

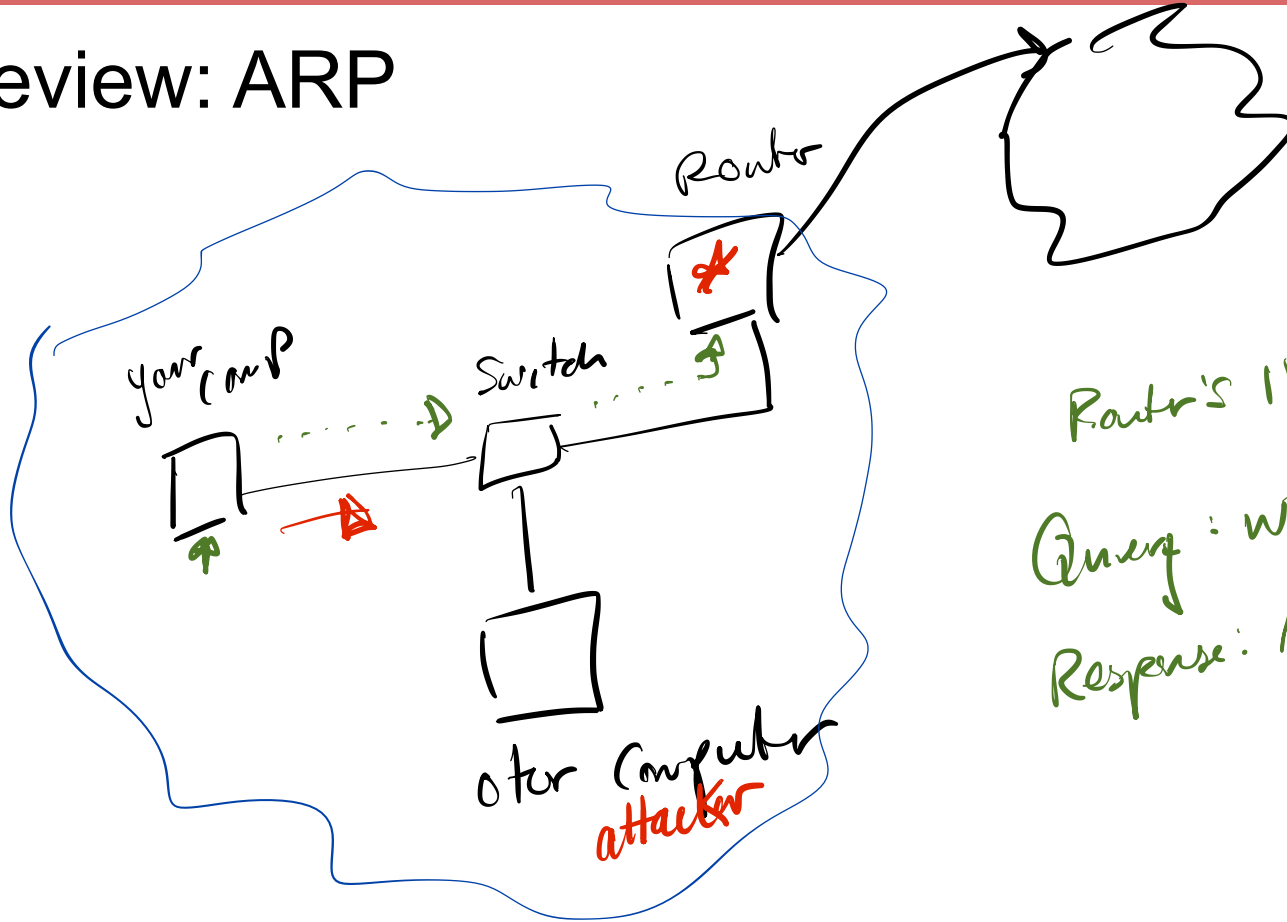
ARP Spoofing Mitigations

- Detection: Watching for potential mismatches ↑ throw an error to user
- Prevention: Centralization of some kind DHCP Server / router / Someone else
- Cryptography: S-ARP

CS558 Network Security

Lecture 4: BGP

Review: ARP



Router's IP \leftrightarrow Router's MAC
Query: who has Router's IP
Response: MAC has IP

Local networks + AS

routing \rightarrow Dijkstra
+ i

nodes is small

2^{32}

Whole Internet

routing \rightarrow decentralized

Full decentralization

\hookrightarrow all the routers gossiping

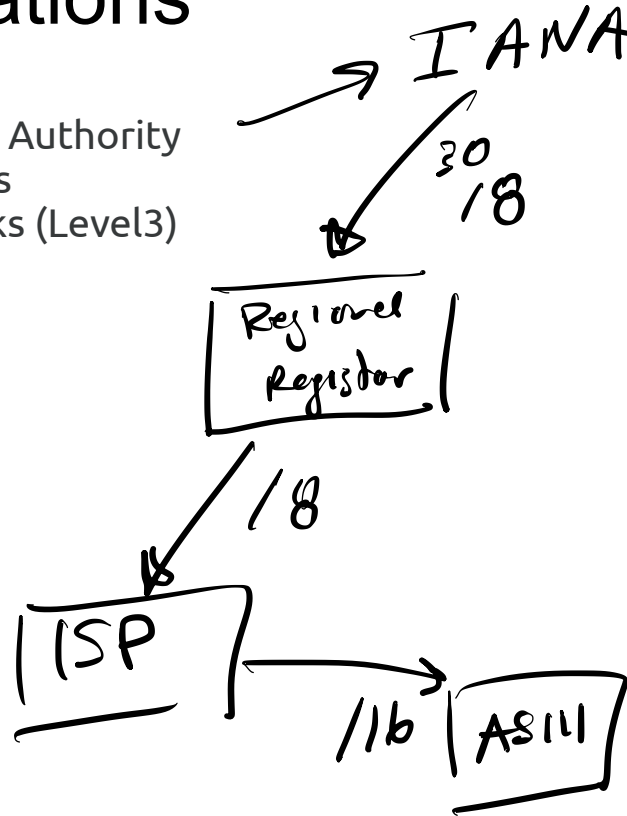
Partial decentralization:

Autonomous Systems \rightarrow local routing

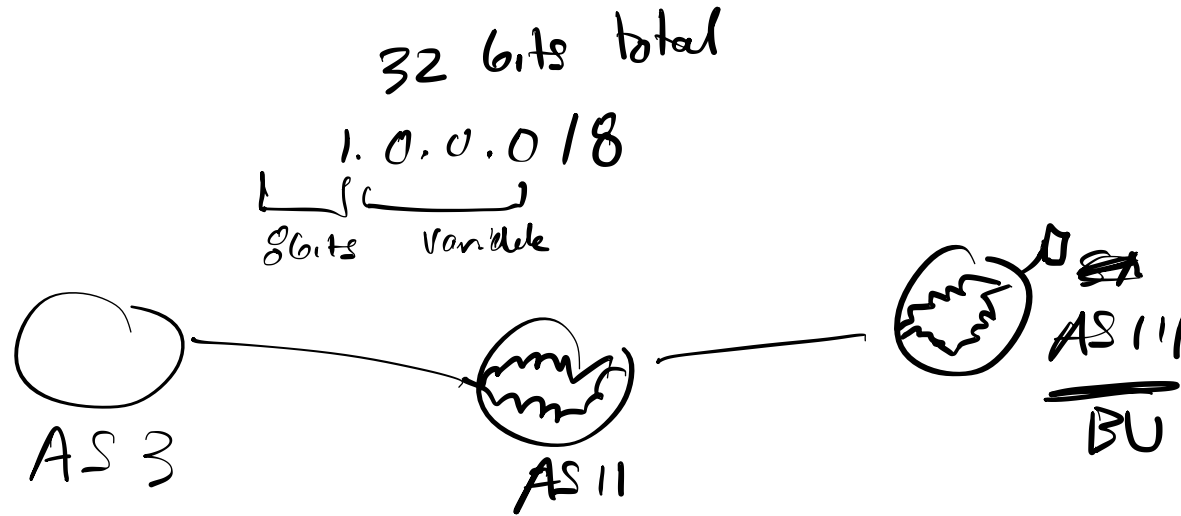
gossiping between AS

Internet Organizations

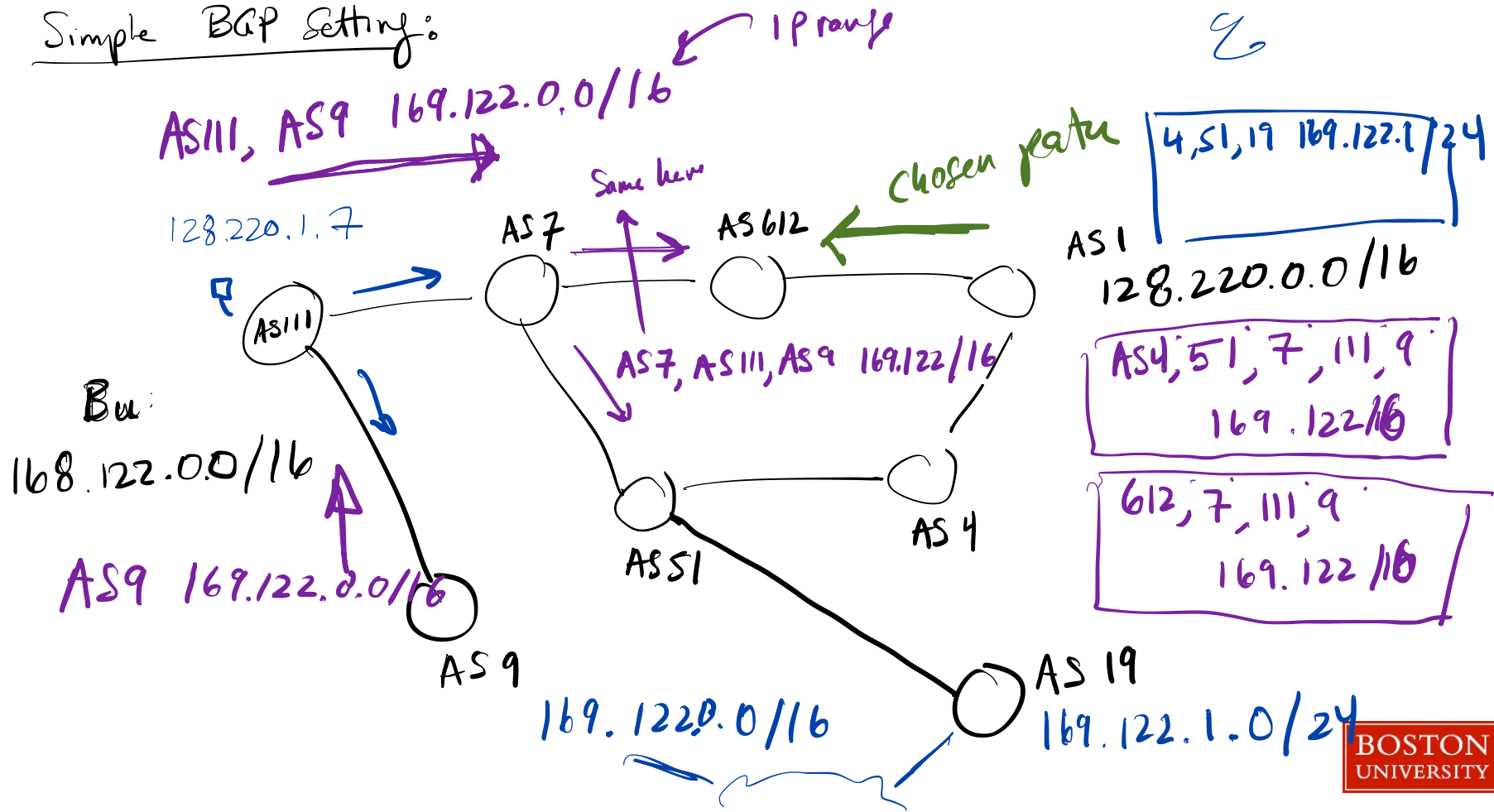
- Internet Assigned Numbers Authority
- Regional Internet Registrars
- ISPs and Backbone Networks (Level3)
- Autonomous Systems




Autonomous Systems Reminder



Simple BGP Setting:



AS number	111				
AS name	BOSTONU-AS				
organization	Boston University				
country	United States 				
AS rank	6782				
customer cone	2 asn	22 prefix	200704 address		
AS degree	6 global	2 transit	5 provider	0 peer	1 customer

AS Rank ▲	AS neighbors ▼	Organization		AS customer cone ▼	number of paths	relationship
1	3356	Level 3 Parent, LLC		46698	129	provider
4	174	Cogent Communications		30142	138	provider
10	3549	Level 3 Parent, LLC		13209	1	provider
86	<u>32787</u>	Akamai Technologies, Inc.		509	190	provider
539	10578	Harvard University		64	56	provider
24236	10961	Boston GigaPoP		1	10	customer


B(order) G(ateway) P(rotocol)

- Announcements form : AS PATH, PREFIX
- Forward announcements around (gossip)
- Partially Decentralized

Textbook BGP Decision Criteria

- Longest Prefix Match

- Shortest Path

- Weight
- Local Preference
- Originate
- AS path length 
- Origin code
- MED
- eBGP path over iBGP path
- Shortest IGP path to BGP next hop
- Oldest Path
- Router ID
- Neighbor IP address

BGP Hijack

— Someone is going to lie

↑

AS

↳ advertise a fake route

— Motivations: — So intended destination is unreachable

— Service loss

— Denial of Service

Real Incidents in Practice

- AS 7007 -- 1997. Disaggregated routes down to ^{1.1.0.0/22}~~1.1.0.0/24~~ and leaked
“And the owner of AS7007 was never able to live it down.”
- Pakistan Telecom -- 2008. Announces a /24 for Youtube
Real Announcement: “208.65.150.0/22”, Fake Announcement: “208.65.153.0/24”
- (AS34109) Cyberbunker vs Spamhaus -- 2013
Announcement: 0.ns.spamhaus.org 204.16.254.40/32
AS34109: 205.189.74.0/24 and 205.19.72.0/23 (March 2013)
AS6453 (TATA): 84.22.106.0/24 as /32's

1.1.1.1 /32