  - Include subnet number, interface, and next hop router
    - Tell router how to route packets to that subnet
  - Functional, but labor intensive to maintain, so seldom used in practice

R1 Routing Table

Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A
150.1.3.0	**E2**	**150.1.2.2**



Learning new routes

- Most routers use a routing protocol to exchange routing info with other routers
  - Routing updates are simply a list of all the subnets in a router’s routing table
  - Receiving router can add those subnets to its routing table, listing incoming interface and sending router as next hop router
- Each router can tell other routers about the routes it knows and learn about new routes from others
  - Allows routers to build and maintain their routing tables autonomously

Learning new routes illustrated – part 1

1

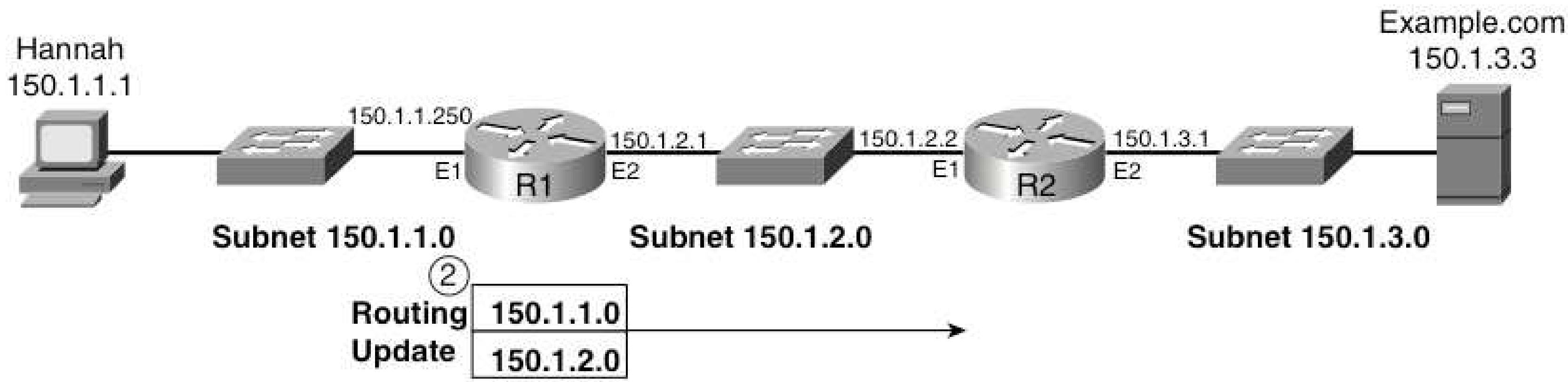
R1 Routing Table - Before Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A

1

R2 Routing Table - Before Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.2.0	E1	N/A
150.1.3.0	E2	N/A



3

R1's Routing Table – After Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A

3

R2 Routing Table - After Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.2.0	E1	N/A
150.1.3.0	E2	N/A
150.1.1.0	**E1**	**150.1.2.1**

Learning new routes illustrated – part 2

1

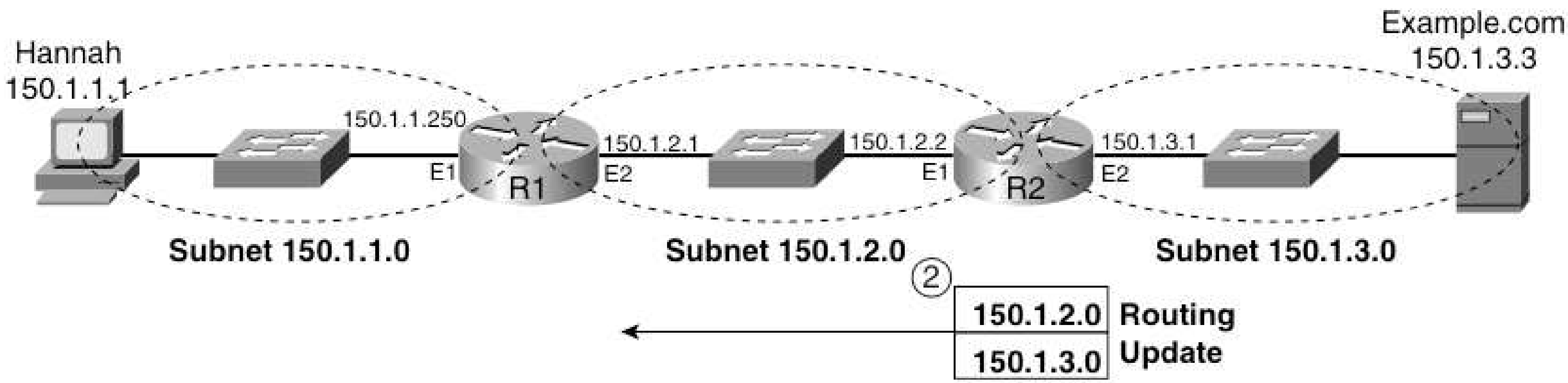
R1 Routing Table - Before Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A

1

R2 Routing Table - Before Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.2.0	E1	N/A
150.1.3.0	E2	N/A
150.1.1.0	**E1**	**150.1.2.1**



3

R1's Routing Table – After Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A
150.1.3.0	**E2**	**150.1.2.2**

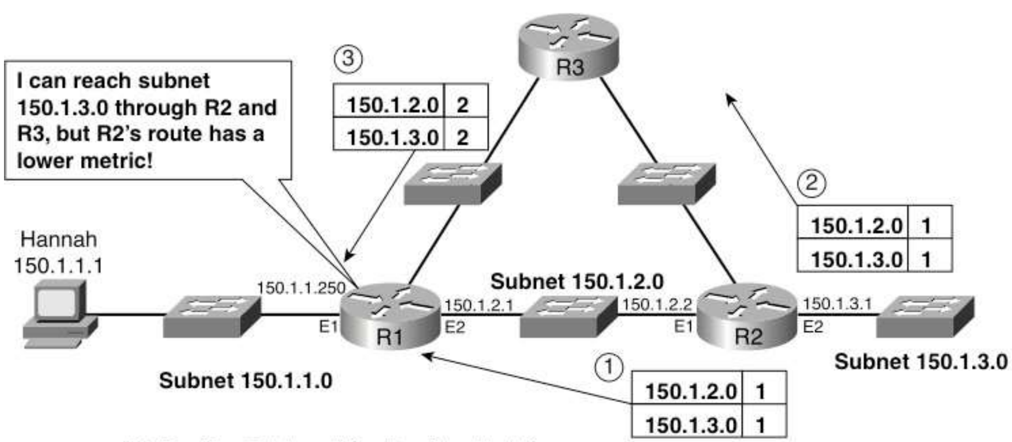
3

R2 Routing Table - After Routing Update

Destination Subnets	Interface	Next-Hop Router
150.1.2.0	E1	N/A
150.1.3.0	E2	N/A
150.1.1.0	**E1**	**150.1.2.1**

Finding the best route

- Most internets contain redundant connections
  - When choices exist, routers need to know which is best
  - Routing protocols provide a numeric metric with each route included in a routing update
    - Lower values indicate better routes
    - Router typically enters all routes in routing table
      - Uses route with lowest metric if available, alternate route otherwise



Destination Subnets	Interface	Next-Hop Router
150.1.1.0	E1	N/A
150.1.2.0	E2	N/A
150.1.3.0	**E2**	**150.1.2.2**

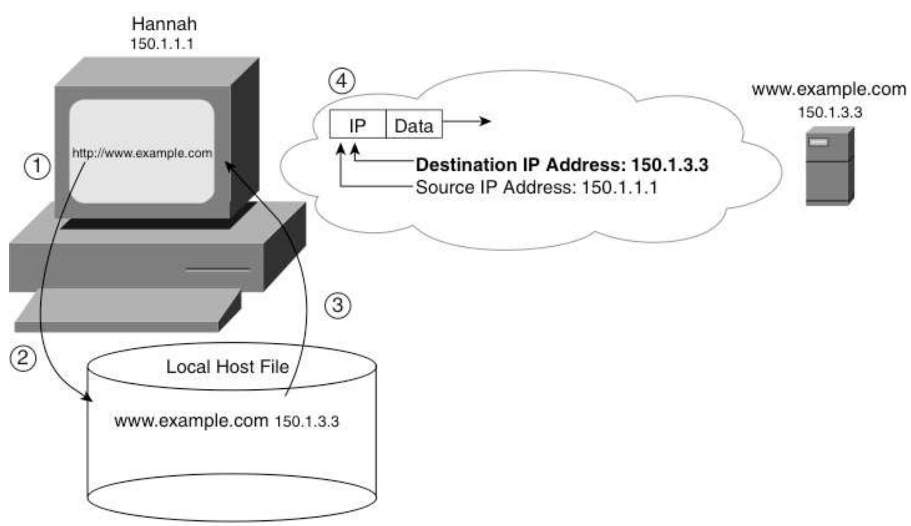
Routing protocols

Routing Protocol	Public/Proprietary	Interior/Exterior
Routing Information Protocol (RIP)	Public	Interior
Interior Gateway Routing Protocol (IGRP)	Proprietary	Interior
Open Shortest Path First (OSPF)	Public	Interior
Enhanced IGRP (EIGRP)	Proprietary	Interior
Border Gateway Protocol (BGP)	Public	Exterior

- Interior routing protocols are primarily intended for use within a single company
- Exterior routing protocols are primarily intended for use between different companies or between ISPs and their customers
- IGRP and EIGRP belong to Cisco Systems
- BGP is used on the Internet

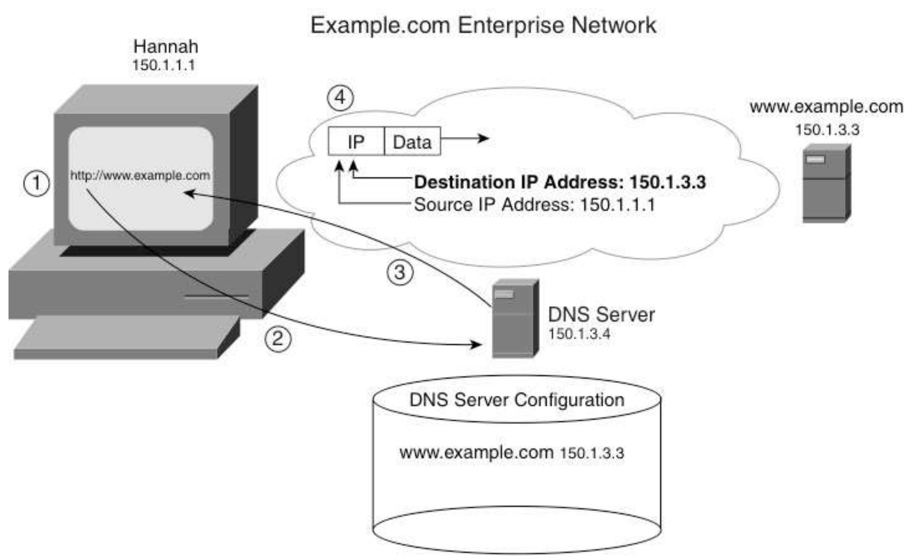
Name resolution

- IP addresses are unwieldy for humans
  - Many computers are therefore also identifiable by hostname
  - But IP headers must contain IP addresses
- Name resolution is process of converting from hostname to IP address
  - One approach is to look it up in a local host file
    - But host files can't possibly be comprehensive and are maintenance intensive
    - So seldom used in practice



Domain Name Service (DNS)

- Most hosts use DNS for name resolution
  - Defines protocols for name resolution and the structure of hostnames
  - Most enterprise networks and ISPs include at least one DNS server
    - Every host on the network is configured with the IP address of one or more DNS servers
      - May be manually configured or automatically configured via DHCP
    - DNS server is essentially a shared host file for the network
      - It knows the hostname and IP address of every host on that network
      - Hosts send a DNS resolution request to the DNS server whenever they require name resolution
      - An administrator must keep the list on the DNS server up to date for all the hosts on the network



Root DNS servers

- Each enterprise DNS server is responsible only for resolving host names for its network
  - Doesn't necessarily know how to resolve hostnames outside its network
- Each enterprise DNS server is configured with the IP addresses of one or more root DNS servers
  - When asked to resolve a hostname it doesn't know, a DNS server will contact a root DNS server for assistance
  - Root DNS servers don't resolve individual hostnames, they resolve domain names
    - Domain names identify enterprise networks, each with their own enterprise DNS server(s)
    - Each root DNS server maintains a list associating a domain name with the IP address(es) of the DNS server(s) for that domain
    - When a root server is asked to resolve a hostname, it returns the IP address of an enterprise DNS server that should know how to resolve it
    - The original DNS server must then send another name resolution request to that domain's enterprise DNS server
    - Most servers will store the answer in a local cache for future reference

Root DNS servers illustrated