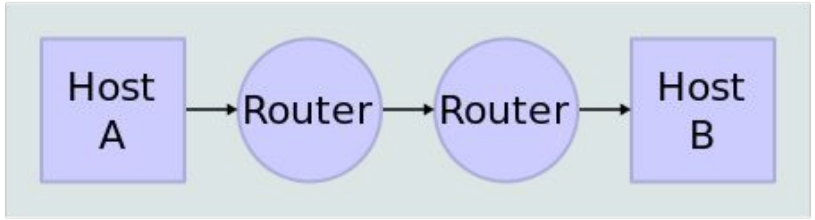
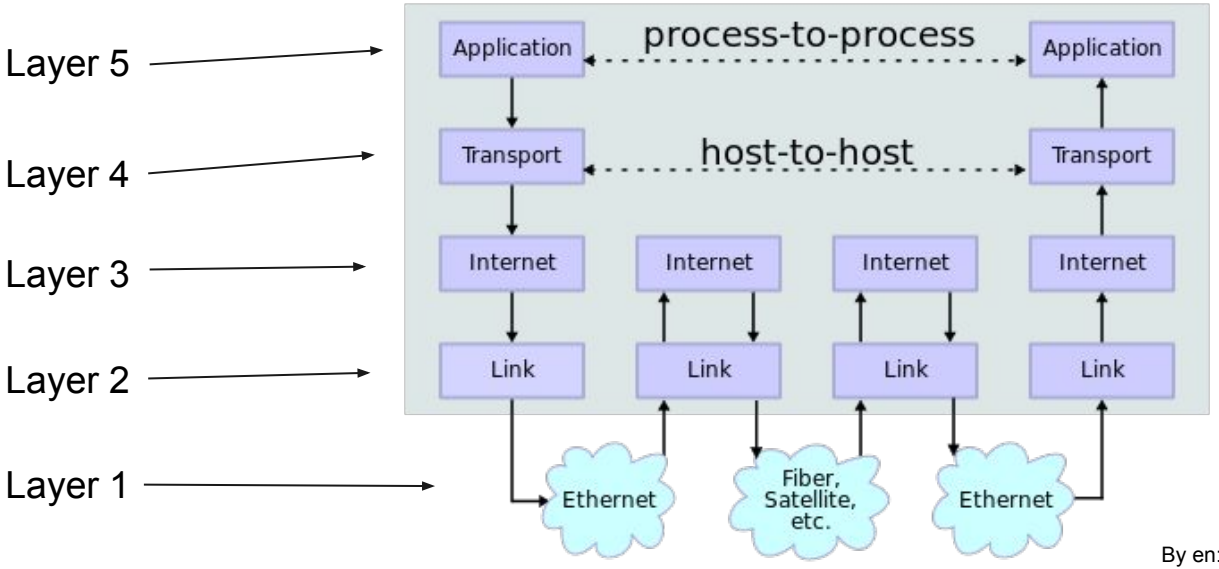
Network Security I

Ethernet/IP Routing, ARP

Network Topology

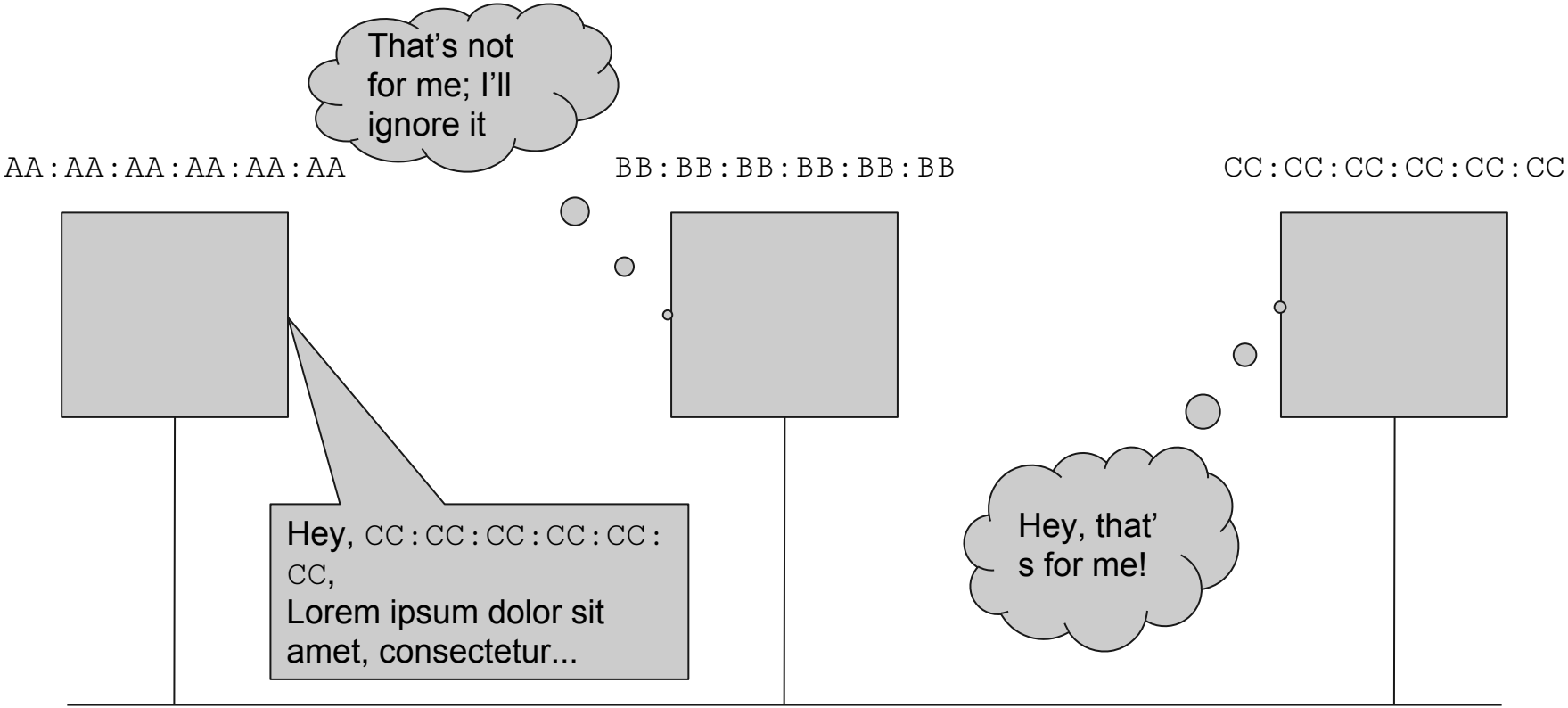


Data Flow

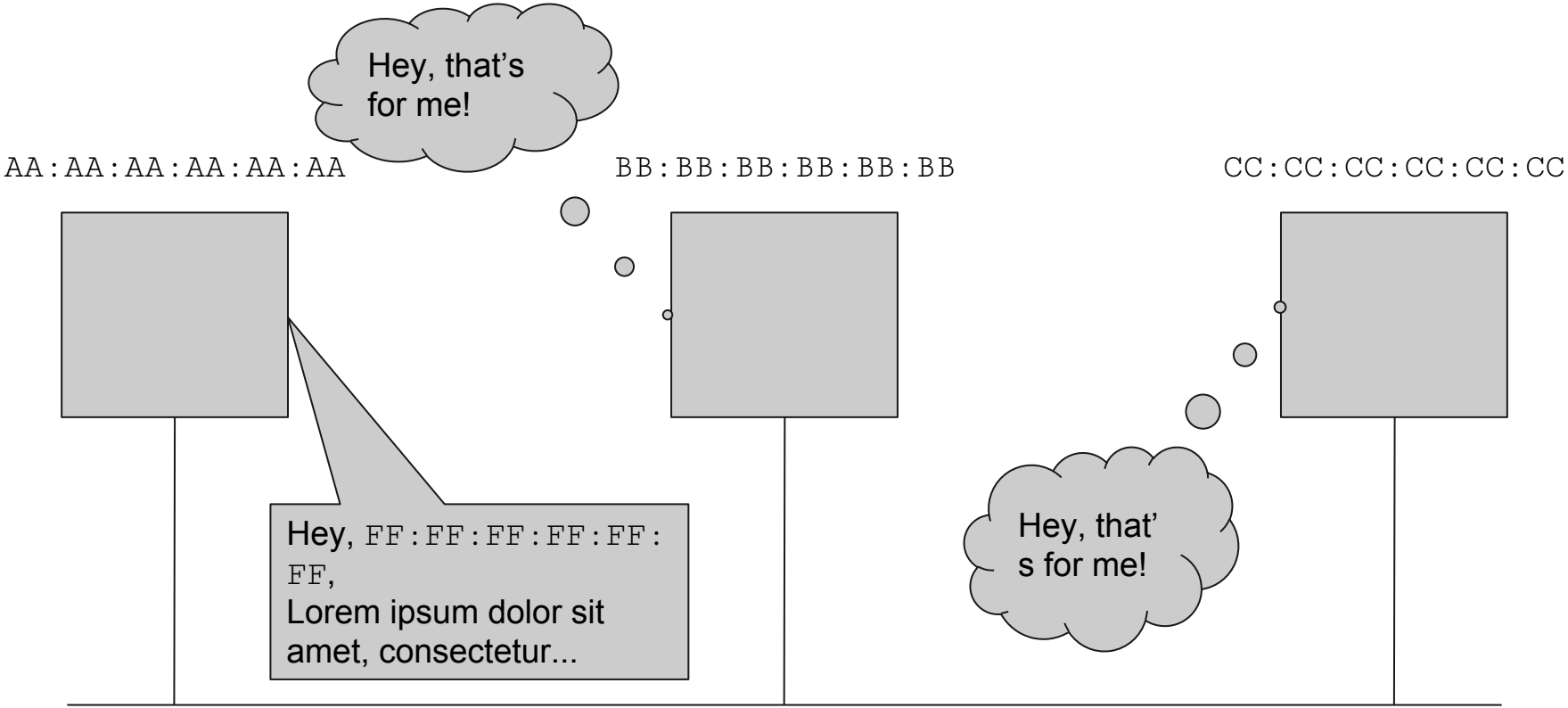


Basics of Ethernet

- 48-bit MAC (Media Access Control) Addresses
  - Globally unique, assigned by manufacturer
- Broadcast medium
  - Everybody connected to a wire
  - Everybody hears all traffic
  - Ignores everything not for them



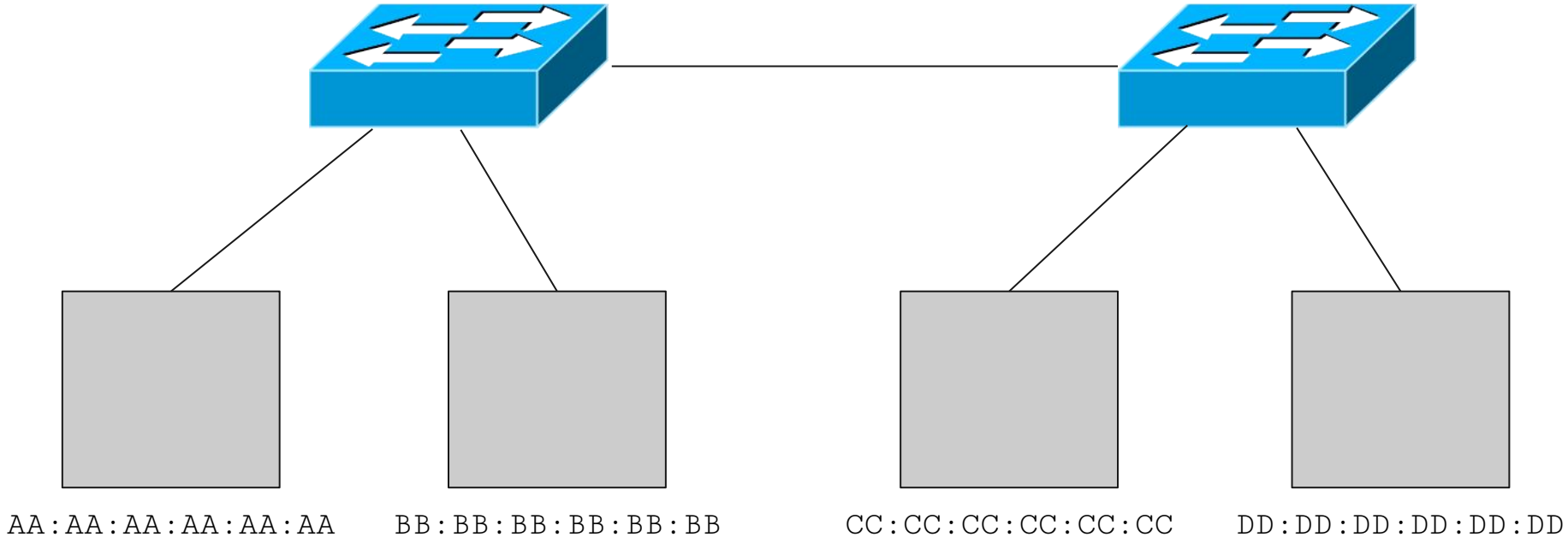
Ethernet is a broadcast medium



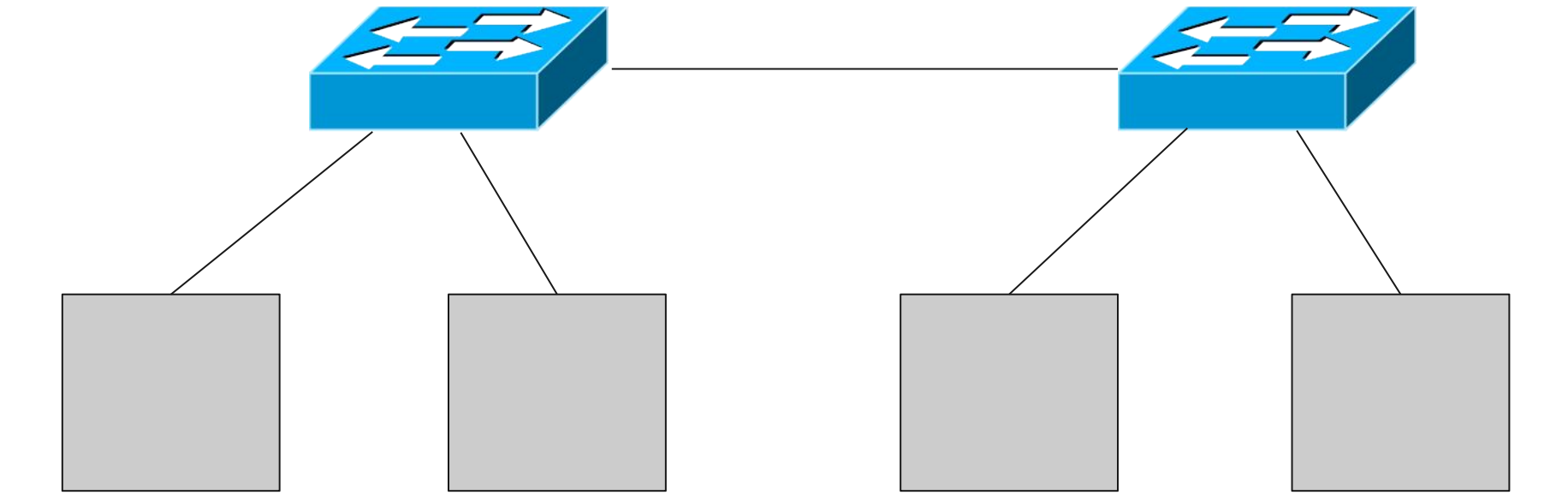
The broadcast address is `FF:FF:FF:FF:FF:FF`

Basics of Ethernet

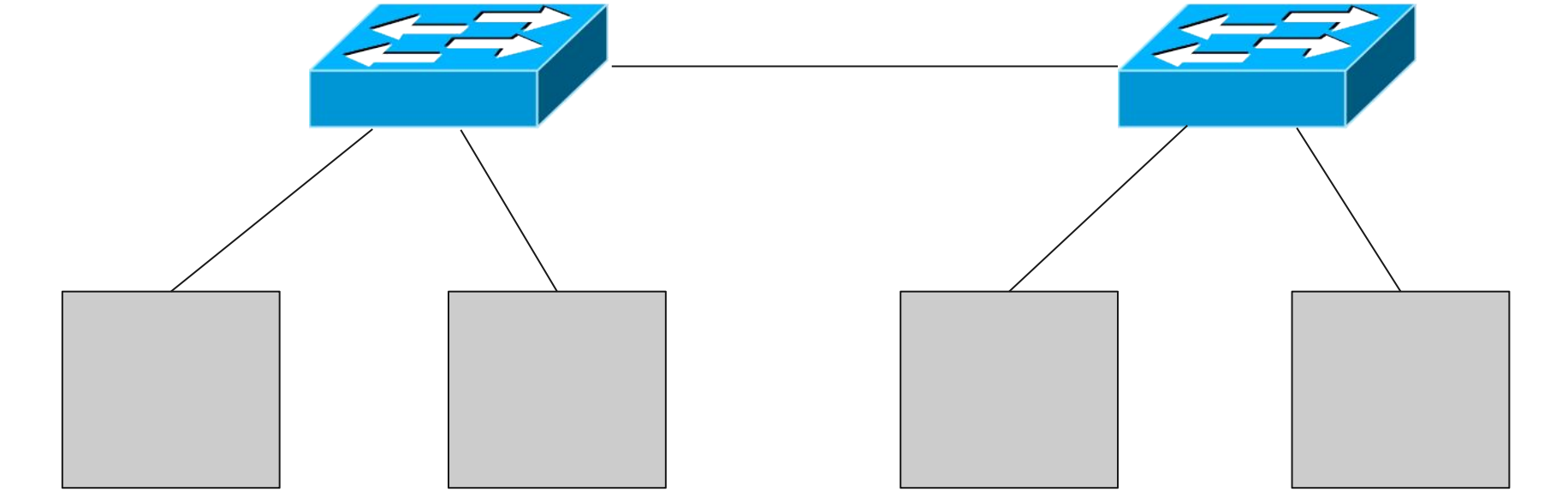
- 48-bit MAC (Media Access Control) Addresses
  - Globally unique, assigned by manufacturer
- Broadcast medium
  - Everybody connected to a wire
  - Everybody hears all traffic
  - Ignores everything not for them
- What about really large networks? Switches!



- Each link is its own broadcast medium

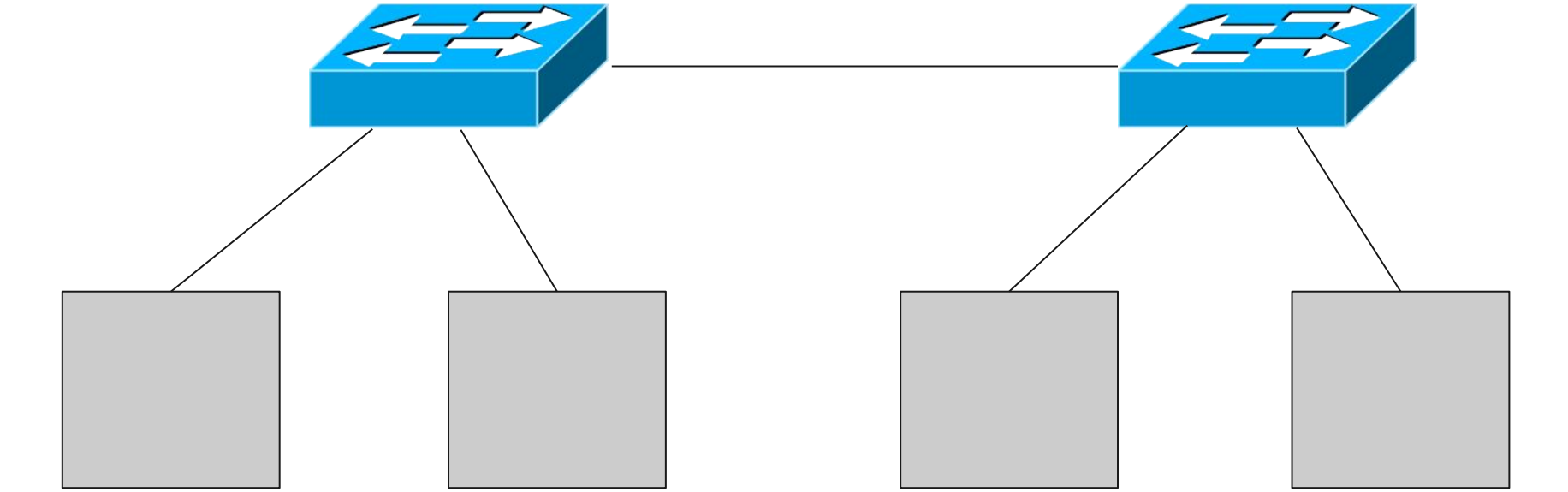


- Each link is its own broadcast medium
- Problem: switches don’t know where anyone is



- Each link is its own broadcast medium
- Problem: switches don't know where anyone is
- Solution: broadcast on all other links

- If you see a frame from a MAC you don't know about, remember it!
- Future traffic to that MAC goes direct

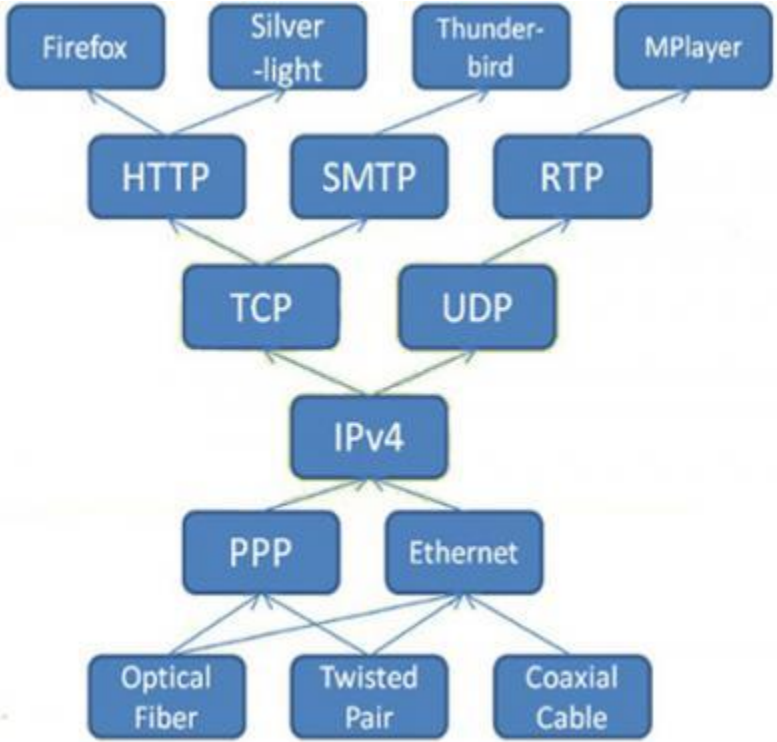


- Each link is its own broadcast medium
- Problem: switches don't know where anyone is
- Solution: broadcast on all other links

- If you see a frame from a MAC you don't know about, remember it!
- Future traffic to that MAC goes direct
- Networks must not have loops!

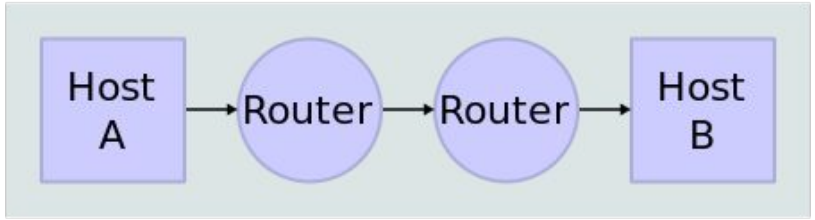
Basics of IP Routing

- Inter-net Protocol: connects multiple networks
- “Network” here means link-layer network
  - e.g., Ethernet
  - WiFi
- Each link-layer protocol is different
- On top of the link layer, it’s all IP
- Enables communication between incompatible networks

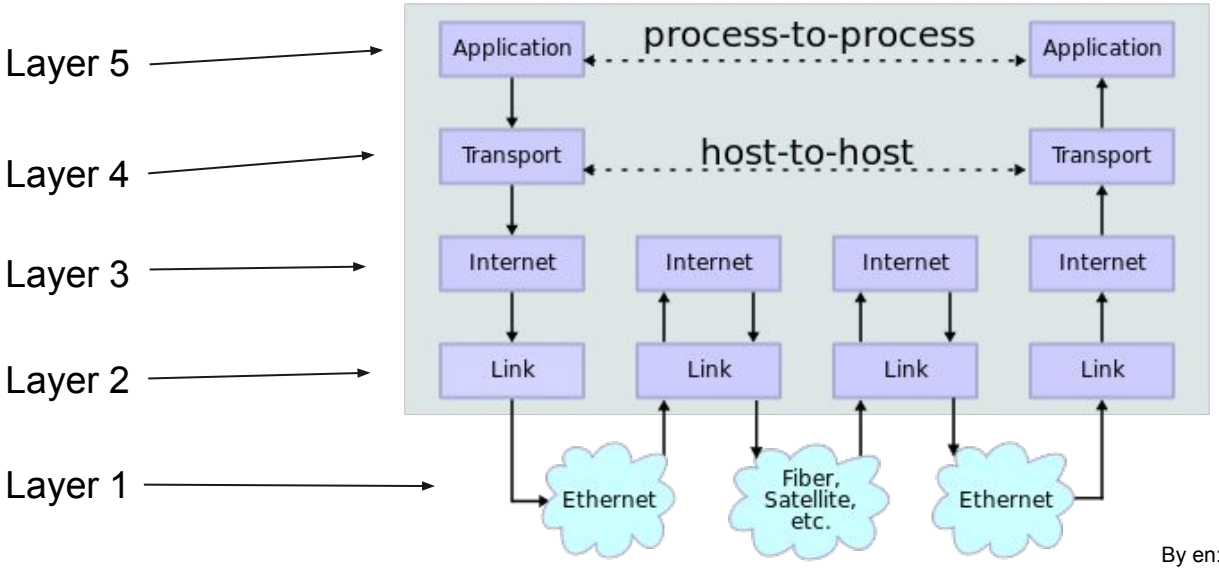


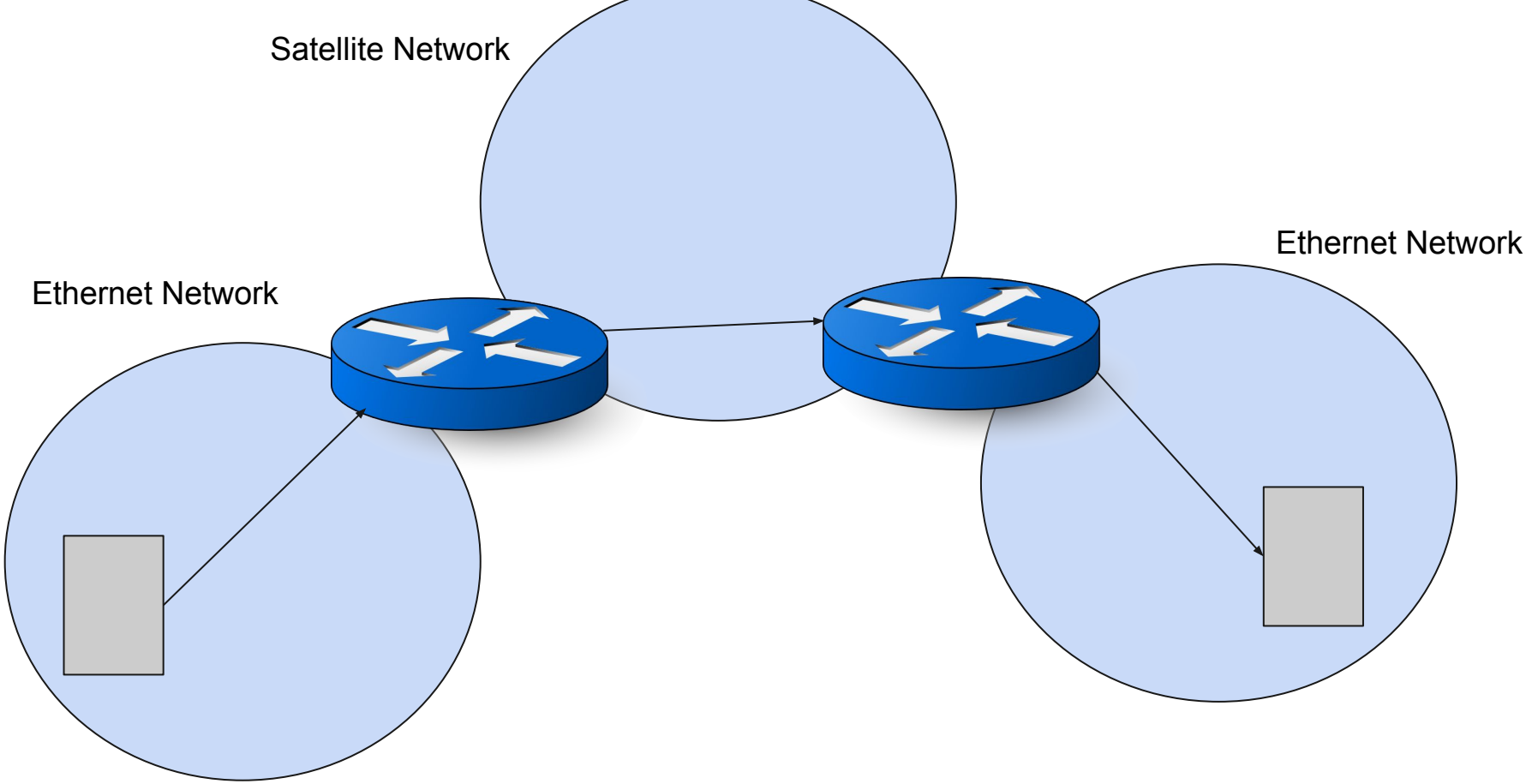
“IP Hourglass”

Network Topology



Data Flow





Note the analogy to the previous slide,
and which protocols are used where

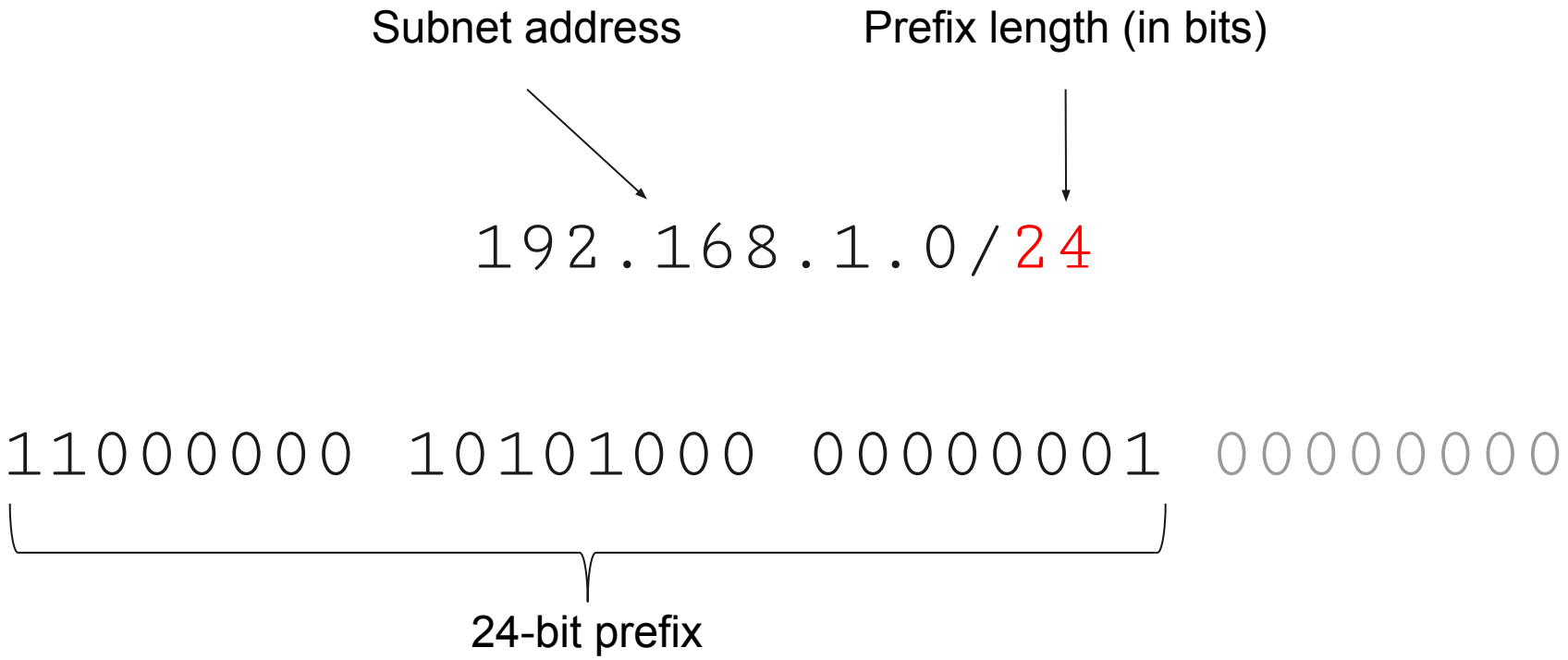
Basics of IP Routing

- Problem: 2^32 = ~4Bn possible IP addresses
- How to remember where each one is?

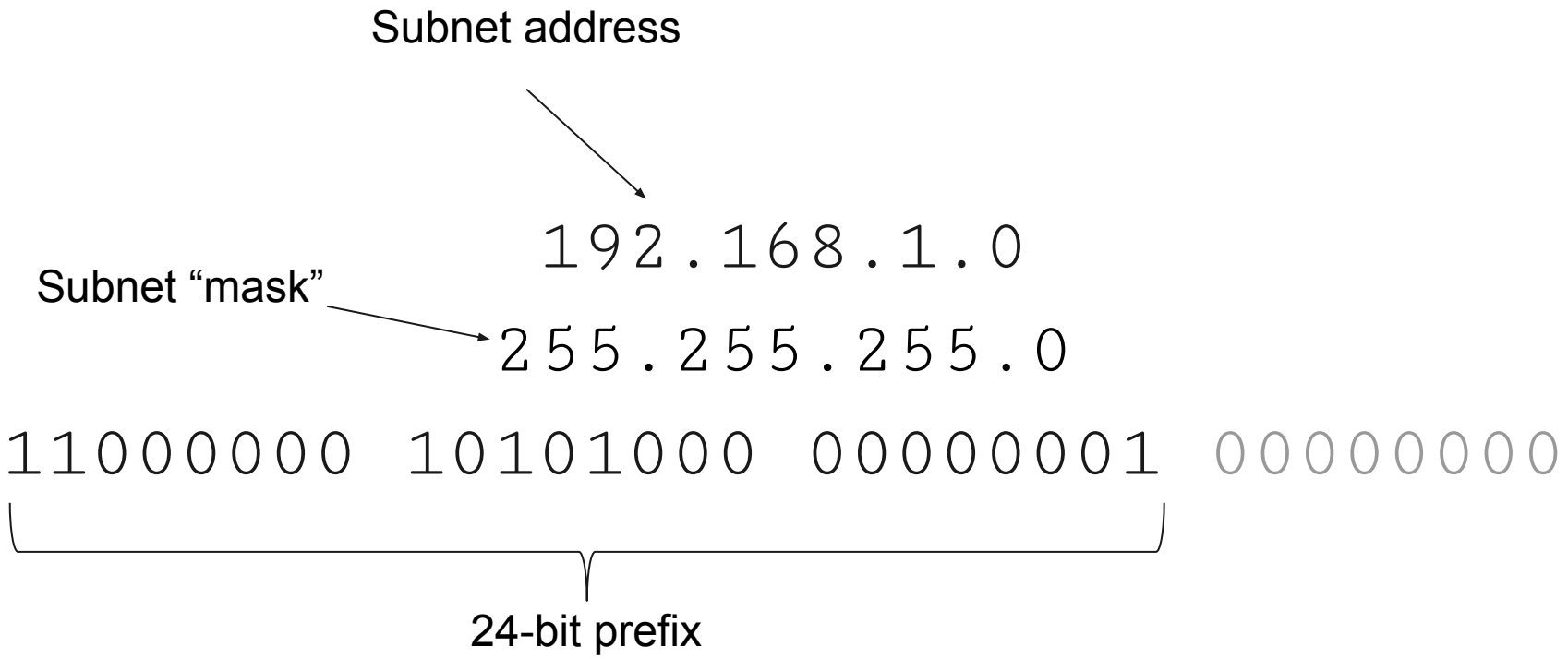
Basics of IP Routing

- Solution: hierarchical division into “subnets”
- Idea: Similar IP addresses are near each other
- Addresses with a common prefix are in the same subnet

Basics of IP Routing



Basics of IP Routing



Basics of IP Routing

Algorithm:

```
address & subnet_mask == prefix
```

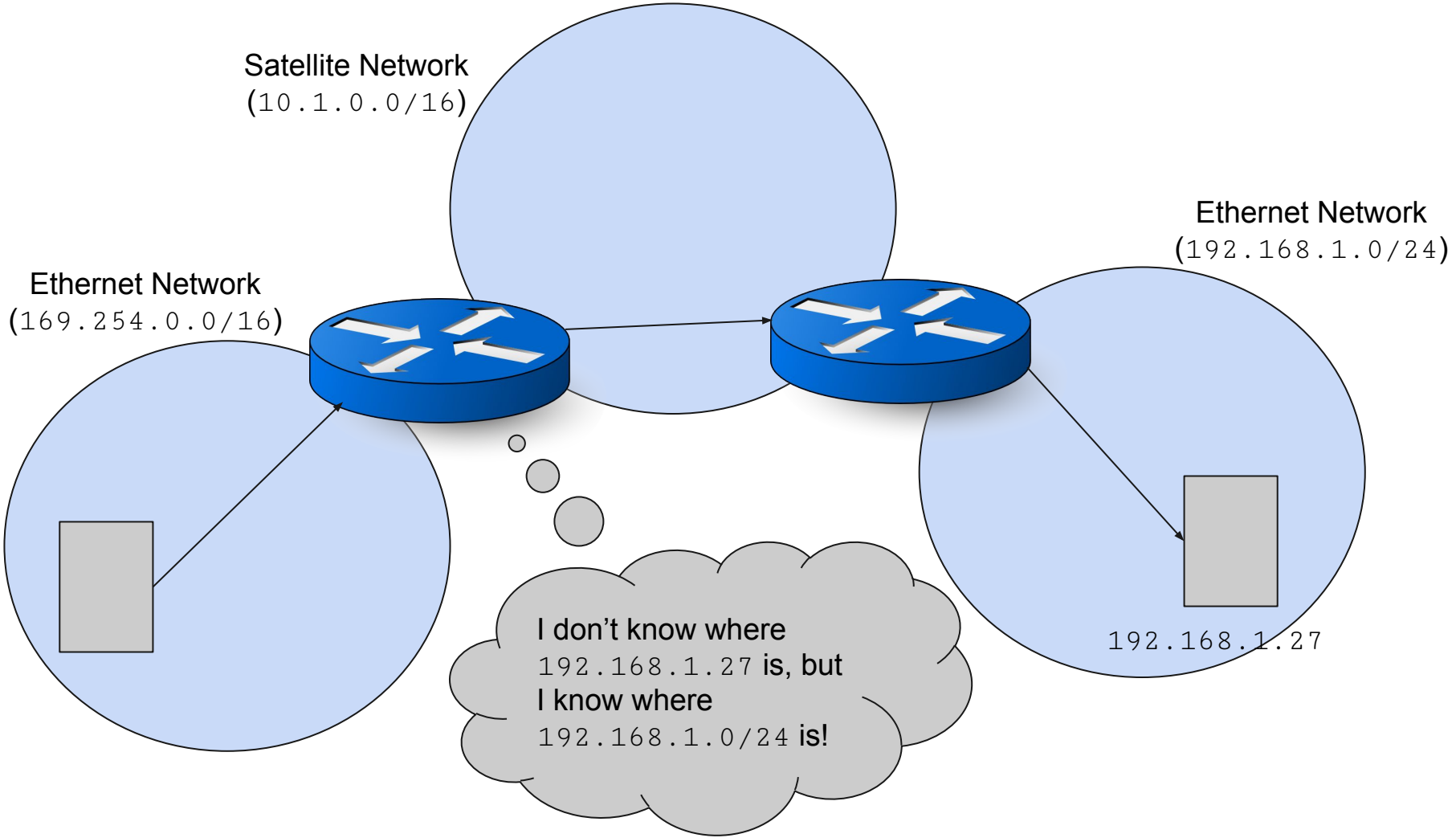
Example:

```
  192.168.1.27
& 255.255.255.0
---------------
  192.168.1.0
```

Basics of IP Routing

Routing algorithm: “longest prefix match”

```
// route to exact IP address
route = in_route_db(prefix, 0);
// subnet with 31-bit prefix
route = in_route_db(prefix, 1);
...
```


Satellite Network
(10.1.0.0/16)
Ethernet Network
(169.254.0.0/16)
Ethernet Network
(192.168.1.0/24)
I don't know where
192.168.1.27 is, but
I know where
192.168.1.0/24 is!
192.168.1.27

Basics of IP Routing

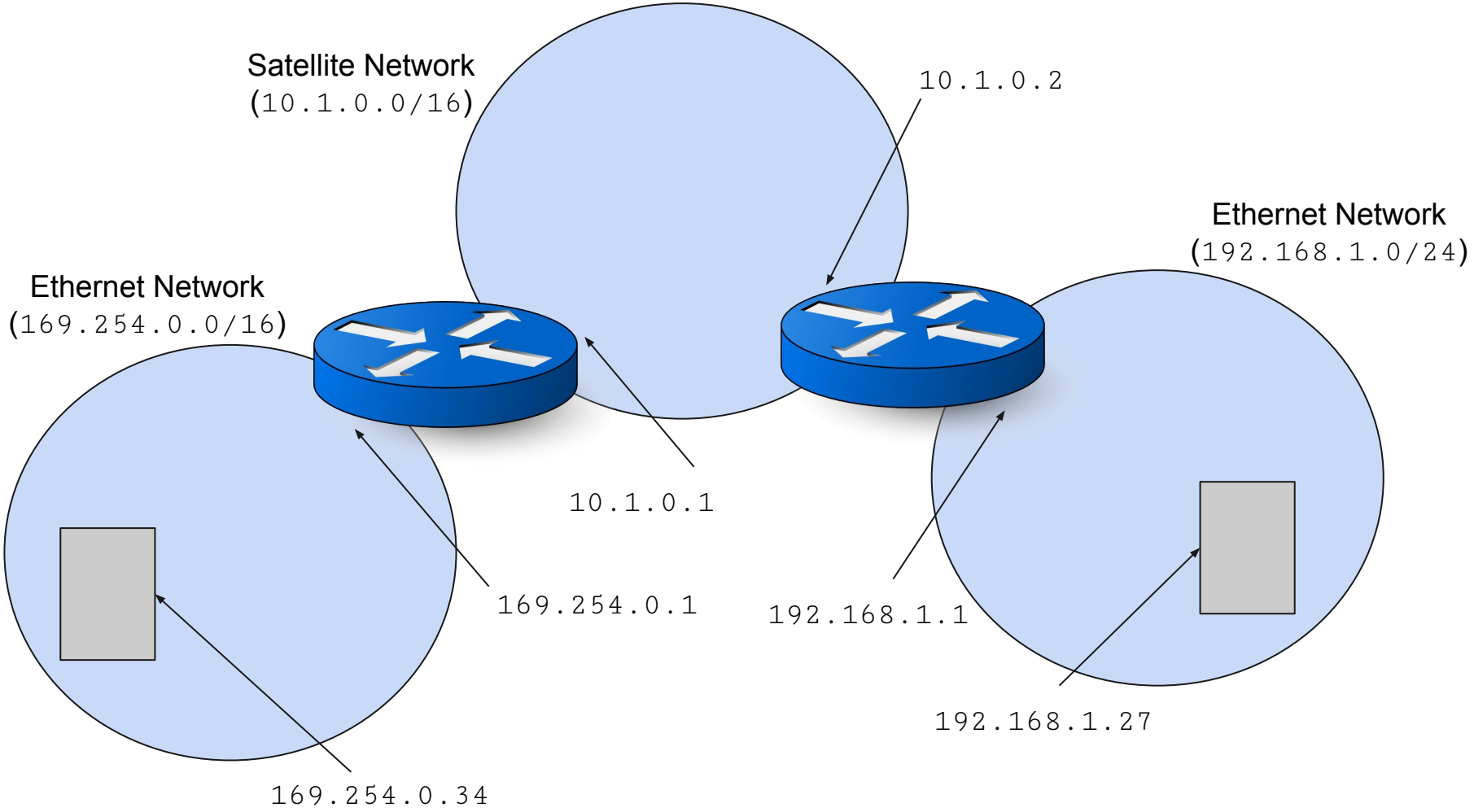
- Problem: what subnet are the routers in?

Basics of IP Routing

- Problem: what subnet are the routers in?
- Answer: they aren't...

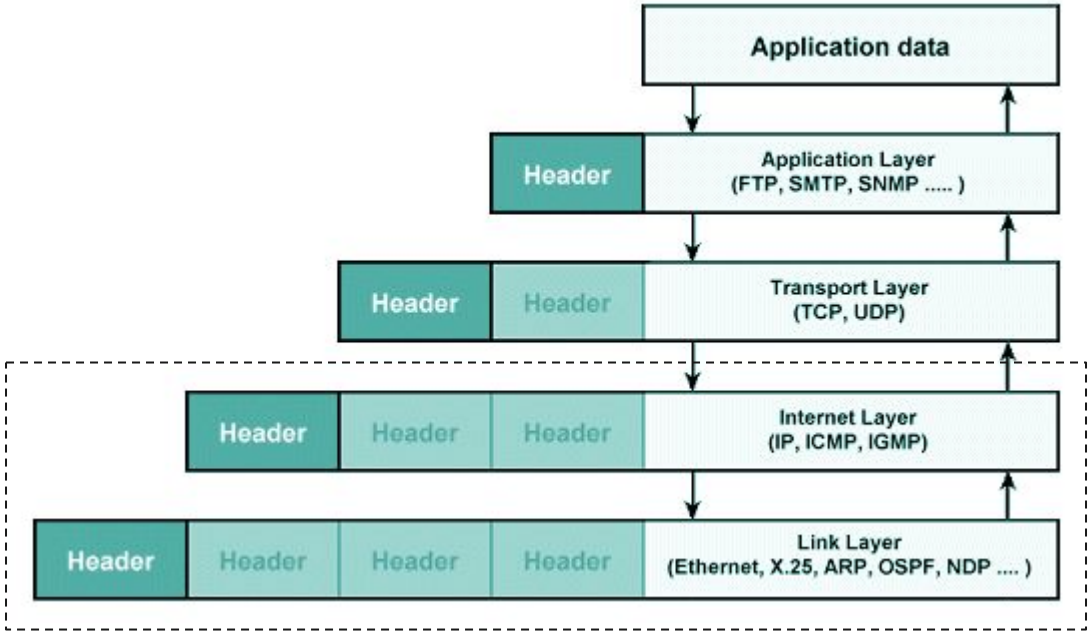
Basics of IP Routing

- *Devices* don't have IP addresses
- *Interfaces* have IP addresses
- "Multi-homed" devices have interfaces in multiple networks


Satellite Network
(10.1.0.0/16)
10.1.0.2
Ethernet Network
(192.168.1.0/24)
Ethernet Network
(169.254.0.0/16)
10.1.0.1
169.254.0.1
192.168.1.1
192.168.1.27
169.254.0.34

Combining Ethernet and IP

- Recall IP hourglass
- IP is agnostic to all other protocols (above and below in the protocol stack)
- Link layer protocols' responsibility to interoperate with IP



Ethernet frame contains IP packet

Combining Ethernet and IP

- Scenario: host A wants to send to host B
- What should we do?

Combining Ethernet and IP

- Scenario: host A wants to send to host B
- What should we do?
  - First: are they in my LAN?
    - Send ethernet frame directly to their MAC
  - Second: if they aren't in my LAN...

Combining Ethernet and IP

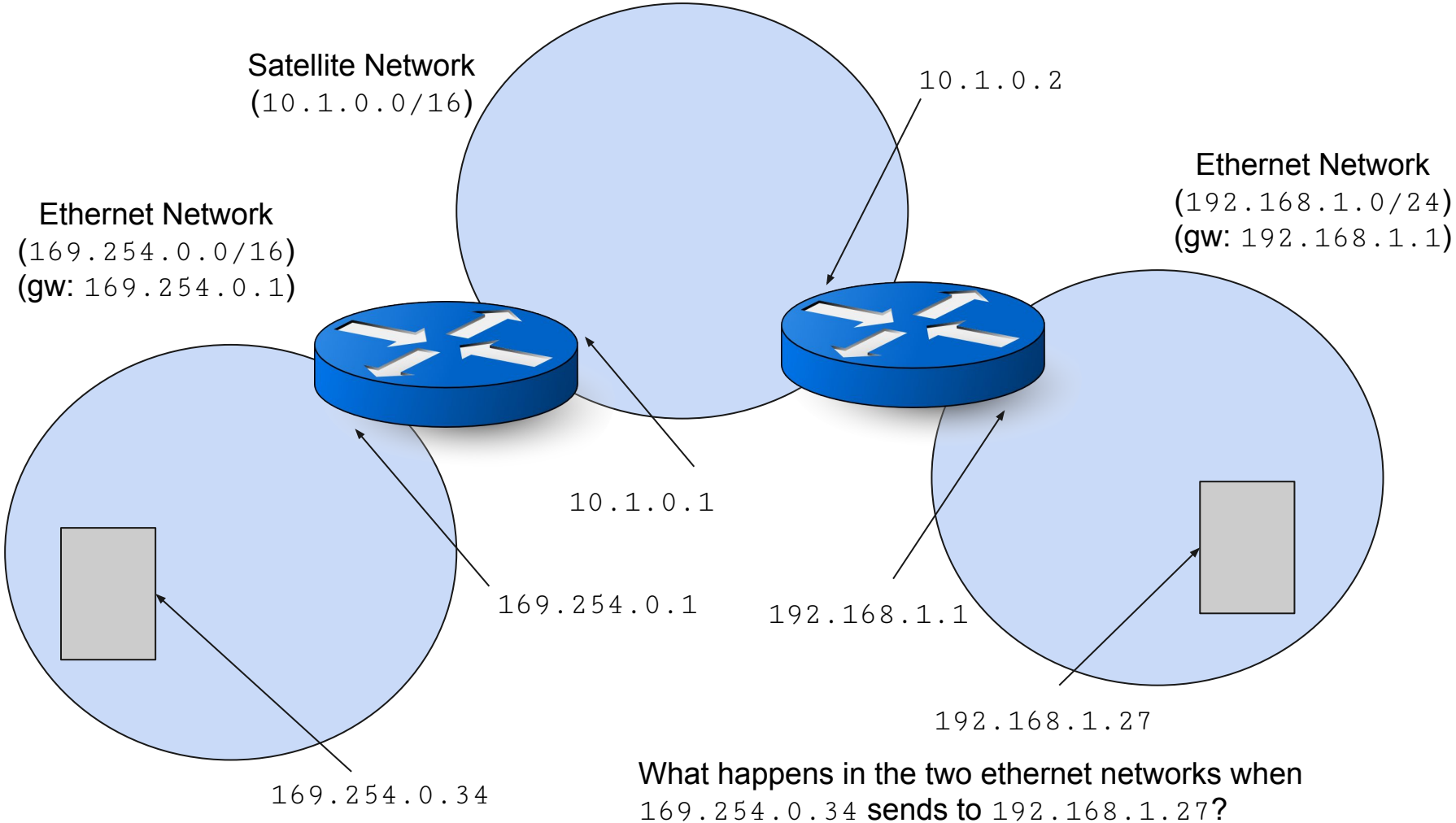
- Scenario: host A wants to send to host B
- What should we do?
  - First: are they in my LAN?
    - Send ethernet frame directly to their MAC
  - Second: if they aren't in my LAN
    - What router in my LAN can talk to their subnet?
    - Send ethernet frame to this router's MAC

Combining Ethernet and IP

- Two questions to answer:
  - Given an IP in my subnet, what's the MAC?
  - Given an IP in another subnet, what router to use?

Combining Ethernet and IP

- Given an IP in my subnet, what's the MAC?
  - Address Resolution Protocol (ARP)
- Given an IP in another subnet, what router to use?
  - Depends on the network
  - In most "edge" networks, only one router
  - Only two routes: "in here" or "out there" (the internet)
  - This single router is the "default gateway"
  - Often configured dynamically using DHCP


Satellite Network
(10.1.0.0/16)
10.1.0.2
Ethernet Network
(192.168.1.0/24)
(gw: 192.168.1.1)
Ethernet Network
(169.254.0.0/16)
(gw: 169.254.0.1)
10.1.0.1
169.254.0.1
192.168.1.1
192.168.1.27
169.254.0.34
What happens in the two ethernet networks when 169.254.0.34 sends to 192.168.1.27?