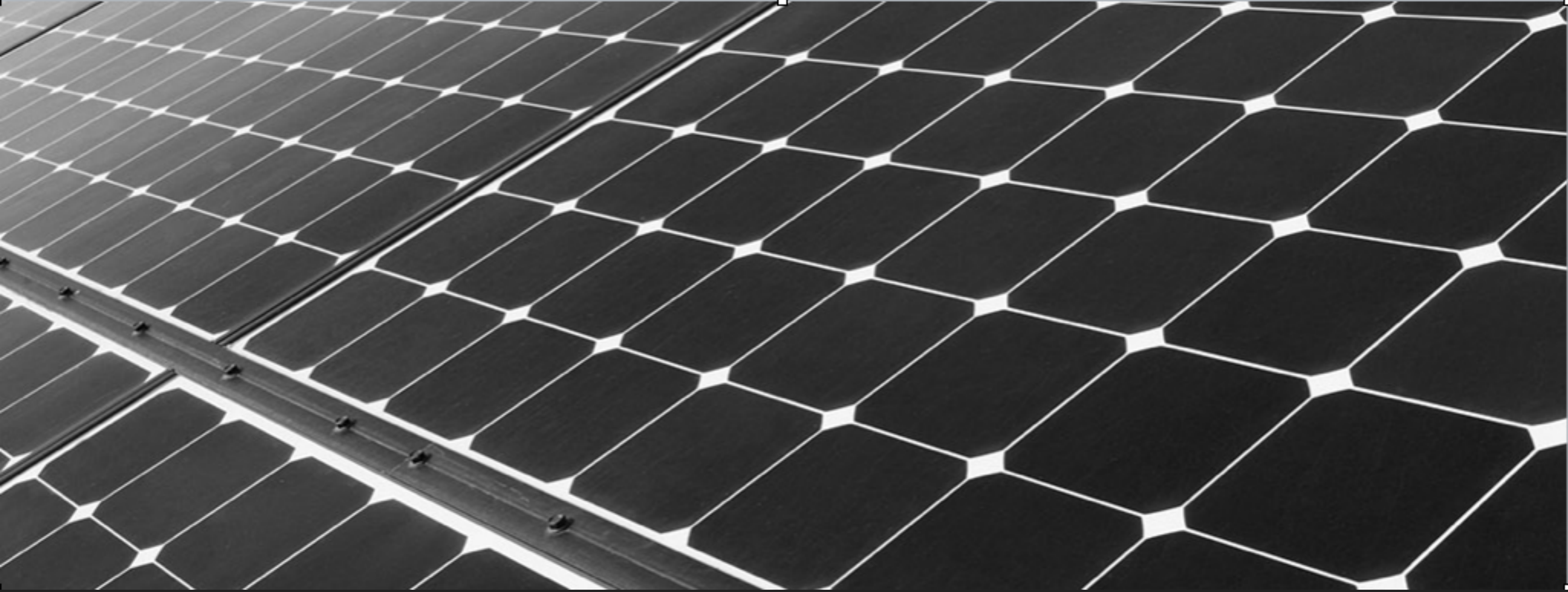


BORDER GATEWAY PROTOCOL ATTACKS

MIKE HAM

BORDER GATEWAY PROTOCOL

> BGP IS THE ROUTING PROTOCOL THAT LITERALLY MAKES THE INTERNET WORK

Ivan Pepelnjak

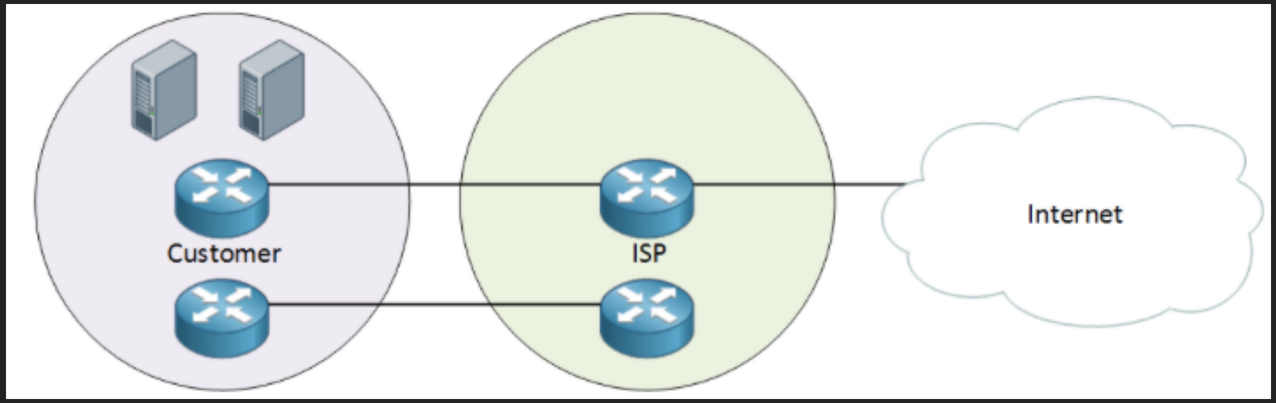
BGP BASICS

- External routing protocol of the internet (we all use it)
- Relevant if you connect to two or more ISPs in your setup
  - Redundant or multi-homed networks especially
- Layer 4 (Transport) protocol, sits on top of TCP IPv4/IPv6
- Peers have to manually form a connection to exchange routes, no automatic discovery

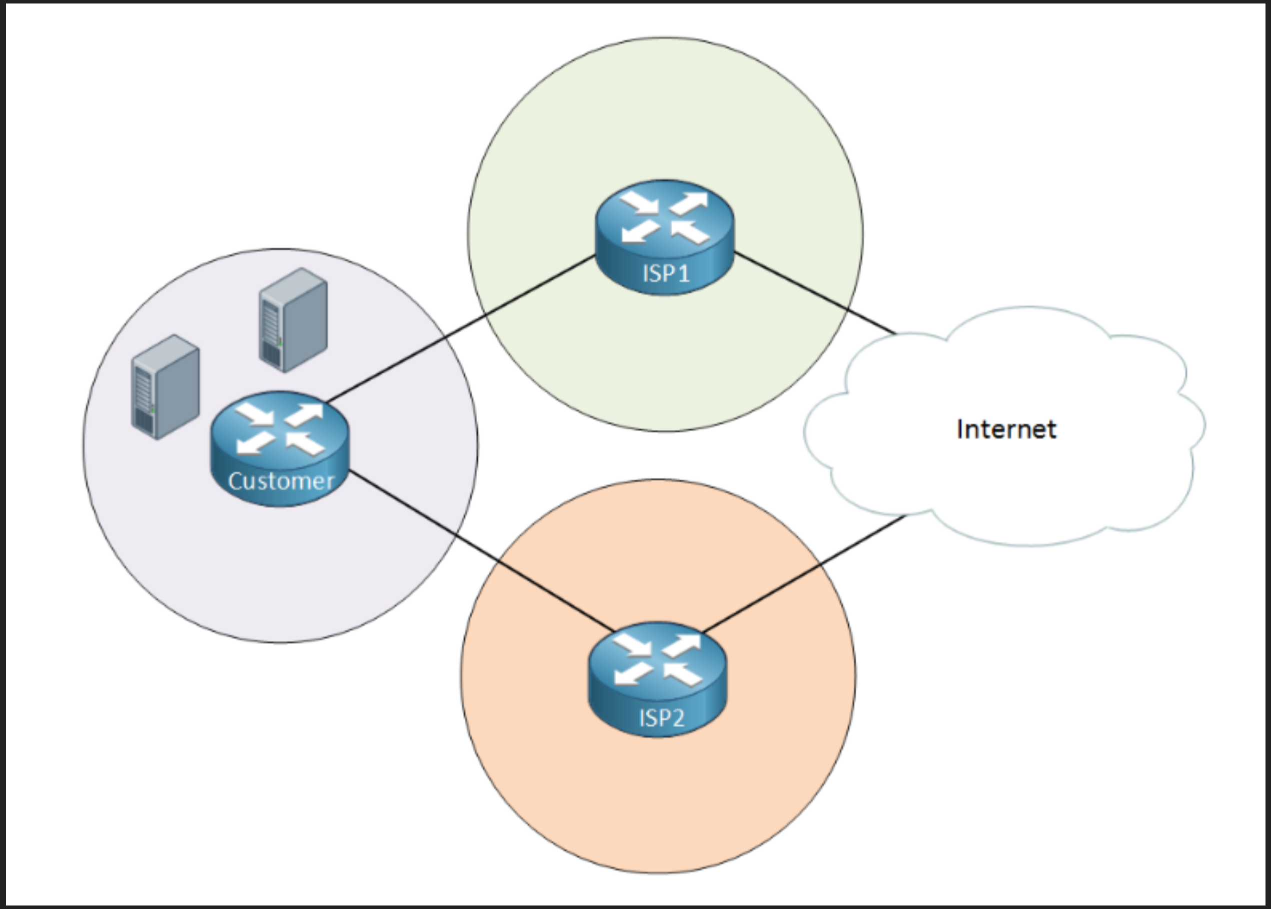
DO I SPECIFICALLY NEED IT?

- If you are just connecting to your ISP, regardless of how many links, you don't *technically* need BGP
  - Your ISP will use it though anyways, so your traffic touches BGP if it leaves to a second ISP
- Connected to two ISPs? You bet you need BGP running

Nope.



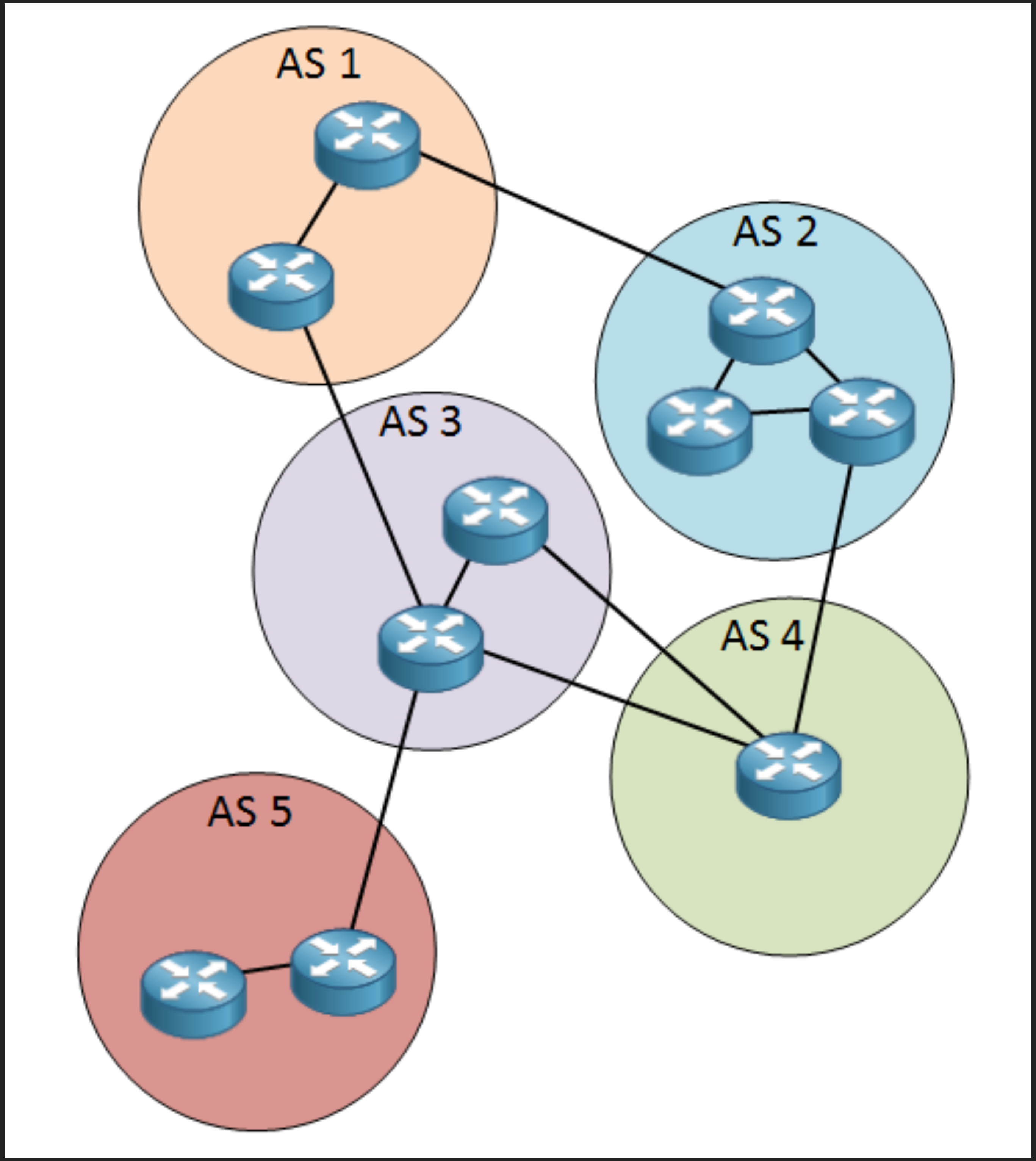
Yep.



BGP UNDER THE HOOD

- Autonomous System (AS) - routing domain, you get a number (ASN) from ARIN that maps to your networks
- Path Vector routing protocol, shortest path wins
  - (A–>B–>C) vs. (F–>E–>D–>C)
- Once you enable BGP, make neighbor adjacency, the routing tables are exchanged, you find the shortest path
- Entire neighbor table received on boot, after that, just the updates come across (no table broadcasts)

ISP LEVEL OF THINGS



WWW.WHATISMYASN.COM

- Your AS Path to this site was: 6939 13576 14263 23122
- Your origin AS is: AS23122 DSU - Dakota State University

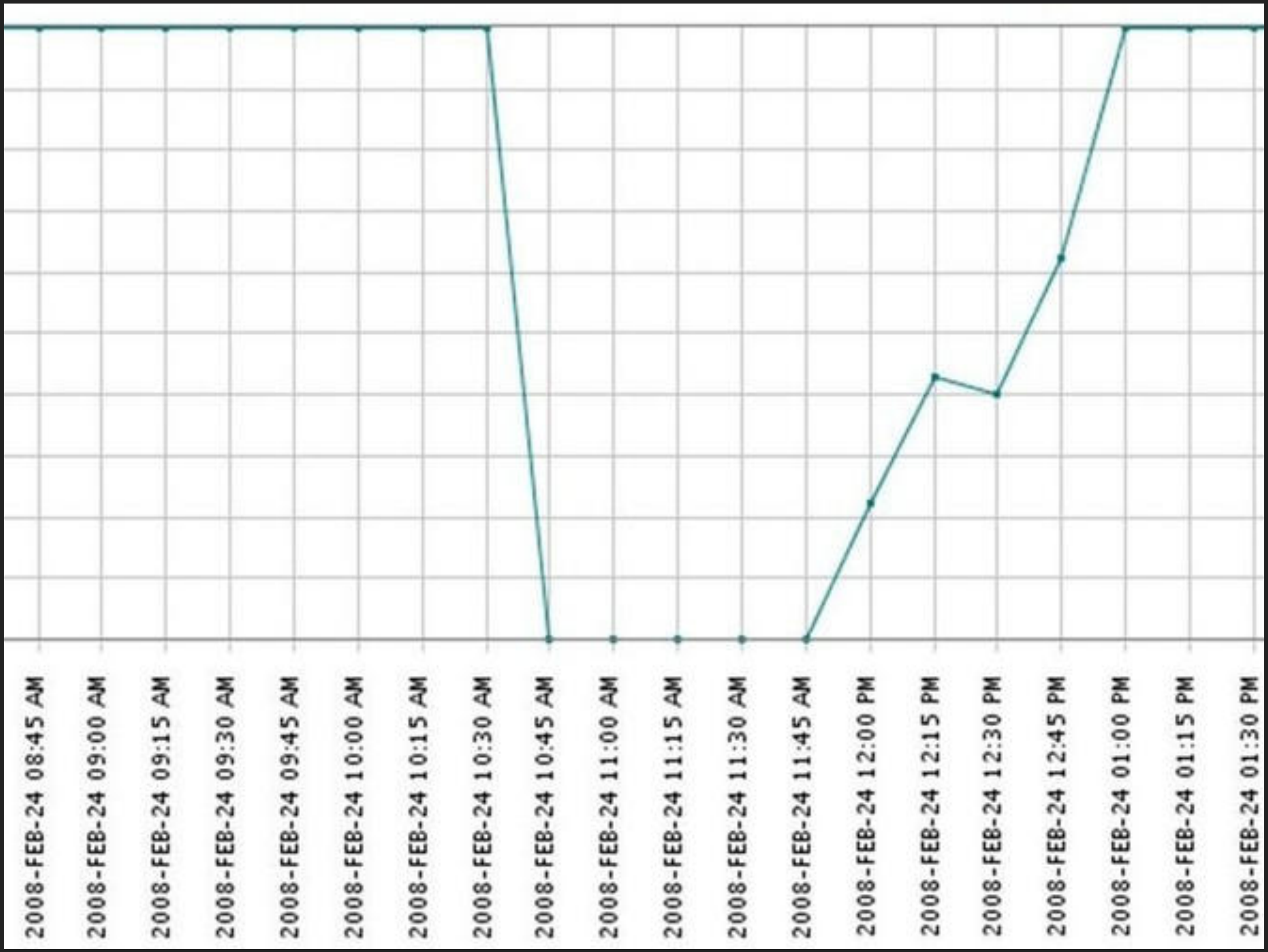
OK, I GET IT, WE USE BGP…CARRY ON

- BGP is so widely used, but yet it’s not the most secure of routing protocols
- If you control an AS, BGP is “readily exploitable”
- You may not care about the technical details of secure routing, but I bet you care about YouTube
  - How else do you find the 10 hour Epic Sax Guy video?
- February 24, 2008 YouTube disappeared for most of the internet because of a single Pakistani ISP, PTCL

PAKISTAN (PCTL) AND YOUTUBE

- Pakistan Telecommunications Authority wanted a YouTube video blocked due to fears of it triggering riots
- At the time, PCTL connected only to PCCW, a Hong Kong telco
- To block the video, PCTL pushed out a bad route update for YouTube, but forgot to tell PCCW to ignore the route
- As a result, PCCW forwarded on the bad route, and YouTube disappeared for a bit

AN HOUR WITHOUT YOUTUBE (KEYNOTE SYSTEMS IMAGE)



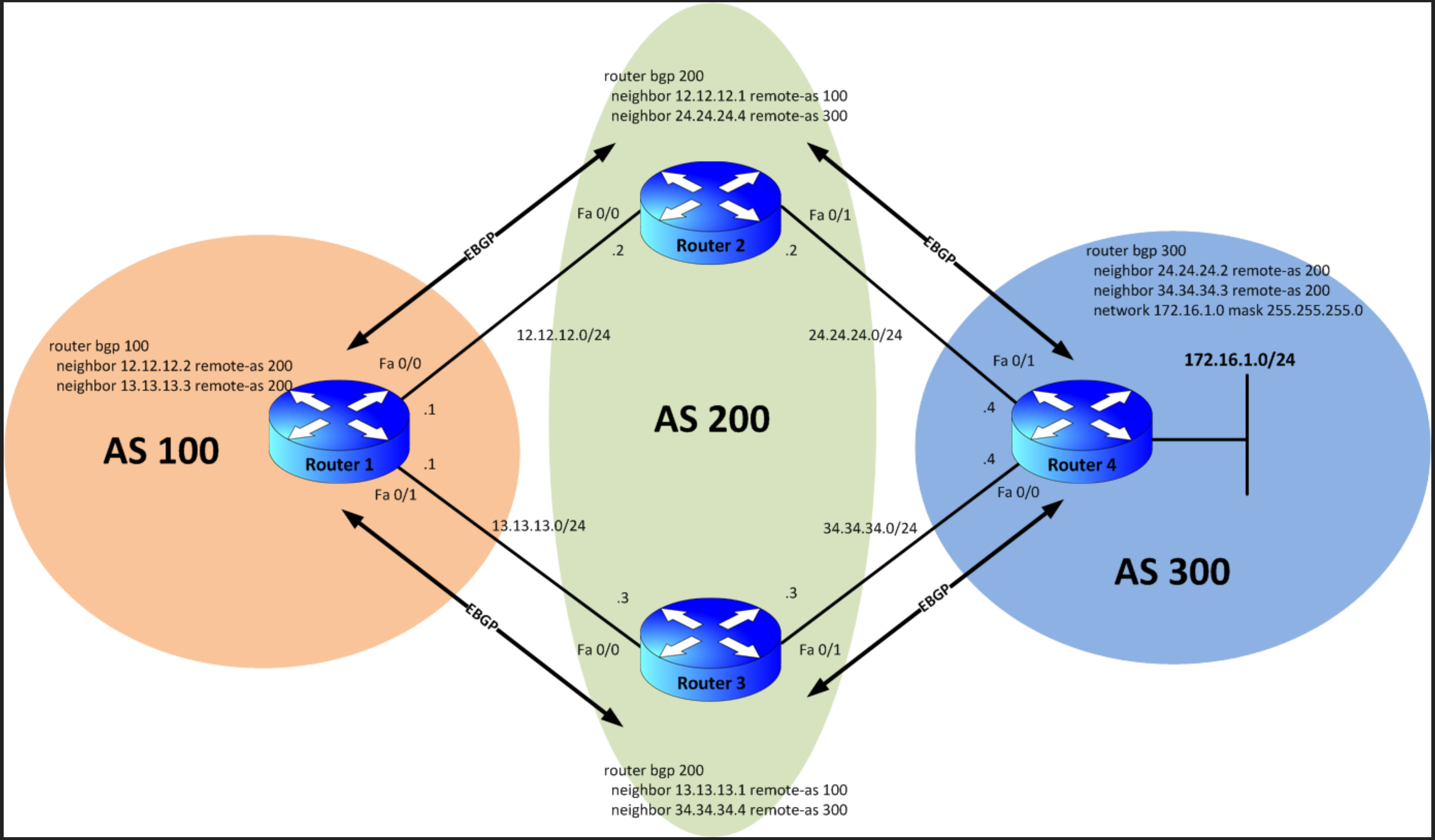
BGP HIJACKING FOR FUN AND PROFIT

- Feb-May 2014 Amazon, OVH, Digital Ocean, LeaseWeb had traffic hijacked
- Traffic was targeted for Bitcoin mining pools
    - Issued a reconnect command, miners pointed to attacker
- Dell SecureWorks led an investigation of sorts, didn’t release where the origination of the hijacks was
- AS path spoofed by Canadian attacker using path prepending
- Attacker was grabbing $9,000/day or about $83,000 total

BGP PATH PREPENDING

- Remember, BGP prefers a short AS_PATH
- Manual manipulation of route, extended with multiple copies of the AS number as the sender
- Legitimately used to ensure proper route selection
- Distribute return traffic load for multihomed customers

CISCO NETWORK DIAGRAM



```
router bgp 200
  neighbor 12.12.12.1 remote-as 100
  neighbor 24.24.24.4 remote-as 300
```

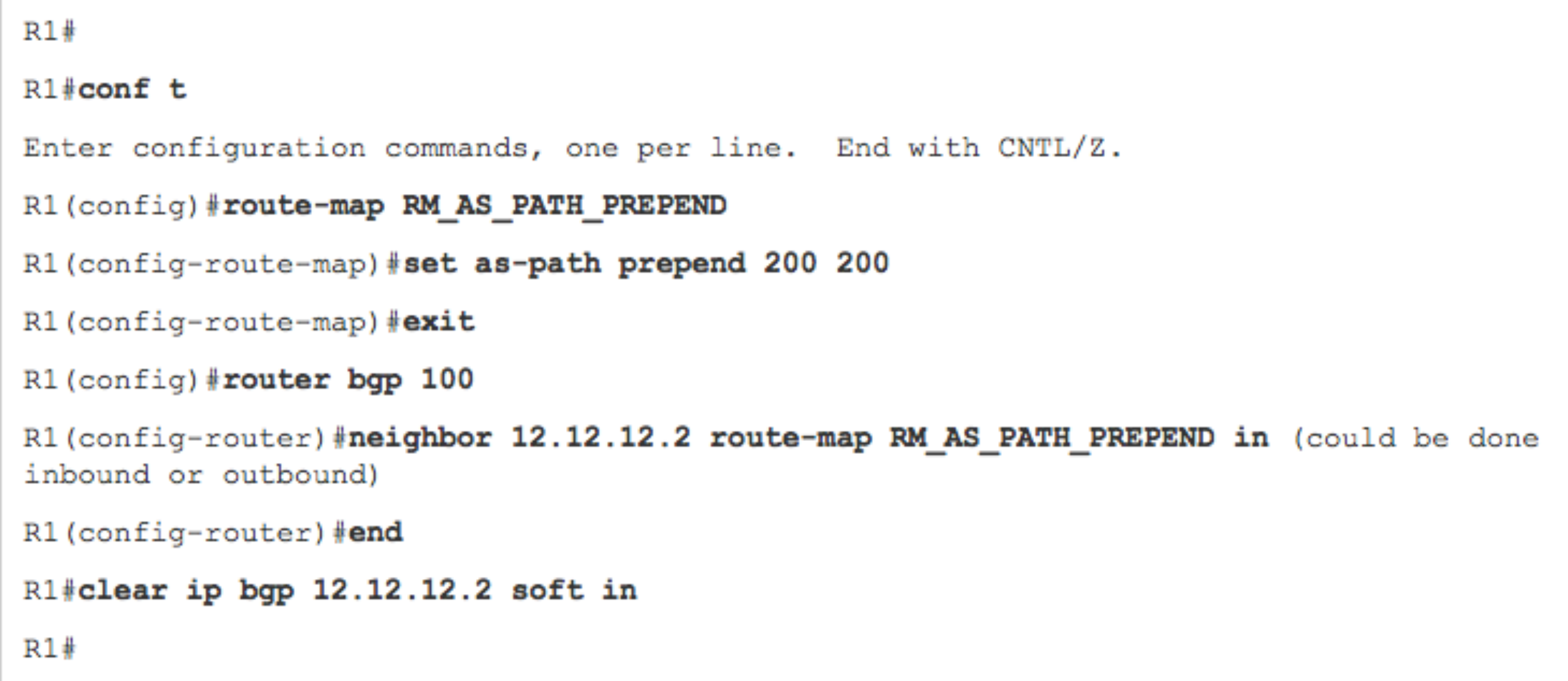
```
router bgp 300
  neighbor 24.24.24.2 remote-as 200
  neighbor 34.34.34.3 remote-as 200
  network 172.16.1.0 mask 255.255.255.0
```

```
router bgp 100
  neighbor 12.12.12.2 remote-as 200
  neighbor 13.13.13.3 remote-as 200
```

```
router bgp 200
  neighbor 13.13.13.1 remote-as 100
  neighbor 34.34.34.4 remote-as 300
```

CISCO PREPENDING

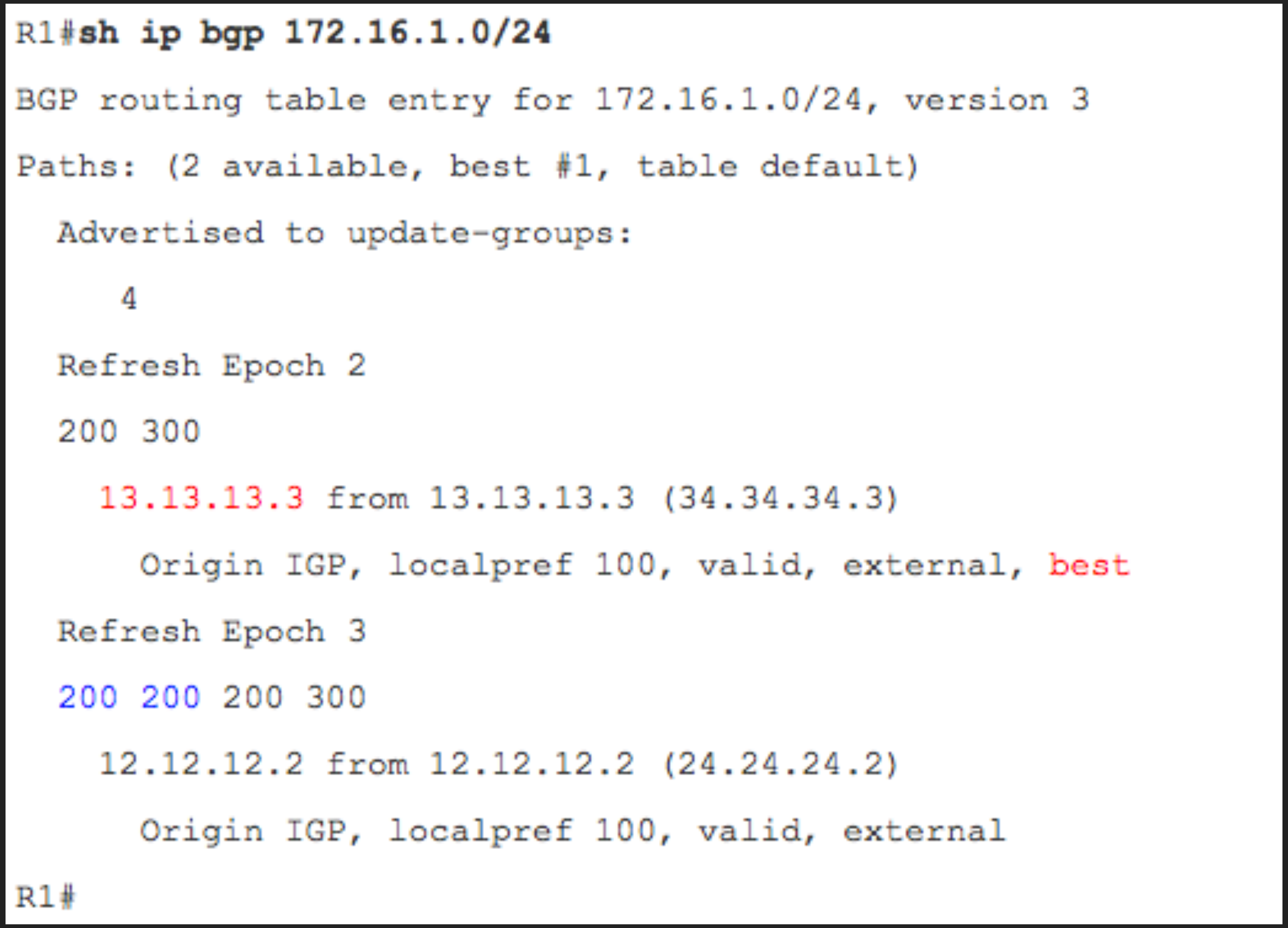
- Adding on a couple of 200 ASNs to the path makes it longer



```
R1#

R1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)#route-map RM_AS_PATH_PREPEND

R1(config-route-map)#set as-path prepend 200 200

R1(config-route-map)#exit

R1(config)#router bgp 100

R1(config-router)#neighbor 12.12.12.2 route-map RM_AS_PATH_PREPEND in (could be done
inbound or outbound)

R1(config-router)#end

R1#clear ip bgp 12.12.12.2 soft in

R1#
```

RESULTING PATH

- It’s just a little bit longer, R3 is more preferred



```
R1#sh ip bgp 172.16.1.0/24
BGP routing table entry for 172.16.1.0/24, version 3
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
     4
  Refresh Epoch 2
  200 300
    13.13.13.3 from 13.13.13.3 (34.34.34.3)
      Origin IGP, localpref 100, valid, external, best
  Refresh Epoch 3
  200 200 200 300
    12.12.12.2 from 12.12.12.2 (24.24.24.2)
      Origin IGP, localpref 100, valid, external
R1#
```

OTHER BGP ATTACK OUTCOMES

- DoS - black-hole portions of the Internet with false routes or killing valid ones
- Sniffing - similar to MITM attack, just using BGP instead
- Redirect Endpoints to Malicious Networks - hijack traffic, send it to the attacker, frequently change the routes
    - Seen in phishing/spam quite a lot
- Route Instabilities
- Revelation of Network Topology

FIX IT. FIX IT. FIX IT. FIX IT. FIX IT. FIX IT.