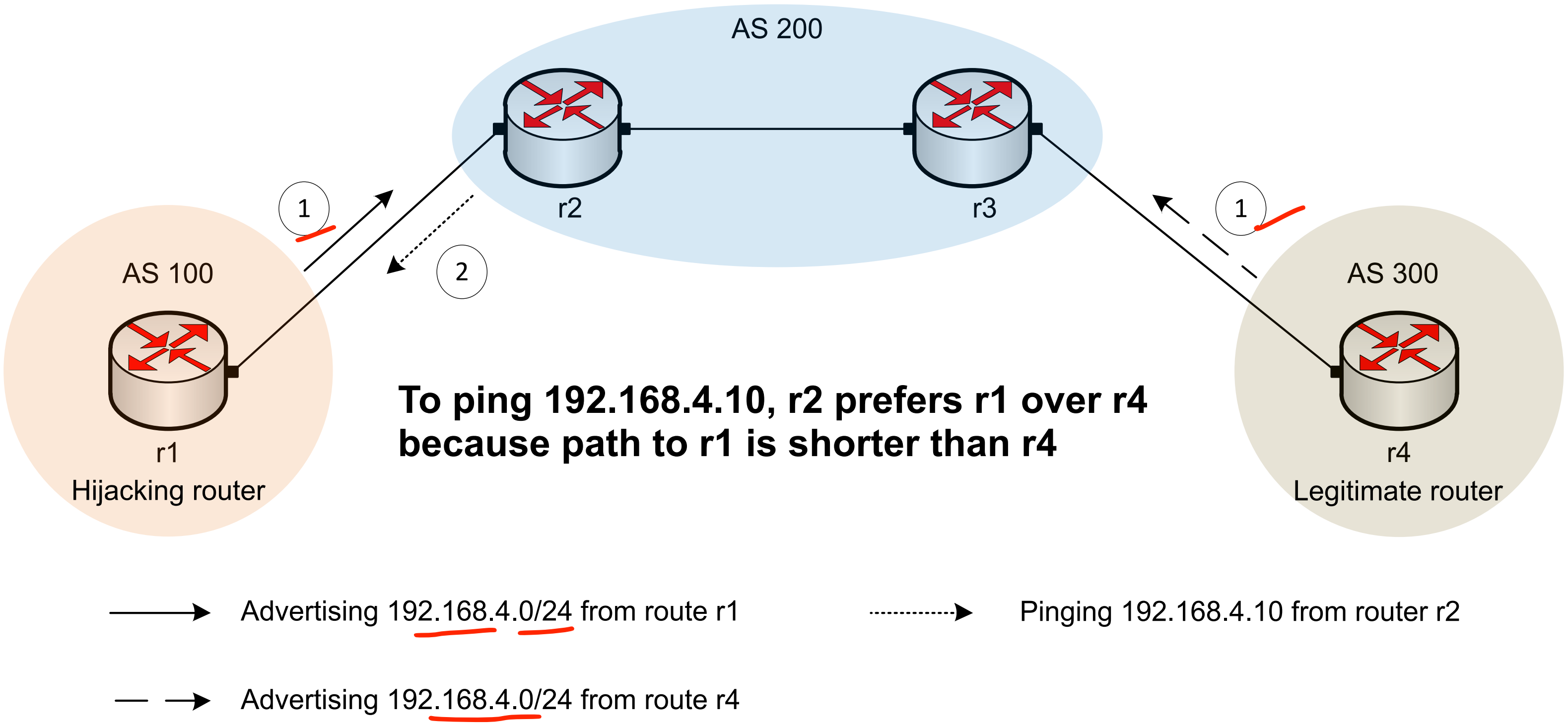
What is BGP Hijacking?

- BGP hijacking is when the attackers maliciously reroute Internet traffic
- It occurs when an unauthorized network originates IP prefix owned by other networks



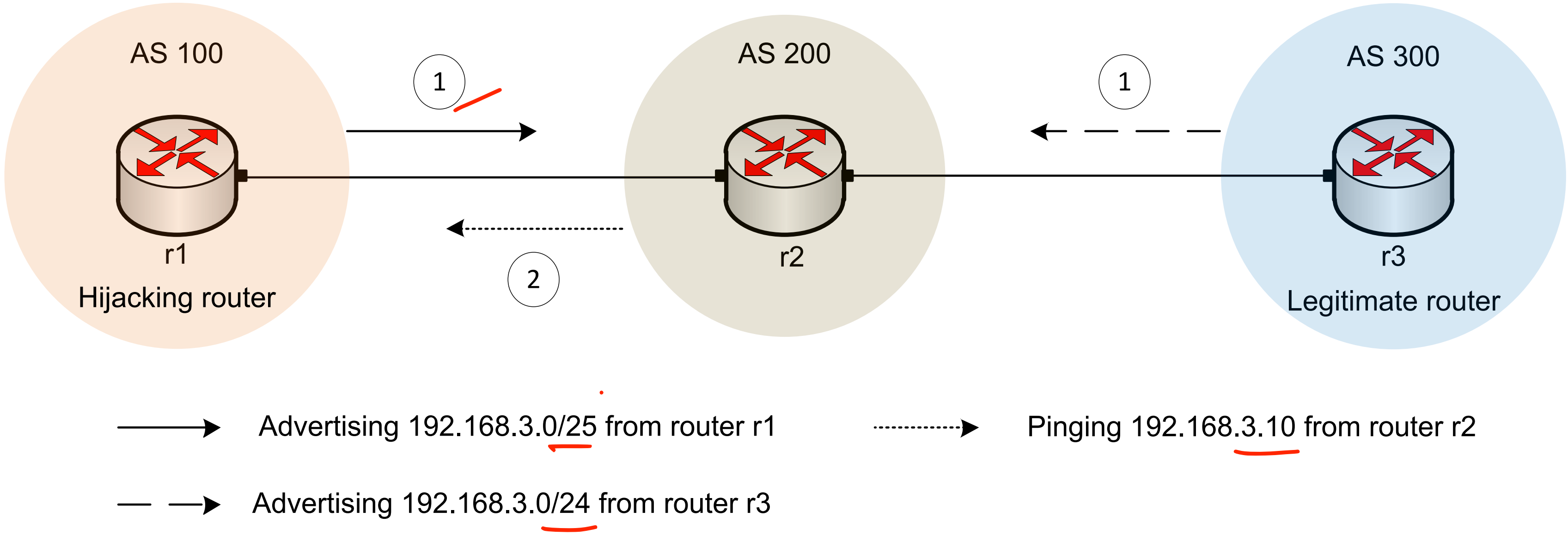
To ping 192.168.4.10, r2 prefers r1 over r4 because path to r1 is shorter than r4

Advertising 192.168.4.0/24 from route r1

Pinging 192.168.4.10 from router r2

Advertising 192.168.4.0/24 from route r4

BGP hijacking using specific IP prefix advertisement



Advertising 192.168.3.0/25 from router r1

Pinging 192.168.3.10 from router r2

Advertising 192.168.3.0/24 from router r3

To ping the network 192.168.3.10, r2 prefers r1 over r3, because r1 made specific announcement (/25)

- https://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/
- https://bgpstream.com/event/270621

BGP Hijacking Attacks

- Large scale BGP hijack out of India (2015)[1]
  - 16,123 hijacked prefixes
- BGP hijack affected Amazon DNS (2018)[2]
  - 5 Amazon routes (prefixes) were affected
- Chinese Telecom performed a two hour BGP hijacking attack on European networks (2019)[3]
  - A significant portion of the traffic was routed through the Chinese Telecom infrastructure before reaching its destination
- Russian telecommunication provider rerouted traffic intended for several networks across the globe (2020)[4]
  - Over 8000 prefixes were rerouted from Cloudfare, Facebook, Google, Amazon, etc.

[1] Toonk, Andree “Large scale BGP hijack out of India”. www.bgpmon.net/massive-route-leak-cause-internet-slowdown/

[2] Nichols Shaun, “AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet”,

[3] Linssen, R. H. H. G. M. "Vulnerability of DNS name servers against BGP hijacking." Bachelor's thesis, University of Twente, 2020

[4] Improta Alessandro, Sani Luca "April Fools’ BGP Hijack”. https://blog.catchpoint.com/2020/04/06/april-fools-bgp-hijack/

BGP Hijack 1: Thieves stole $150K in Ethereum

- eNet was commandeered by miscreants to persuade its peers – potentially Hurricane Electric, Level 3, and others

- This reroute the internet's traffic from some AWS Route 53 DNS servers to a malicious DNS server acted as AWS DNS (hacked by thieves)

- The DNS servers misdirected visitors to MyEtherWallet.com to a phishing website

- How to stop?
  - DNSSEC = resolvers would deny fake records
  - HSTS = browsers would prevent visiting self-signed certs

source: https://www.theregister.com/2018/04/24/myetherwallet_dns_hijack/

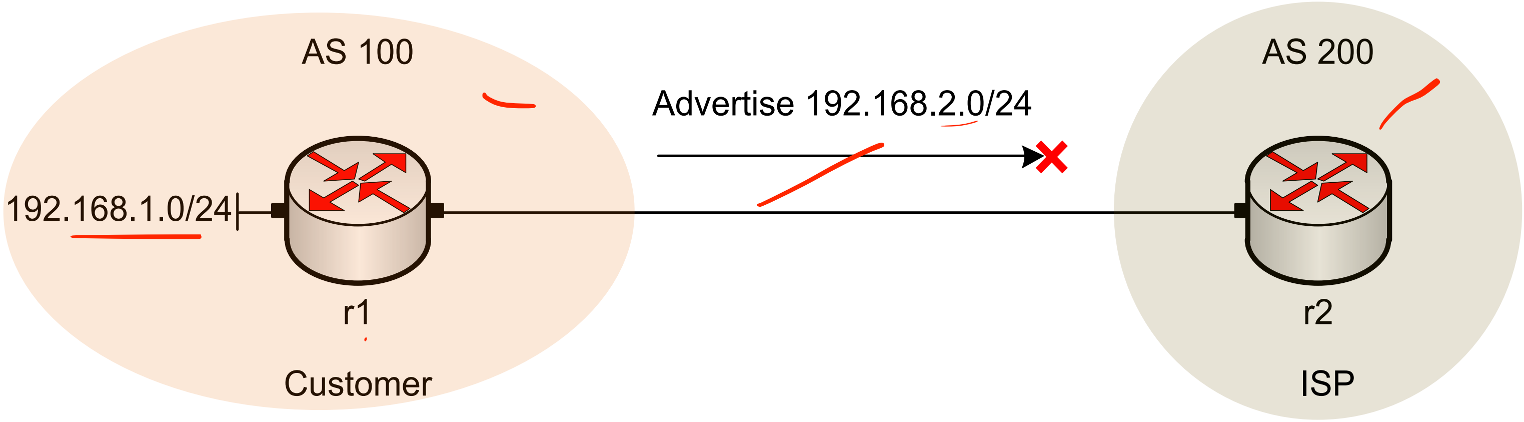
BGP Hijack 2: China telecom routes European traffic

- Swiss company Safe Host leaking over 70,000 routes to China Telecom in Germany.
- The Chinese telecommunication company then announced these routes on to the global Internet, which resulted in large amounts of web traffic destined for some of the largest European mobile networks to be redirected through China Telecom's network.
- In 2010, China Telecom hijacked 15% of the world's Internet prefixes, which resulted in popular websites being rerouted through China for around 18 minutes. The incident impacted US government (".gov") and military (".mil") sites as well..
- The carrier has been constantly misdirecting Internet traffic through its network in China for several years.
- How to stop ? -- RPKI to secure BGP

source: https://www.securityweek.com/china-telecom-routes-european-traffic-its-network-two-hours, https://essay.utwente.nl/80731/1/Linssen_BA_EEMCS.pdf

Using IP Prefix Filters to Mitigate BGP Hijacking

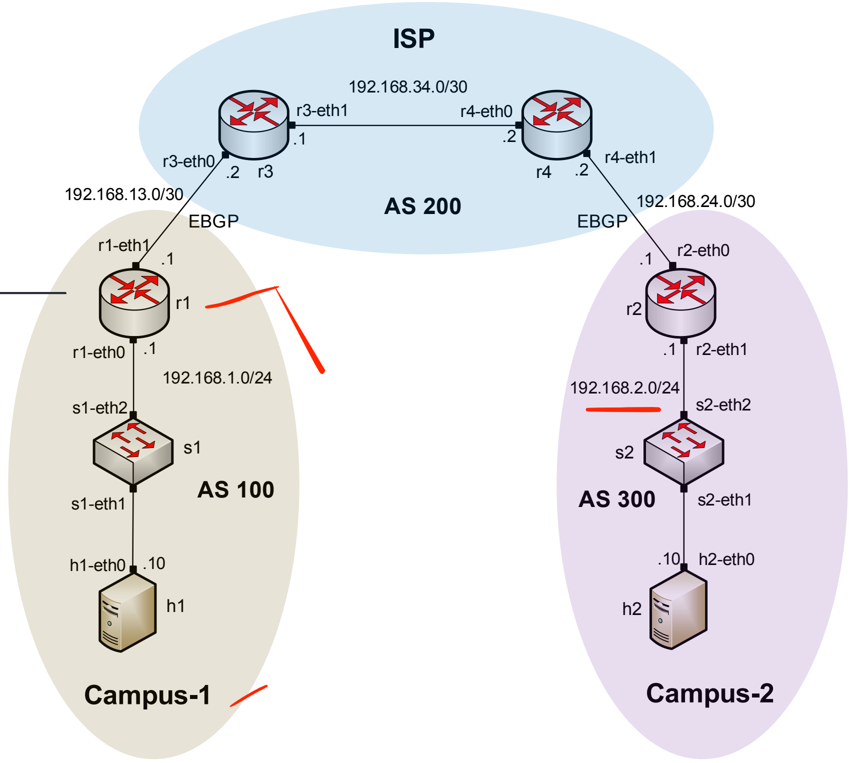
- A router can limit the number of BGP route advertisements by configuring IP prefix filters
- “Most important is to secure the inbound routing advertisements, particularly from customer networks, through the use of explicit prefix-level filters…”[1]



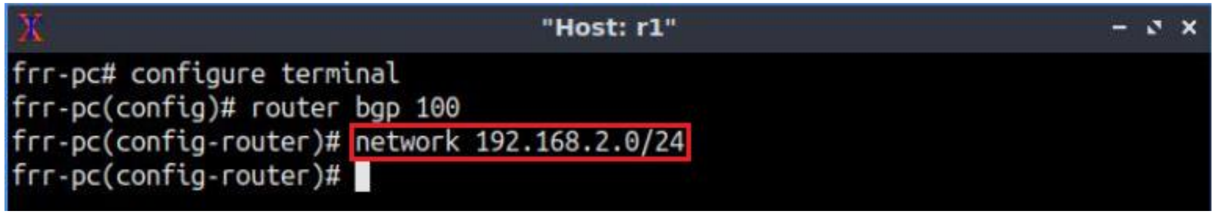
[1] “MANRS Implementation Guide”. https://www.manrs.org/isps/guide/filtering/

Lab 13 Configuration

- Router r1 hijacks (advertises) the network 192.168.2.0/24



Router r1

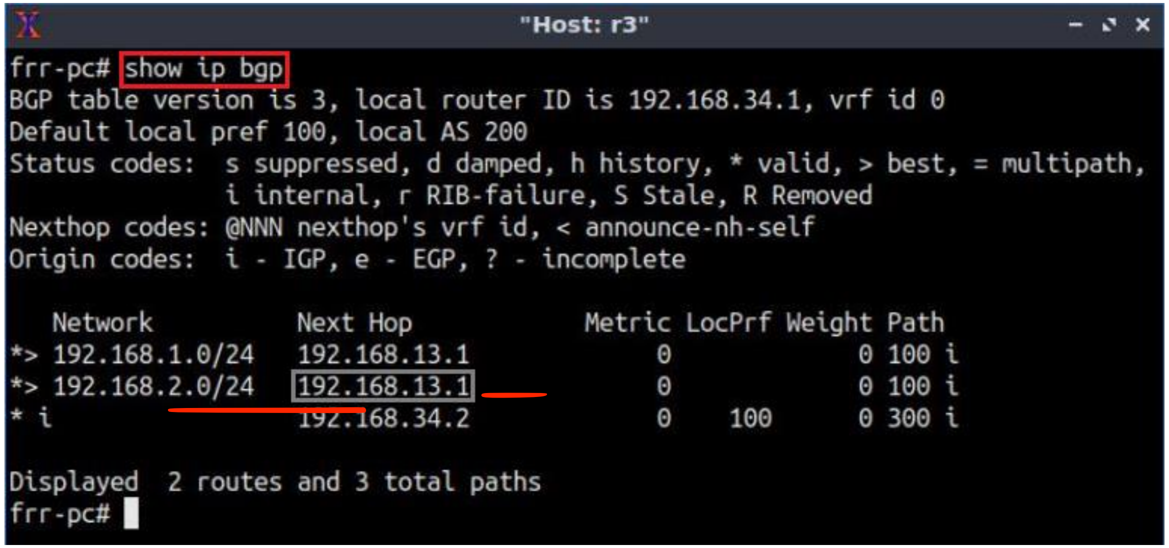


```
frr-pc# configure terminal
frr-pc(config)# router bgp 100
frr-pc(config-router)# network 192.168.2.0/24
frr-pc(config-router)#
```

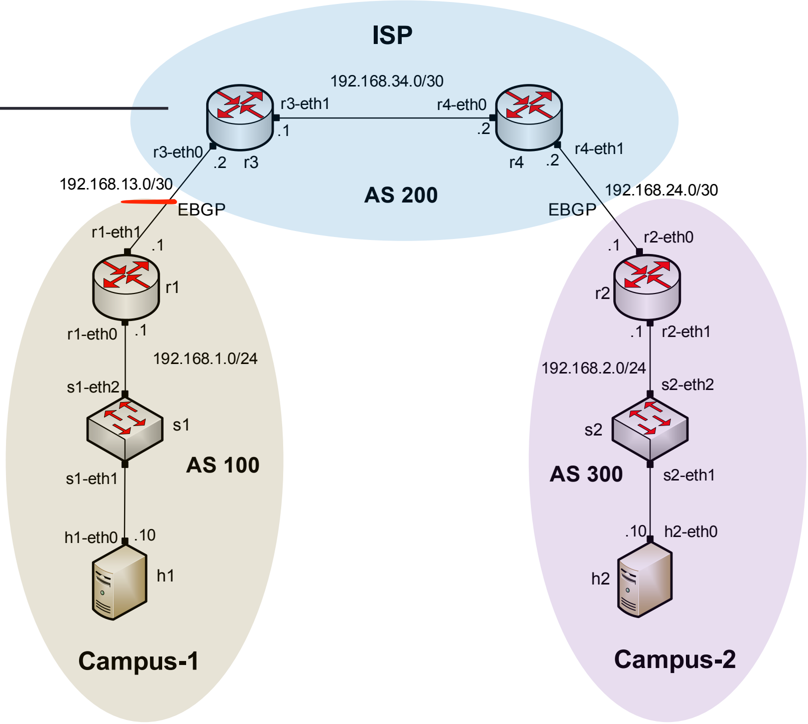
Lab 13 Configuration

- Router r3 changes the next hop of Campus-2 (192.168.2.0/24)

Router r3

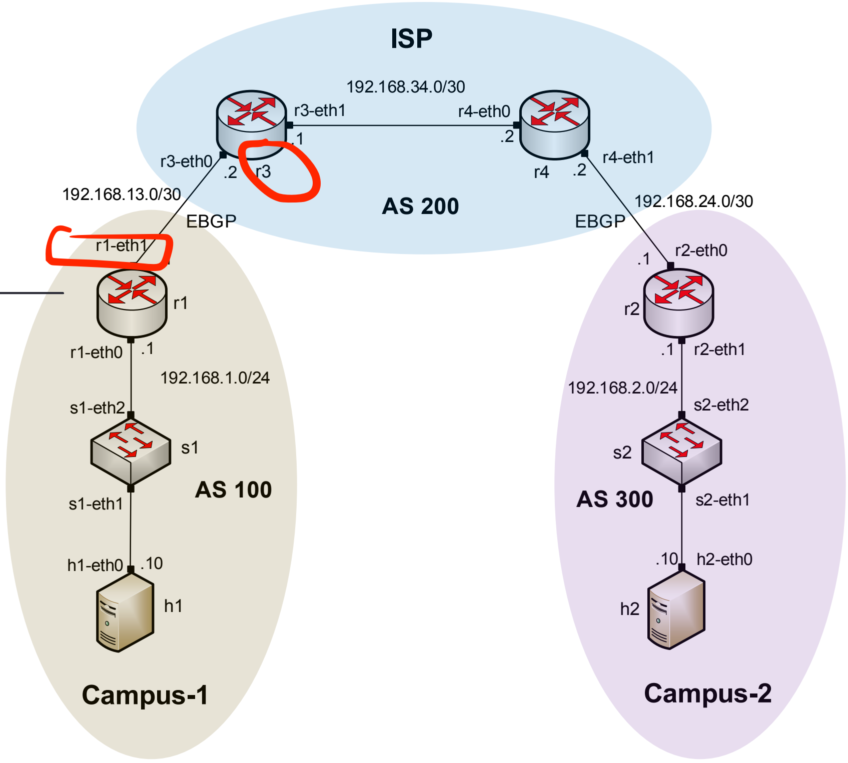


```
frr-pc# show ip bgp
BGP table version is 3, local router ID is 192.168.34.1, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0/24   192.168.13.1             0             0 100 i
*> 192.168.2.0/24   192.168.13.1             0             0 100 i
* i                 192.168.34.2             0    100      0 300 i

Displayed  2 routes and 3 total paths
frr-pc#
```

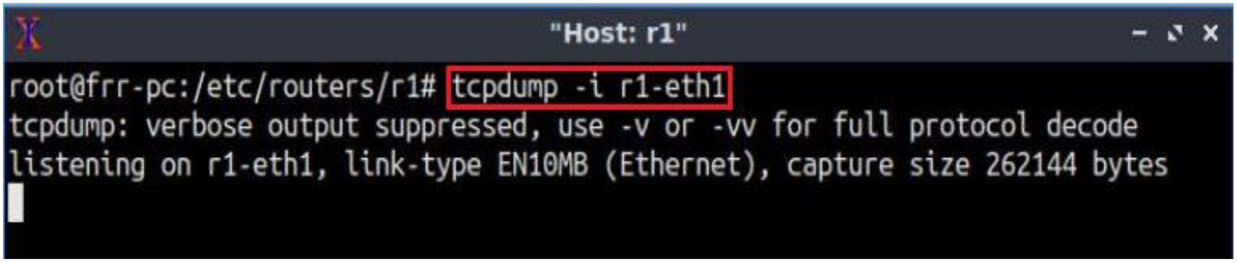


Lab 13 Configuration

- Capture the packets on router r1, specifically at r1-eth1



Router r1

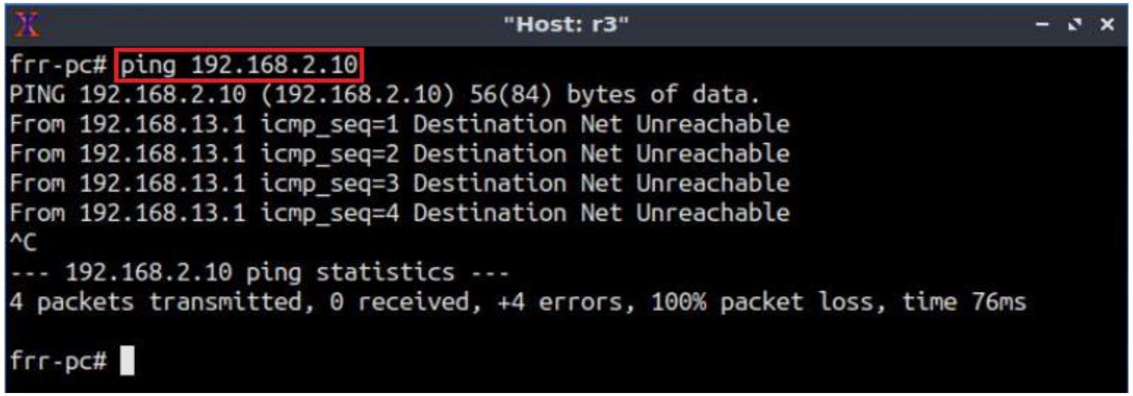


```
root@frr-pc:/etc/routers/r1# tcpdump -i r1-eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on r1-eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

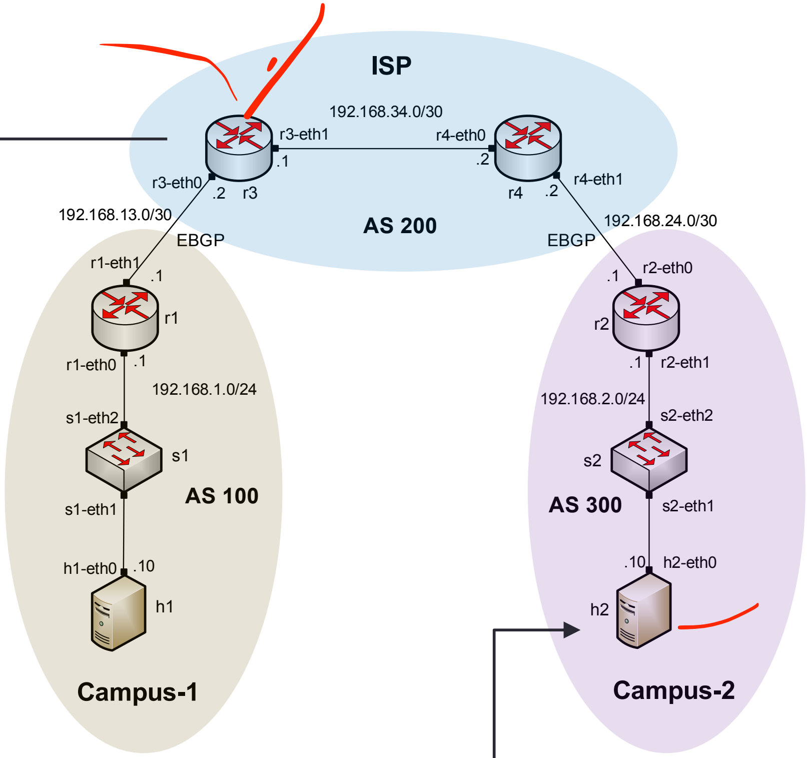
Lab 13 Configuration

- Ping the victim (192.168.2.10) from the ISP (router r3)

Router r3



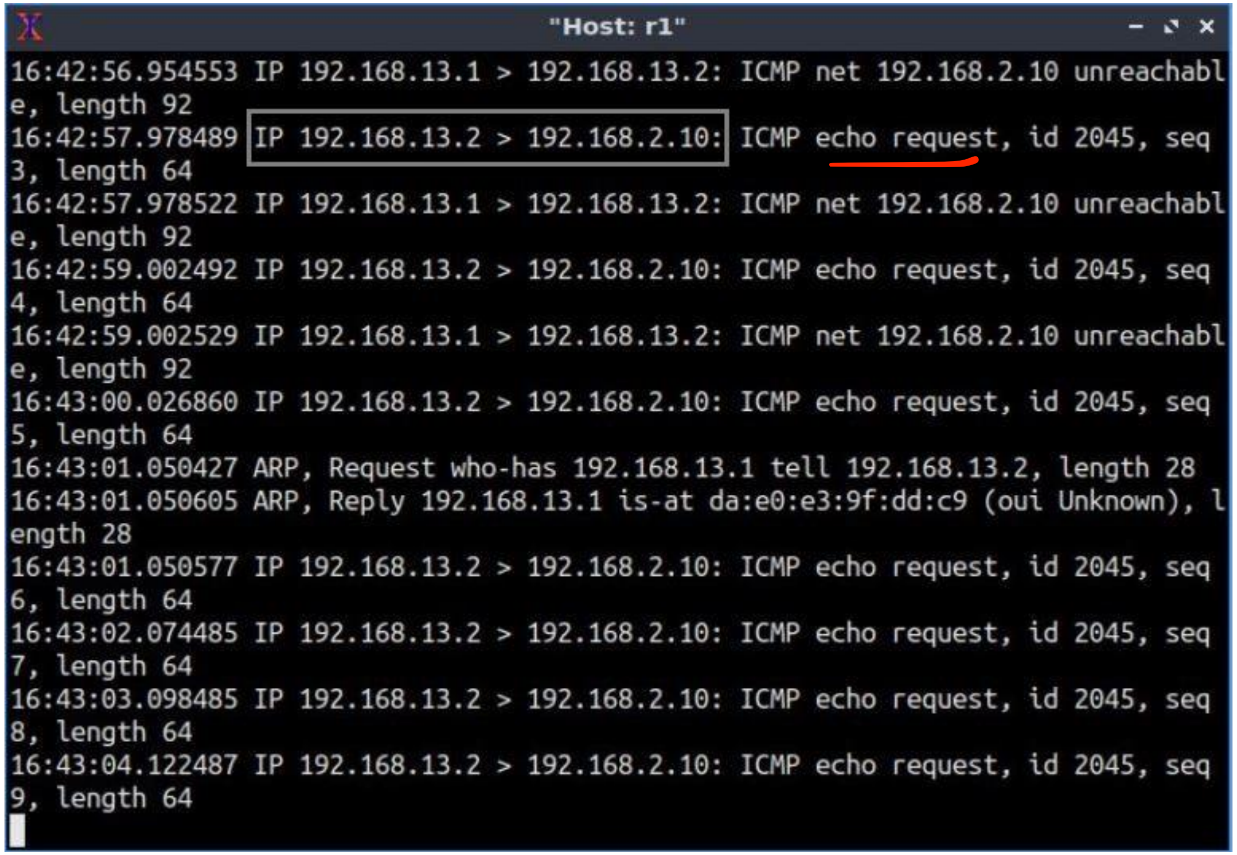
```
frr-pc# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
From 192.168.13.1 icmp_seq=1 Destination Net Unreachable
From 192.168.13.1 icmp_seq=2 Destination Net Unreachable
From 192.168.13.1 icmp_seq=3 Destination Net Unreachable
From 192.168.13.1 icmp_seq=4 Destination Net Unreachable
^C
--- 192.168.2.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 76ms

frr-pc# 
```



victim

Lab 13 Configuration

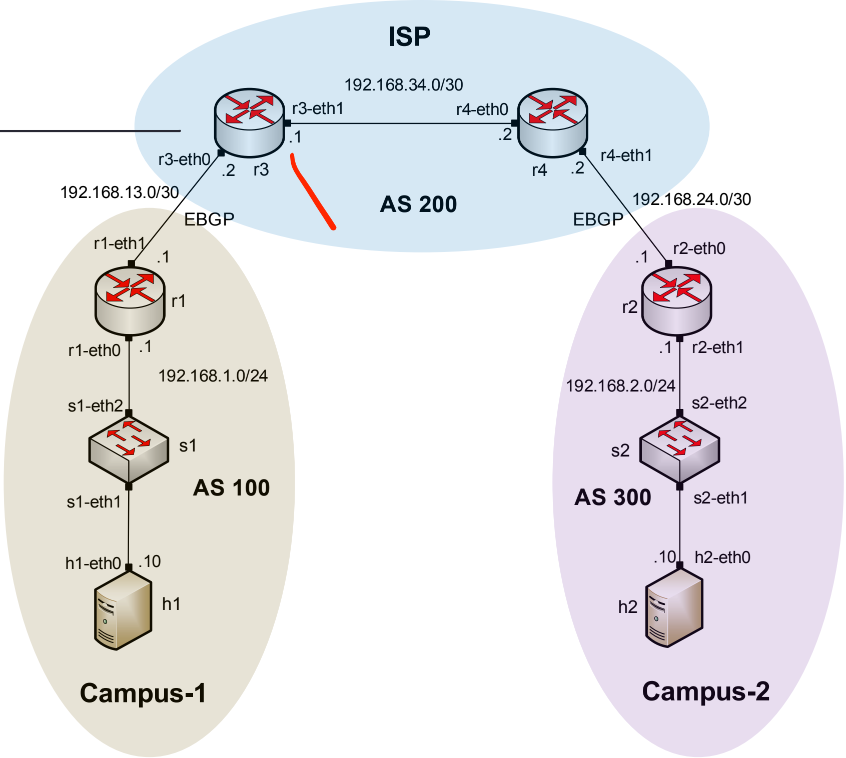
- The traffic to network 192.168.2.10 will be rerouted to the hijacking router



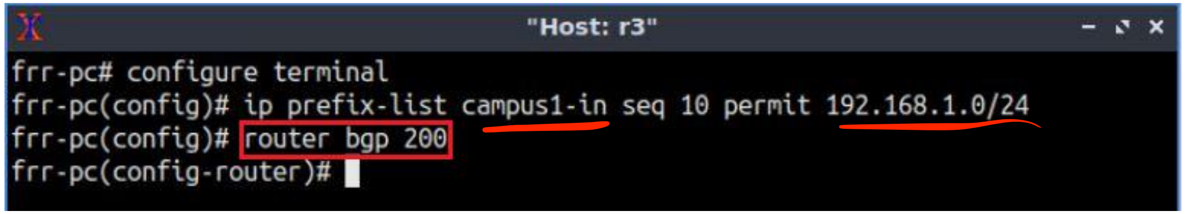
```
16:42:56.954553 IP 192.168.13.1 > 192.168.13.2: ICMP net 192.168.2.10 unreachabl
e, length 92
16:42:57.978489 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
3, length 64
16:42:57.978522 IP 192.168.13.1 > 192.168.13.2: ICMP net 192.168.2.10 unreachabl
e, length 92
16:42:59.002492 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
4, length 64
16:42:59.002529 IP 192.168.13.1 > 192.168.13.2: ICMP net 192.168.2.10 unreachabl
e, length 92
16:43:00.026860 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
5, length 64
16:43:01.050427 ARP, Request who-has 192.168.13.1 tell 192.168.13.2, length 28
16:43:01.050605 ARP, Reply 192.168.13.1 is-at da:e0:e3:9f:dd:c9 (oui Unknown), l
ength 28
16:43:01.050577 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
6, length 64
16:43:02.074485 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
7, length 64
16:43:03.098485 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
8, length 64
16:43:04.122487 IP 192.168.13.2 > 192.168.2.10: ICMP echo request, id 2045, seq
9, length 64
```

Lab 13 Configuration

- Configure IP prefix list on the ISP (router r3)



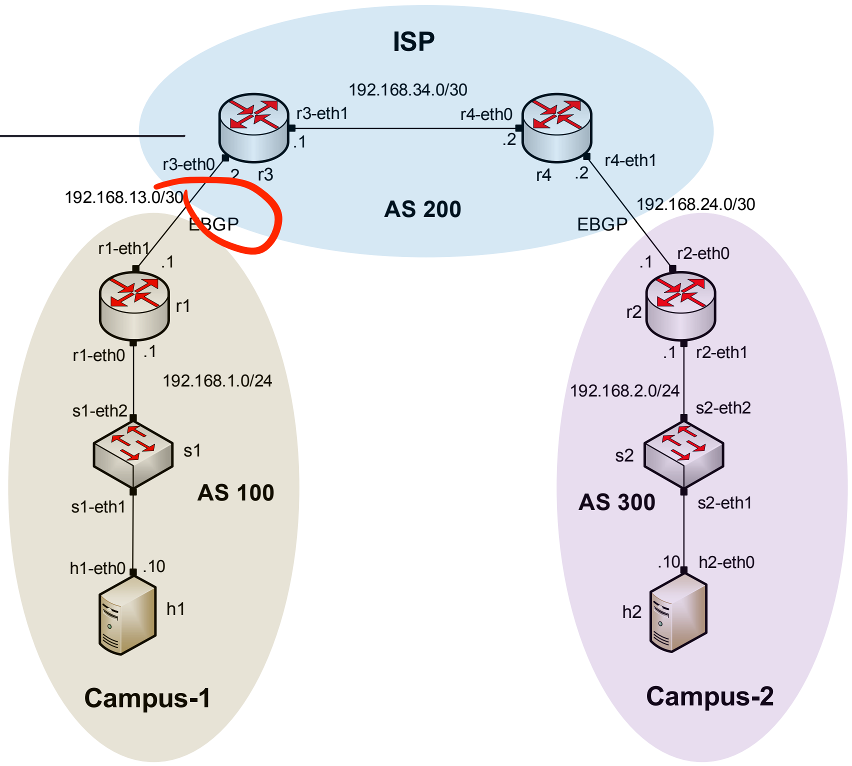
Router r3



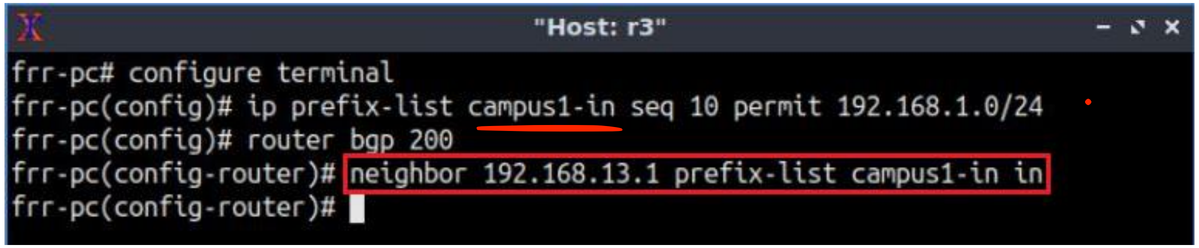
```
frr-pc# configure terminal
frr-pc(config)# ip prefix-list campus1-in seq 10 permit 192.168.1.0/24
frr-pc(config)# router bgp 200
frr-pc(config-router)#
```

Lab 13 Configuration

- Apply the prefix list to router r3 neighbor



Router r3

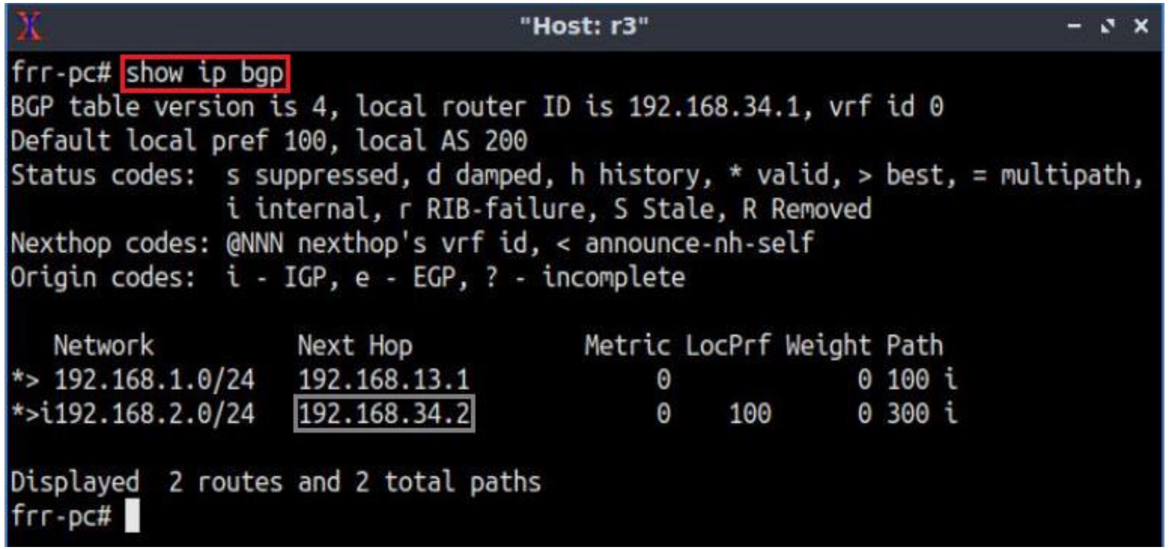


```
frr-pc# configure terminal
frr-pc(config)# ip prefix-list campus1-in seq 10 permit 192.168.1.0/24
frr-pc(config)# router bgp 200
frr-pc(config-router)# neighbor 192.168.13.1 prefix-list campus1-in in
frr-pc(config-router)# 
```

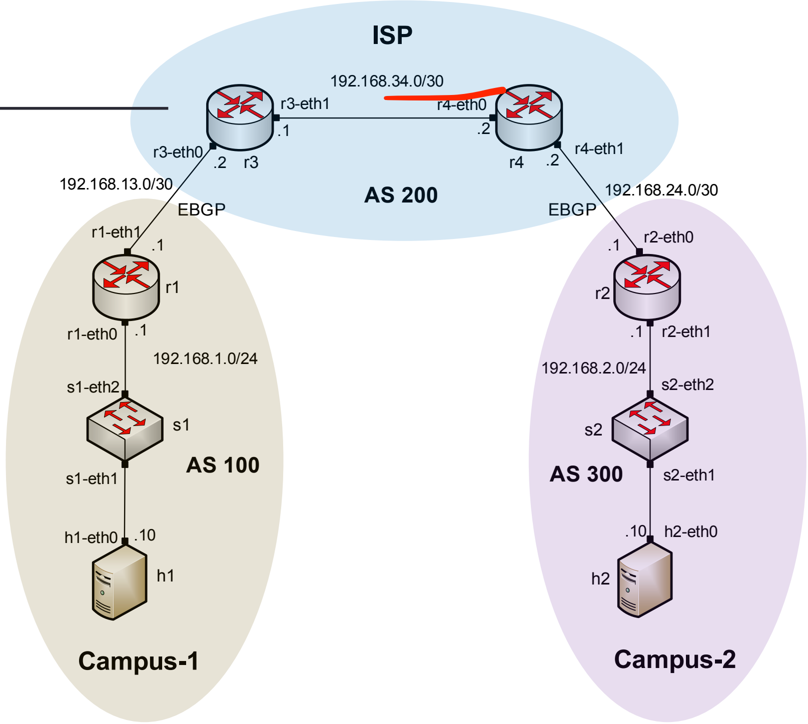
Lab 13 Configuration

- Router r3 readjusts its BGP table back to normal

Router r3



```
frr-pc# show ip bgp
BGP table version is 4, local router ID is 192.168.34.1, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0/24   192.168.13.1             0             0 100 i
*>i192.168.2.0/24   192.168.34.2             0    100      0 300 i

Displayed  2 routes and 2 total paths
frr-pc# 
```


ISP
192.168.34.0/30
r3-eth1
r4-eth0
.1
.2
r3-eth0
.2
r3
r4
.2
r4-eth1
192.168.13.0/30
AS 200
192.168.24.0/30
EBGP
EBGP
r1-eth1
.1
.1
r2-eth0
r1
r2
r1-eth0
.1
.1
r2-eth1
192.168.1.0/24
192.168.2.0/24
s1-eth2
s2-eth2
s1
s2
AS 100
AS 300
s1-eth1
s2-eth1
h1-eth0
.10
.10
h2-eth0
h1
h2
Campus-1
Campus-2