

SIGN THEN ENCRYPT


Joe Biden



Gabe Kaprielian



Congress



$\sigma \leftarrow \text{Sign}_{pk}(\text{"I quit."})$

$c \leftarrow \text{Enc}_{pk}(\text{"I quit."} || \sigma)$

\xrightarrow{c}

$(\text{"I quit."} || \sigma) \leftarrow \text{Dec}_{sk}(c)$

"ha.nice"

$c \leftarrow \text{Enc}_{pk}(\text{"I quit."} || \sigma)$

\xrightarrow{c}

$(\text{"I quit."} || \sigma) \leftarrow \text{Dec}_{sk}(c)$

Oh. This is signed by Joe. okay?

Problem: No receiver binding!

ENCRYPT THEN SIGN

Julie

$c \leftarrow \text{Enc}_{pk}(\text{crypto ans})$

$\sigma \leftarrow \text{Sign}_{sk}(c)$

Student

Gabe

$(c || \sigma)$ ~~X~~ \rightarrow

$(c || \sigma)$
 \downarrow

$\sigma \leftarrow \text{Sign}_{sk}(c)$

$(c || \sigma) \rightarrow$

Oh, this student
just sent me
the crypto answers.
Nice.

Problem: No sender binding!

OSI LAYERS

Application Layer

Presentation Layer

Session Layer

Transport Layer

← BGP

Network Layer

← IP layer

← ARP

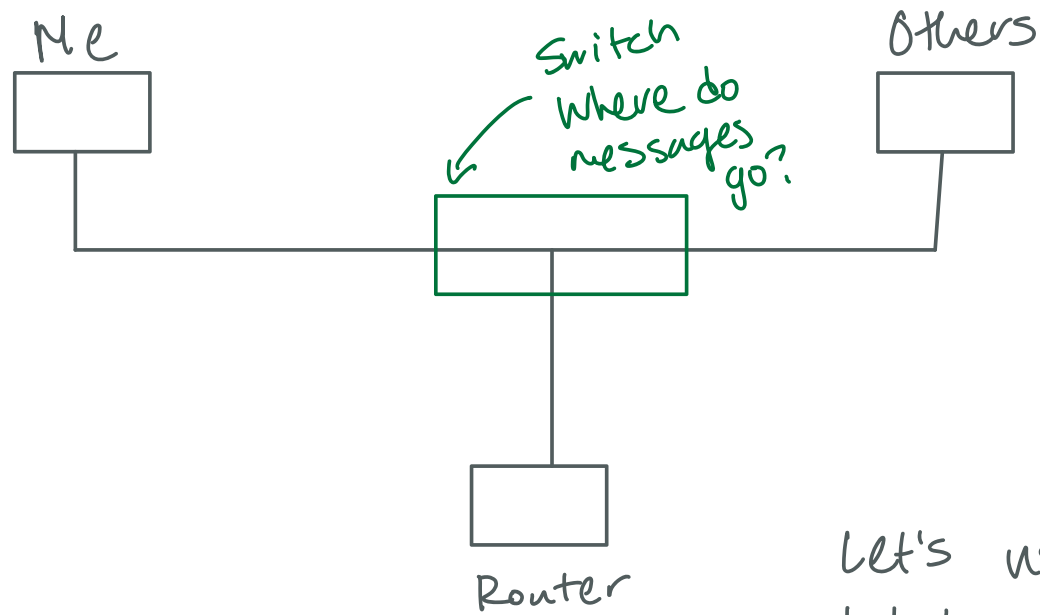
Data Link Layer

← MAC address

Physical Layer

← Ethernet

LINK LAYER



Let's use MAC addresses to label where messages should go.

MAC ADDRESSES

- 48 bits long
- Carried everywhere
- Unique identifier.

We need to learn the router's MAC address.
I know the Router's IP, but I need to find
the MAC Address.

How? (A)ddress (R)esolution (P)rotocol.

Goal: We want an Ad-Hoc, Fast, Decentralized way to
do this.

What do we do? Ask.

ARP

me
192.168.1.5 wants to know the MAC addr
for 192.168.1.1.
Router.

Broadcast: "who has 192.168.1.1?
Tell 192.168.1.5."] ARP
Query.

Response: "Tell 192.168.1.5 that
[MAC Addr] is holding
198.168.1.1."] ARP
Response

Nice. Now What?

IP Reminder

$$\underbrace{168.121}_{\text{fixed bits}} / \underbrace{16}_{\text{\# of fixed bits.}}$$

How are IP addresses Assigned?

IANA



RIR



ISP



AS

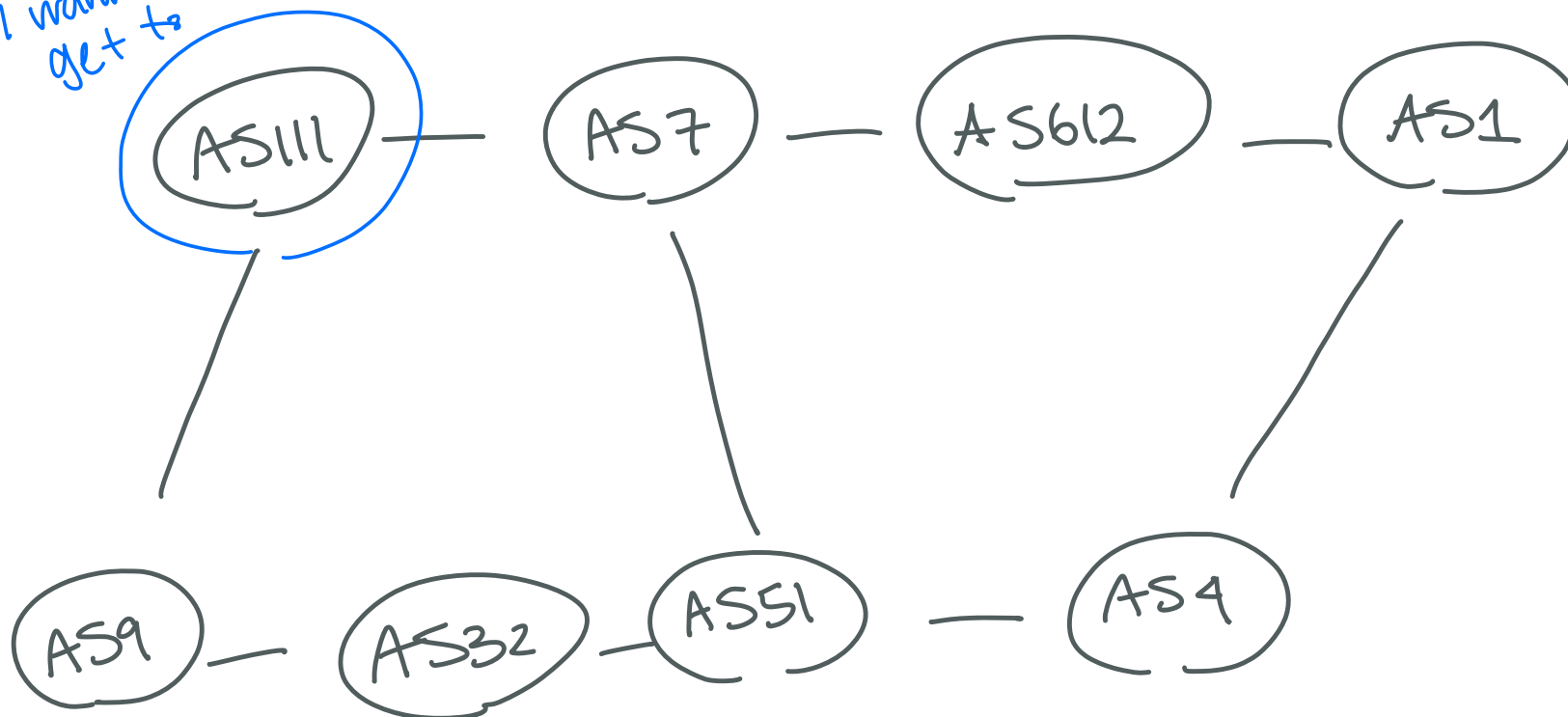


Hold IP addresses,
somehow need to get
to location.

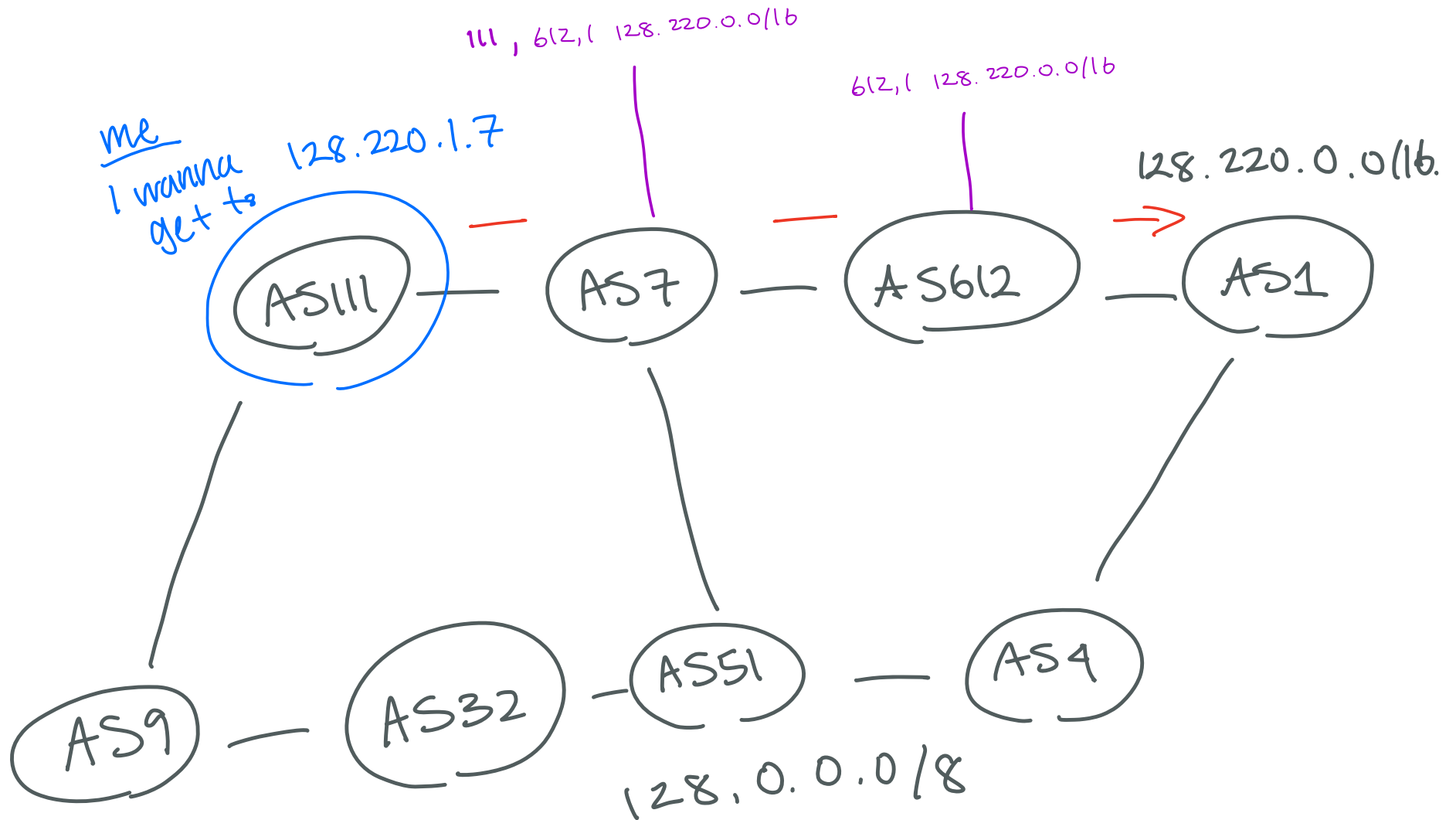


Customer

me
I wanna
get to 128.220.1.7



Announcements.



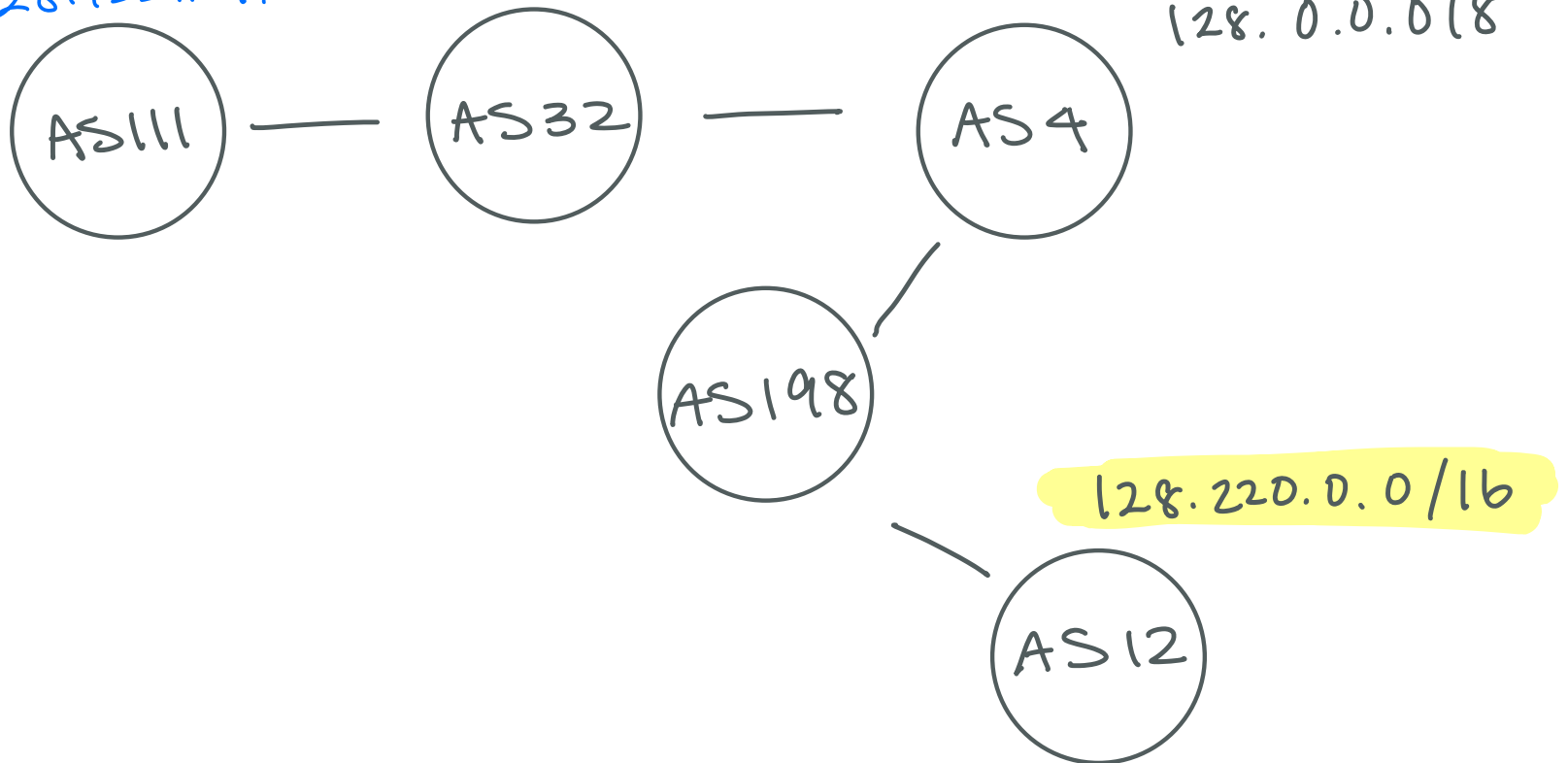
Basically gossip.

BGP RULES

1) Longest Prefix Match

2) Shortest AS Path

Want 128.122.1.7.

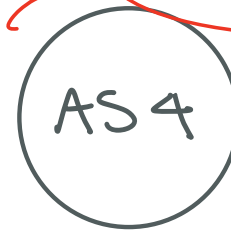
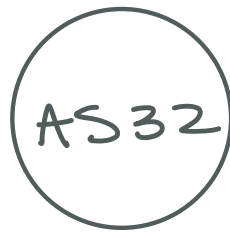


BGP RULES

1) Longest Prefix Match

2) Shortest AS Path

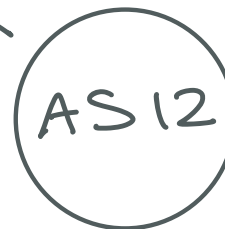
Want 128.122.1.7.



128.121.0.0/16



128.121.0.0/16



PROBLEMS W/ BGP

- Shorter Path Attack (One-hop Attack)

 - ↳ still scary, but limited scale.
not global

- Subprefix Attack

 - ↳ really scary
global impact

Defenses

- Prefix Filtering
- RPKI
- Route Origin Authorization.

EXAMPLE

