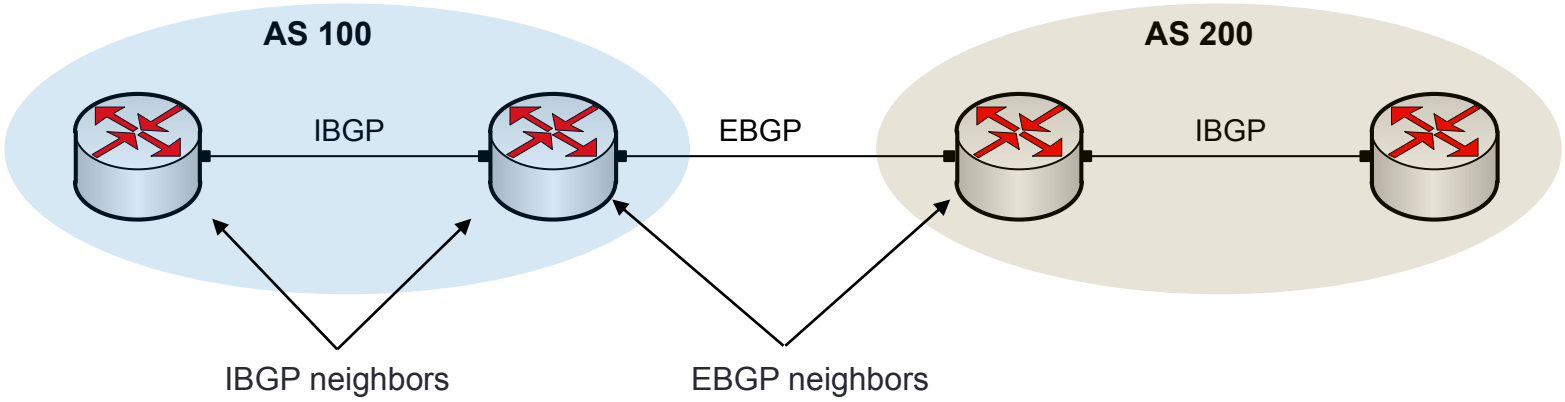
What will be covered ?

- Attacks on BGP protocol and security mechanisms
- Class 1: BGP basics
- Class 1: BGP Authentication
- Class 2: BGP Hijacking and mitigation techniques
- Class 2: IP spoofing, DoS attacks, and mitigation techniques

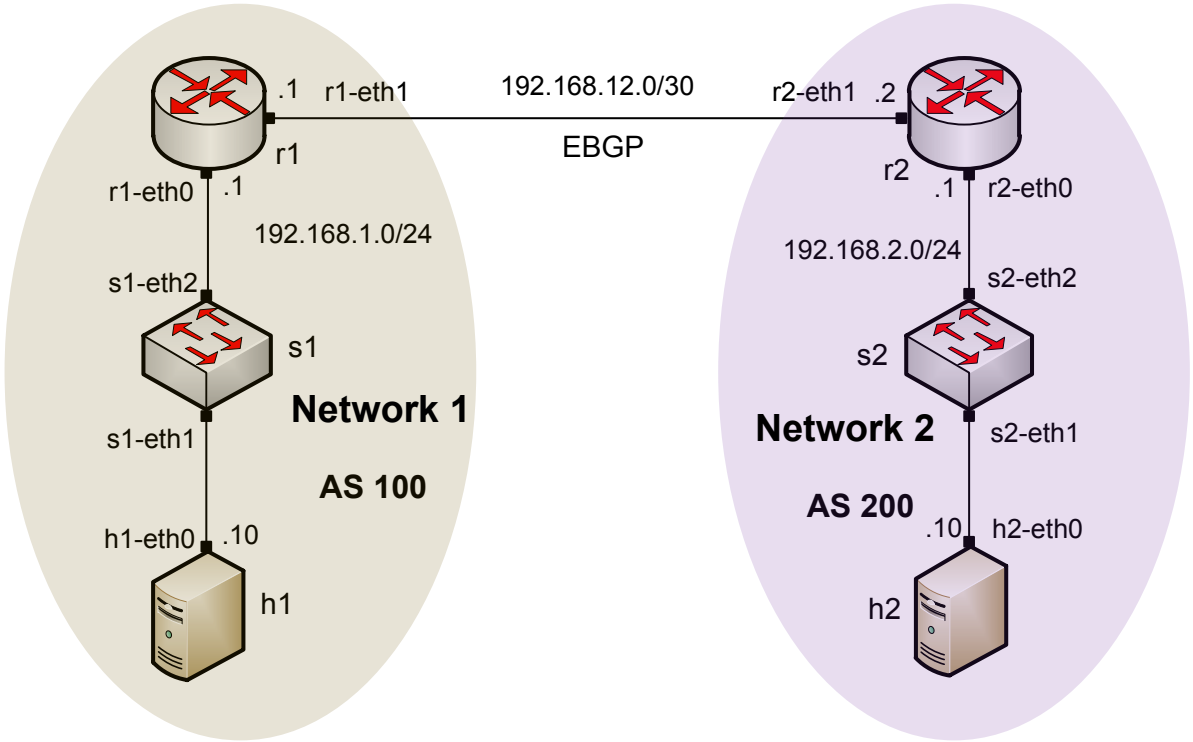
What is BGP?

- The Internet can be viewed as a collection of networks or Autonomous Systems (ASes) that are interconnected
- BGP is an exterior gateway protocol designed to exchange routing and reachability information among ASes on the Internet



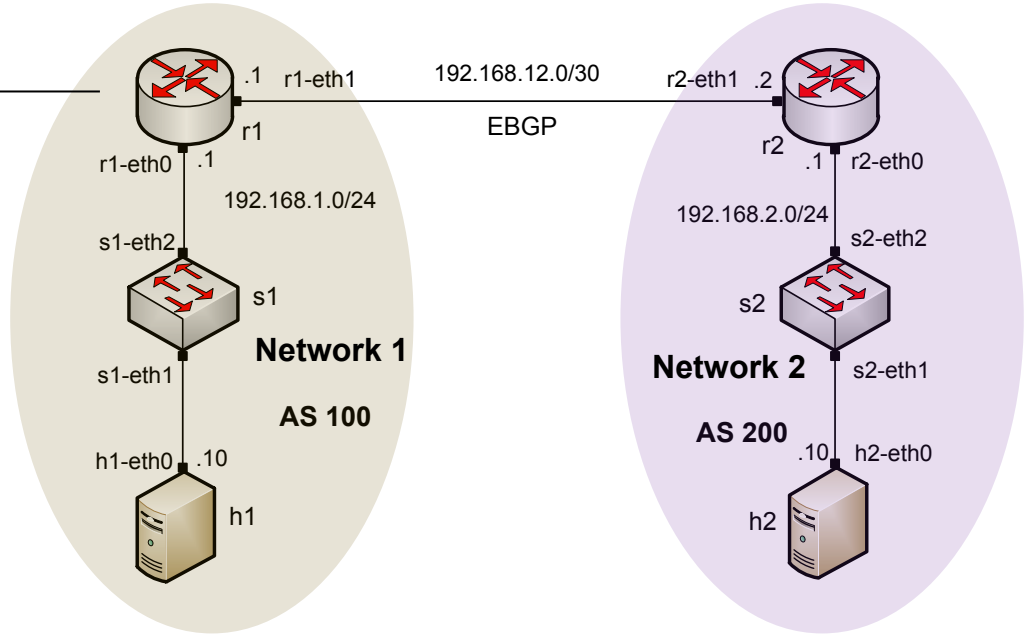
Lab 3 Topology

- Network 1 in AS 100 consists of a host, a switch, and a router
- Network 2 in AS 200 consists of a host, a switch, and a router



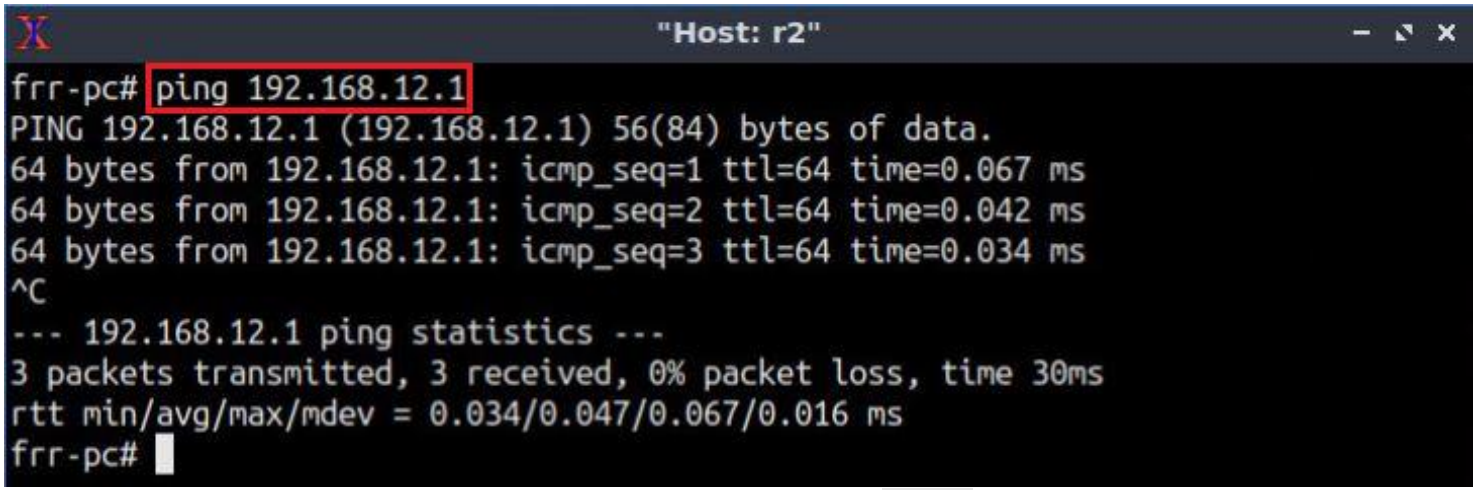
Lab 3 Configuration

- Establishing BGP neighborhood



Router r1

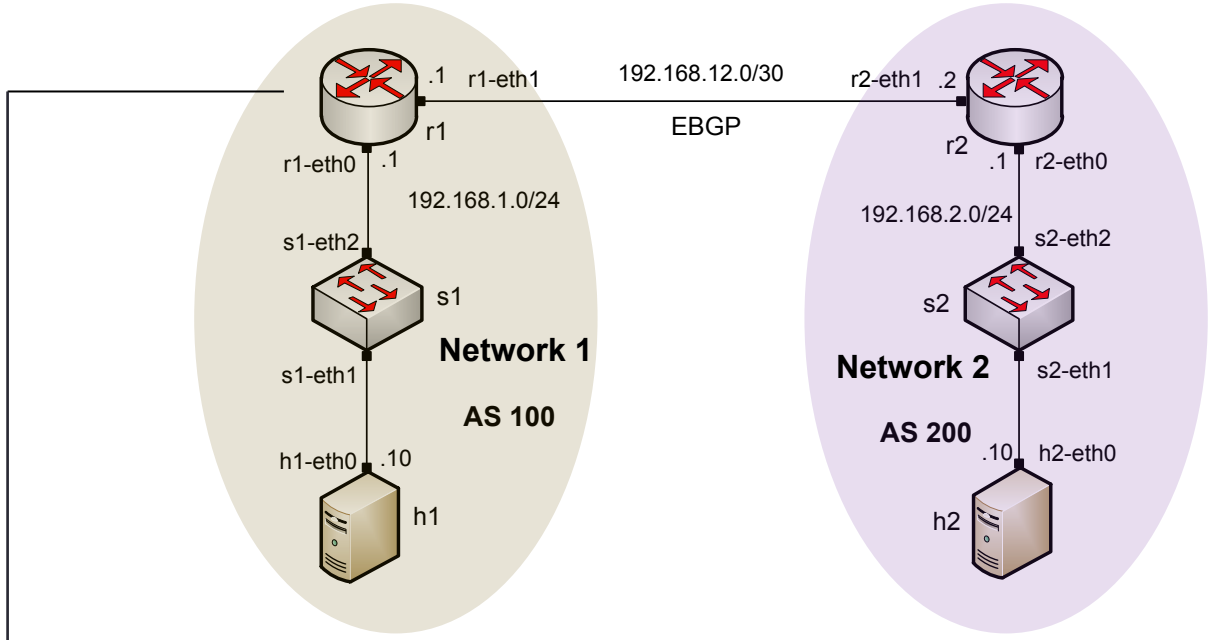
```
"Host: r1"
root@frr-pc:/etc/routers/r1# bgpd
root@frr-pc:/etc/routers/r1# vtysh

Hello, this is FRRouting (version 7.2-dev).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr-pc# configure terminal
frr-pc(config)# router bgp 100
frr-pc(config-router)# neighbor 192.168.12.2 remote-as 200
frr-pc(config-router)#
```


"Host: r2"
frr-pc# ping 192.168.12.1
PING 192.168.12.1 (192.168.12.1) 56(84) bytes of data.
64 bytes from 192.168.12.1: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 192.168.12.1: icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from 192.168.12.1: icmp_seq=3 ttl=64 time=0.034 ms
^C
--- 192.168.12.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 30ms
rtt min/avg/max/mdev = 0.034/0.047/0.067/0.016 ms
frr-pc#


"Host: r2"
frr-pc# ping 192.168.1.10
connect: Network is unreachable
frr-pc#

Lab 3 Configuration

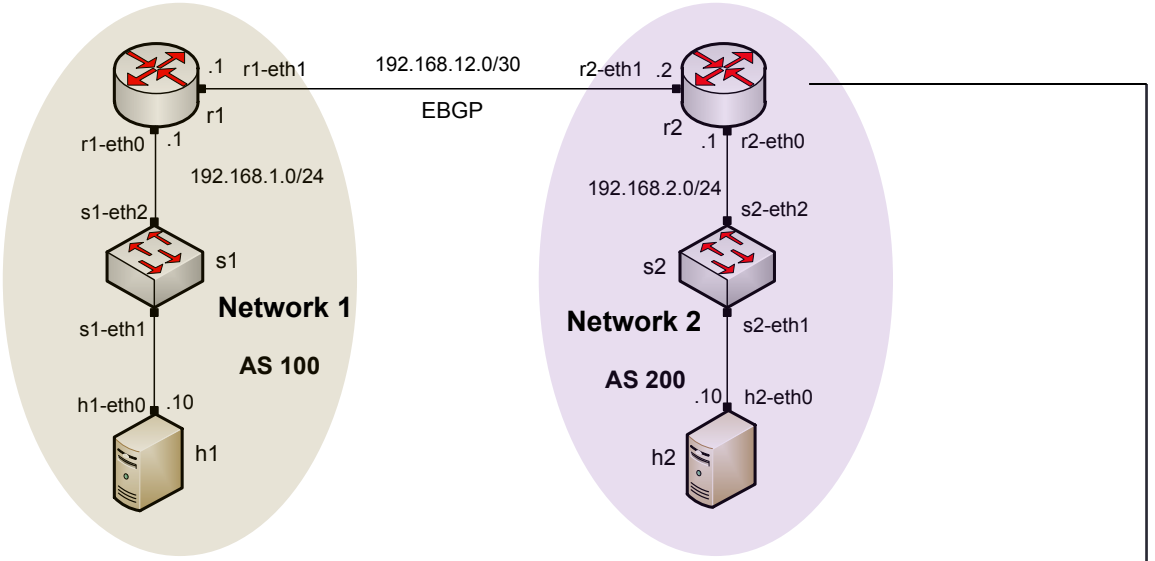
- Advertising a network in BGP

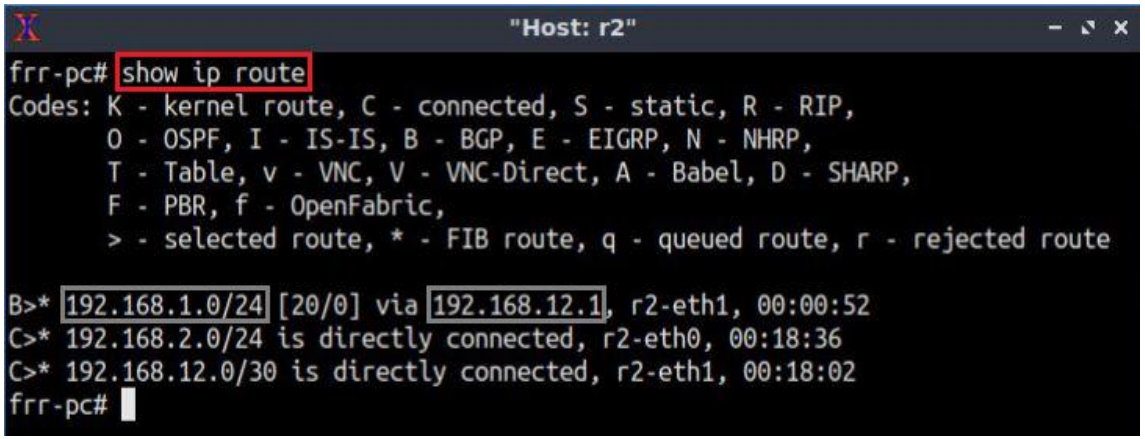


Router r1

Lab 3 Configuration

- Routing table: lists the routes learned from different routing protocols

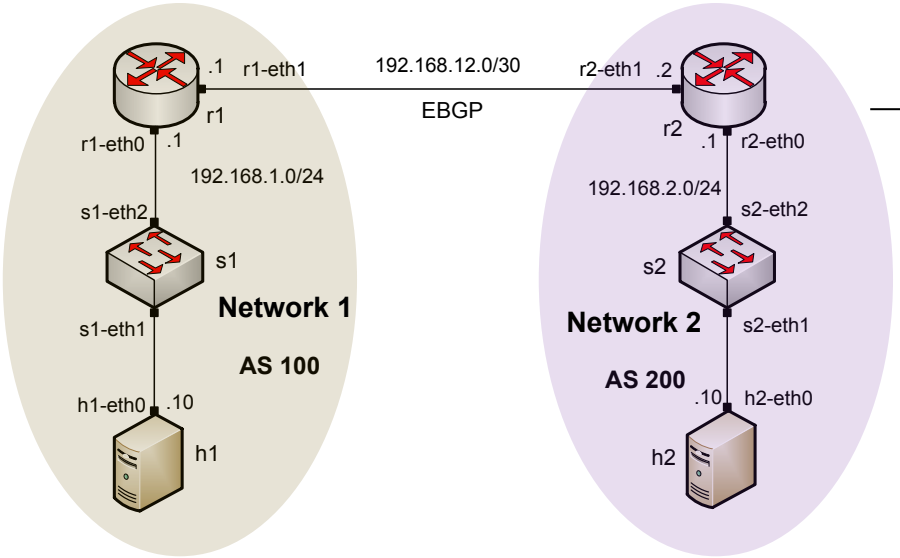


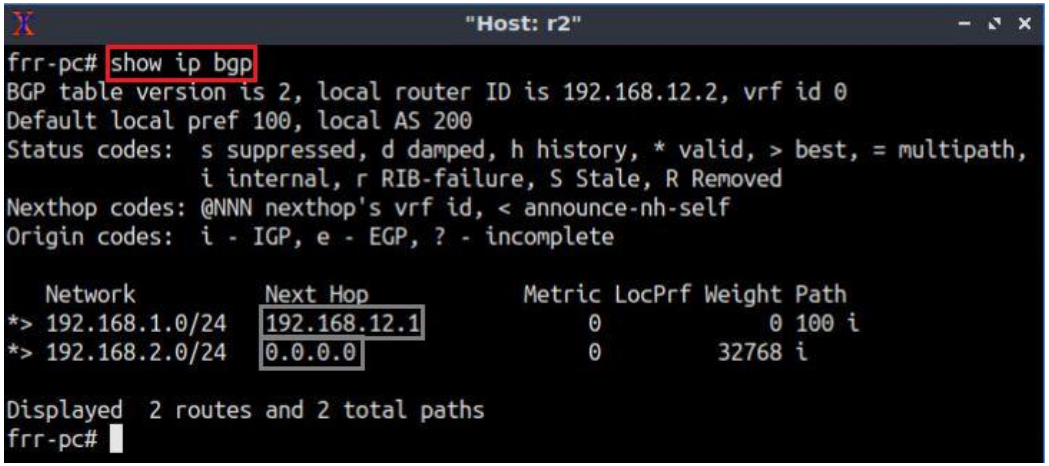


Router r2

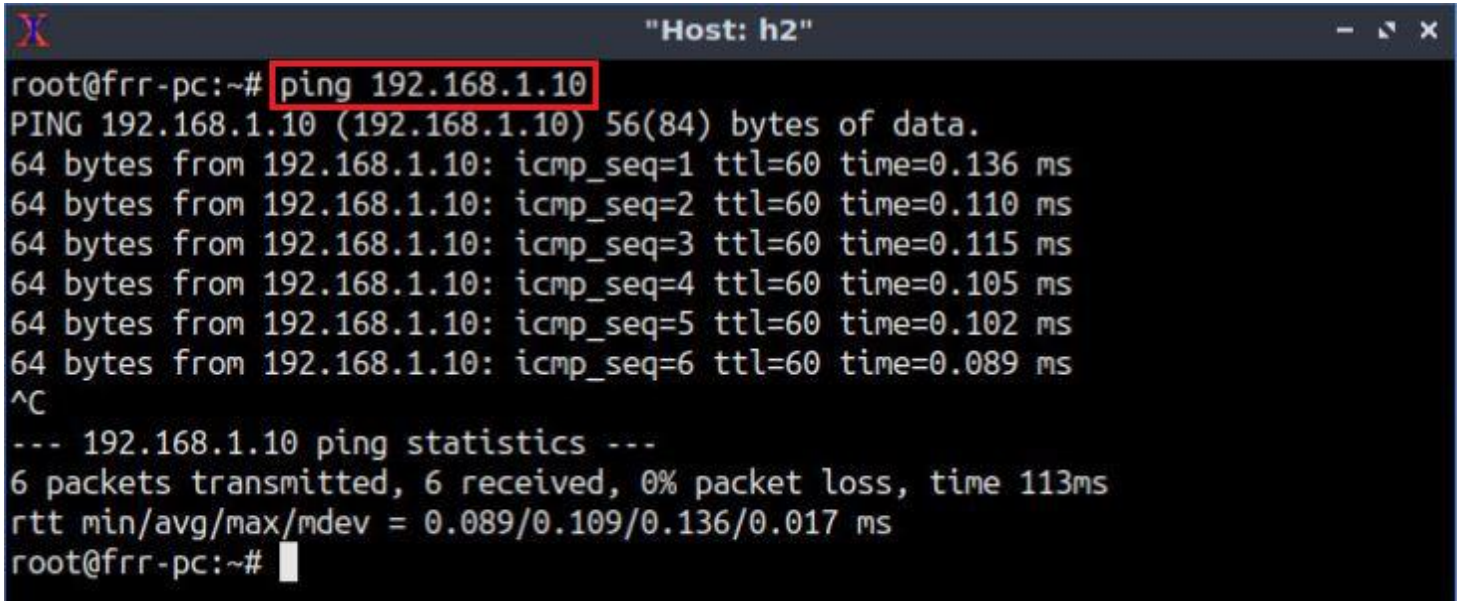
Lab 3 Configuration

- BGP table: lists the routes learned from BGP routing protocol





Router r2


"Host: h2"
root@frr-pc:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=60 time=0.136 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=60 time=0.110 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=60 time=0.115 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=60 time=0.105 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=60 time=0.102 ms
64 bytes from 192.168.1.10: icmp_seq=6 ttl=60 time=0.089 ms
^C
--- 192.168.1.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 113ms
rtt min/avg/max/mdev = 0.089/0.109/0.136/0.017 ms
root@frr-pc:~#

Security issues

- A router may be talking to a wrong device
  1. Reroutes traffic to an intruder (advertise prefix)
  2. Pretends to be your friend (spoofing)

- Content/Advertisements can be modified in transit

TCP reset attacks

EBGP sessions run over TCP

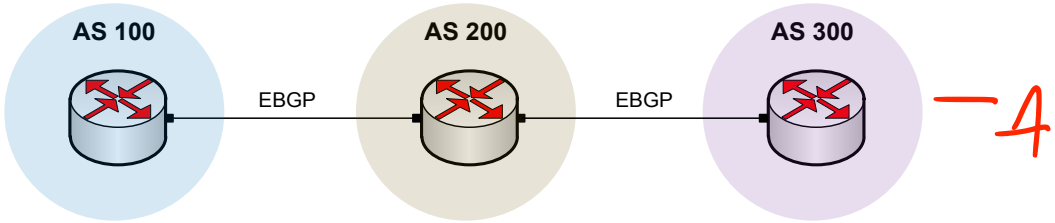


Figure 1. Routers in different ASes run EBGP to advertise routing information.

- If AS 100 sends *TCP reset packet* to AS 200, AS200 tear down TCP session with AS100
- An attacker can send a spoofed TCP reset to AS200 -- interrupts traffic flow between AS100 and AS200
- What an attacker needs?
  - right IP address, BGP port (179), right seq number
  - Simply sends packets with all possible sequence numbers – takes a minute or so

Security mechanism: TCP MD5 Hash Algorithm and password

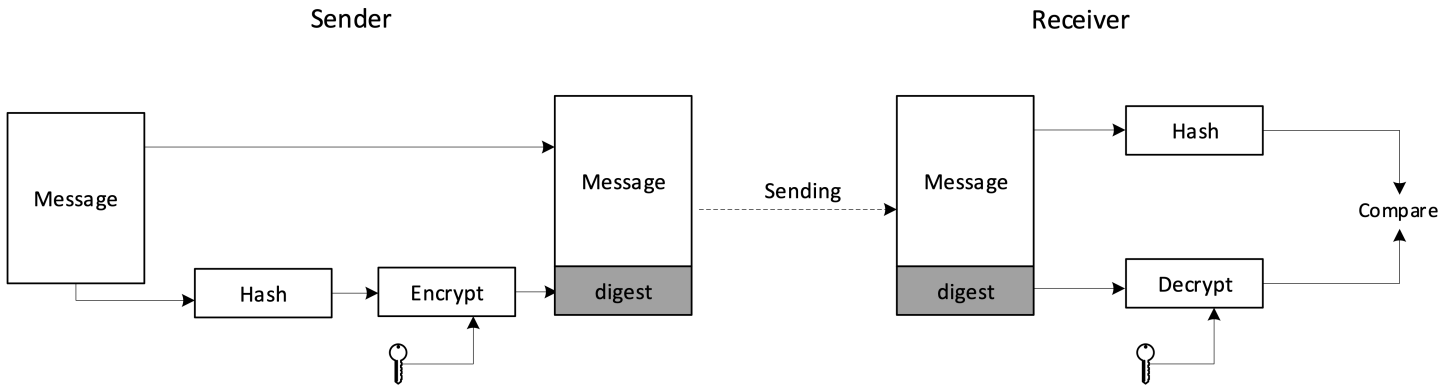
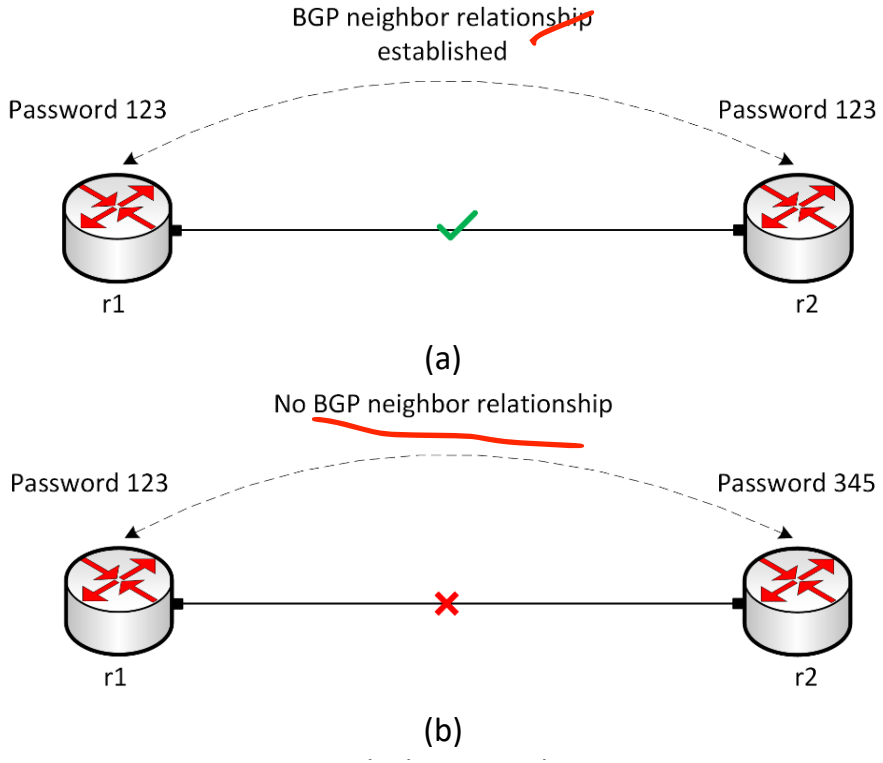


Figure 2. MD5 hash algorithm.

- TCP MD5 hash algorithm
  - Cryptographic function
  - Input: Arbitrary length message
  - Output: 128-bit message digest

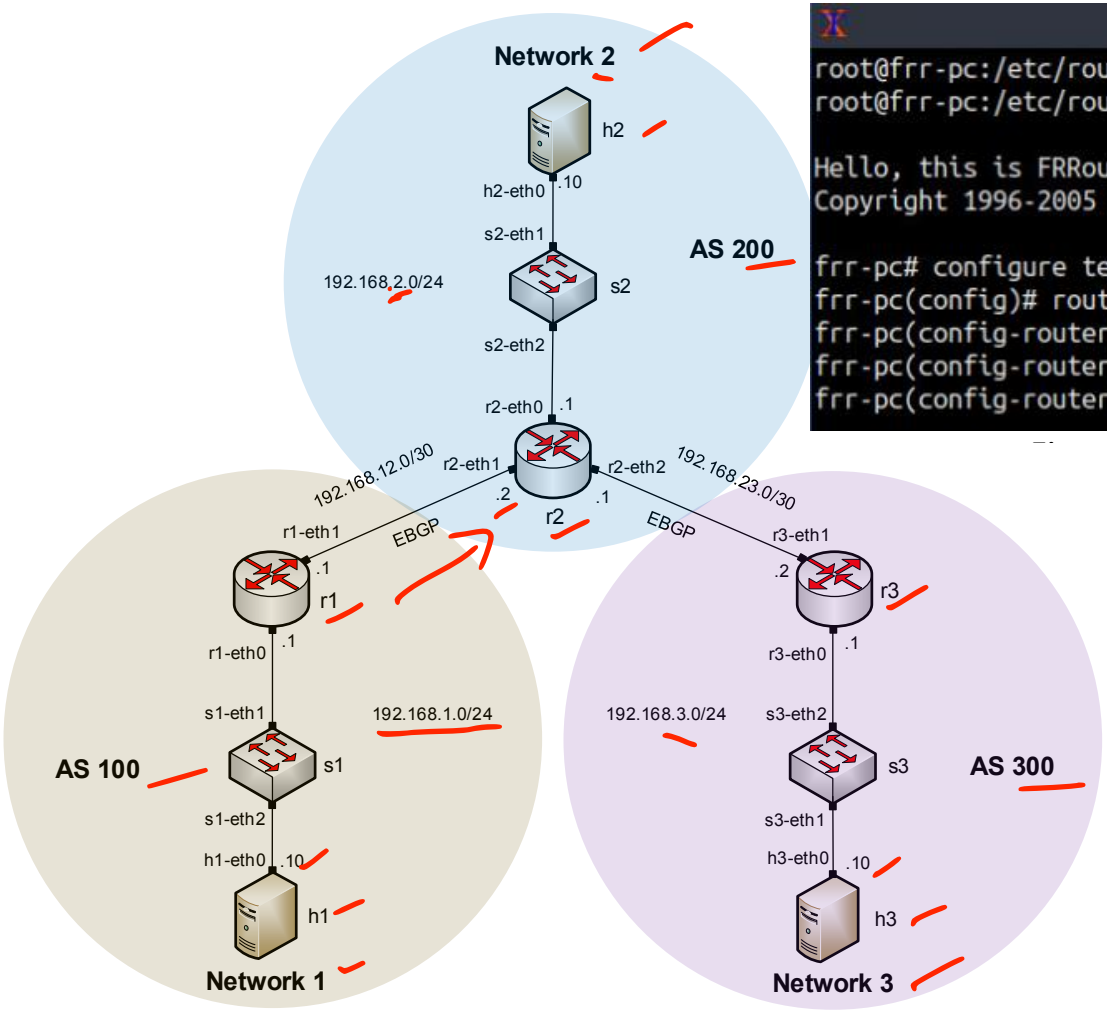
- Computationally hard to produce
  - Two messages with same digest
  - Same message given a digest

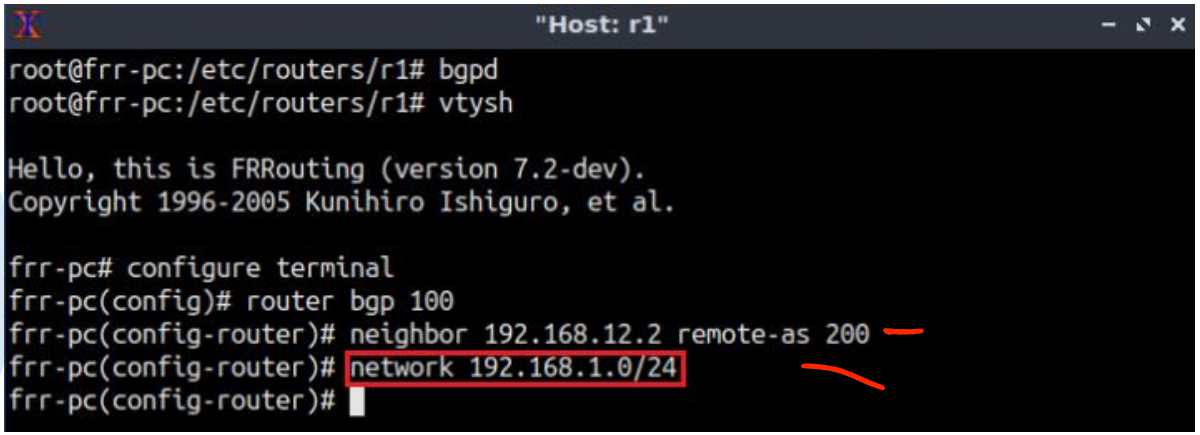
BGP Authentication



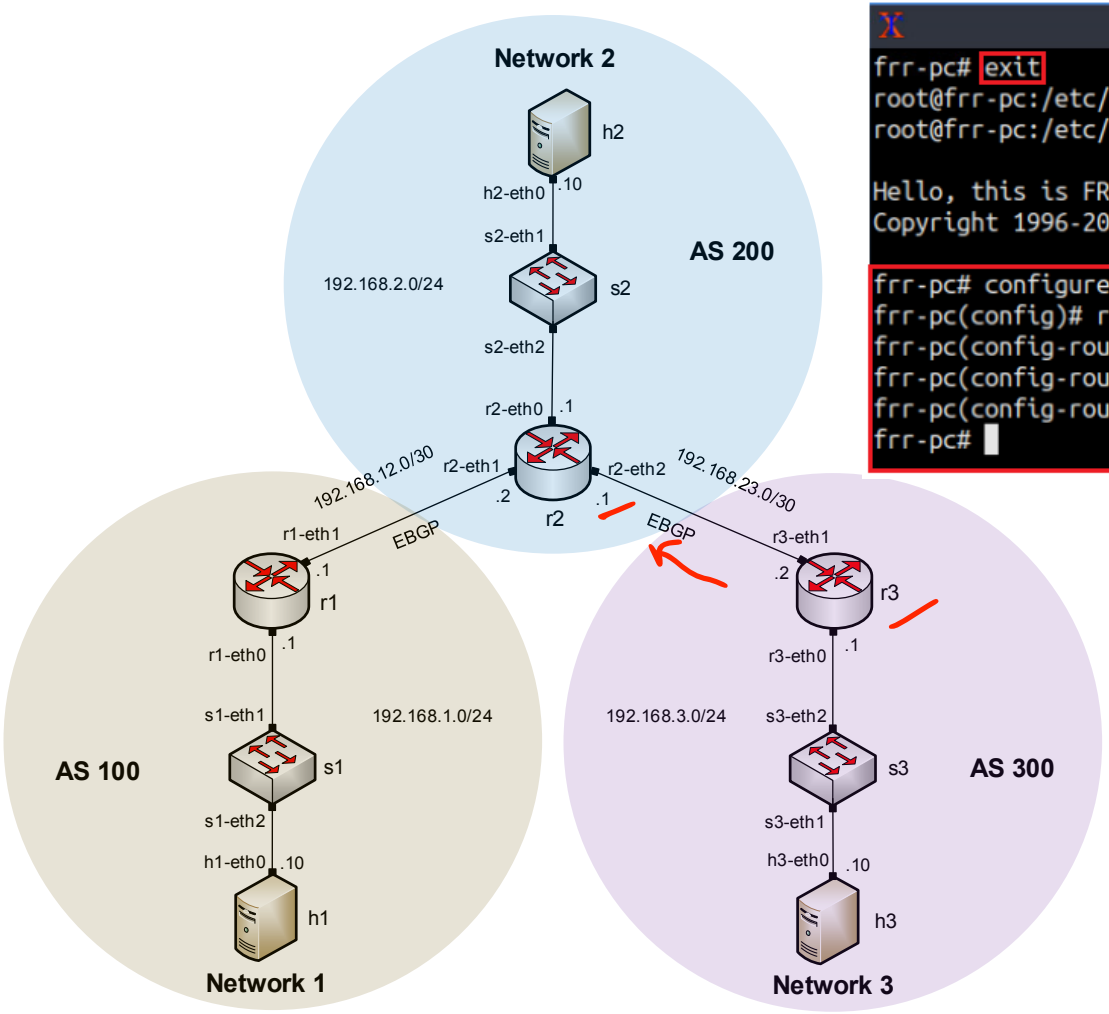
BGP peers must be configured with the same password to establish BGP neighbor relationship

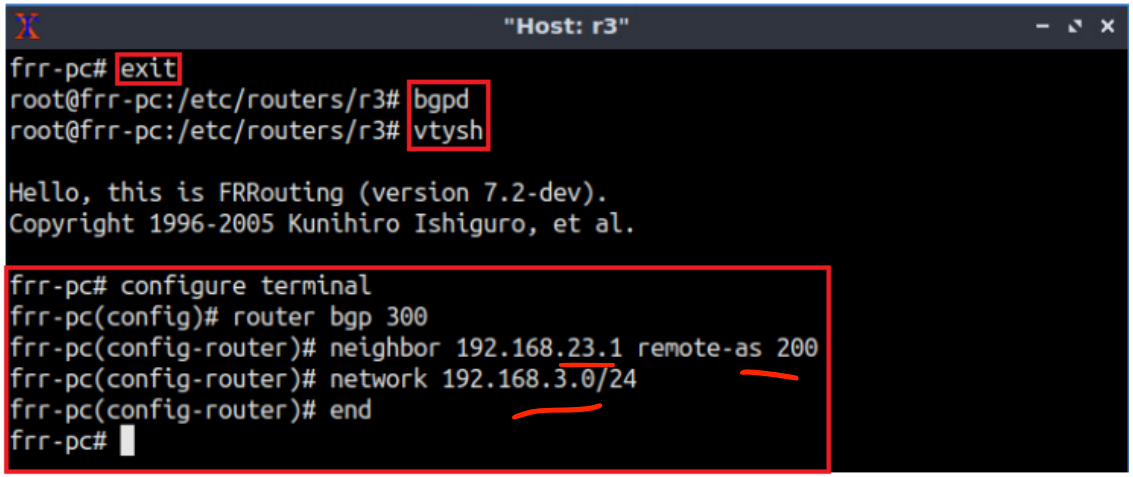
Example topology



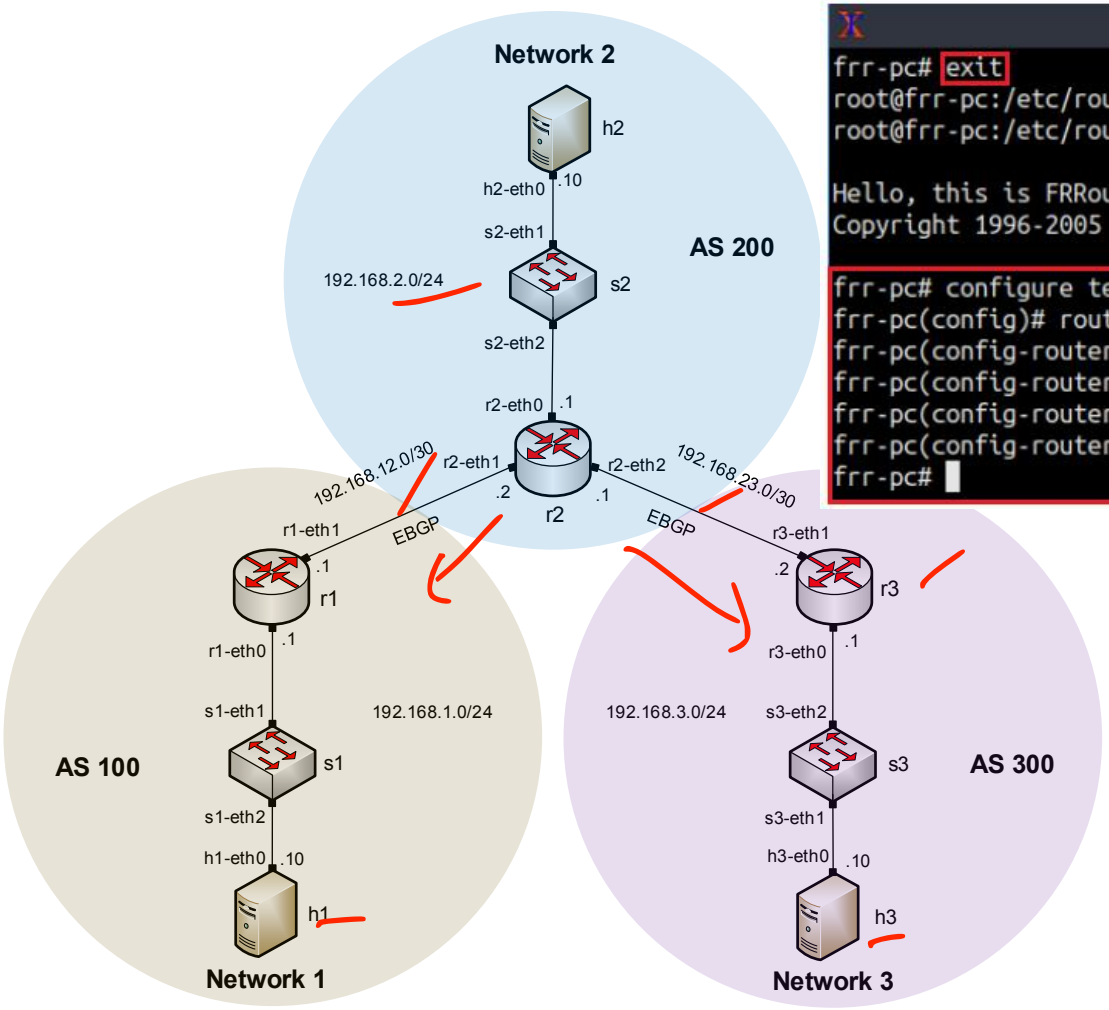


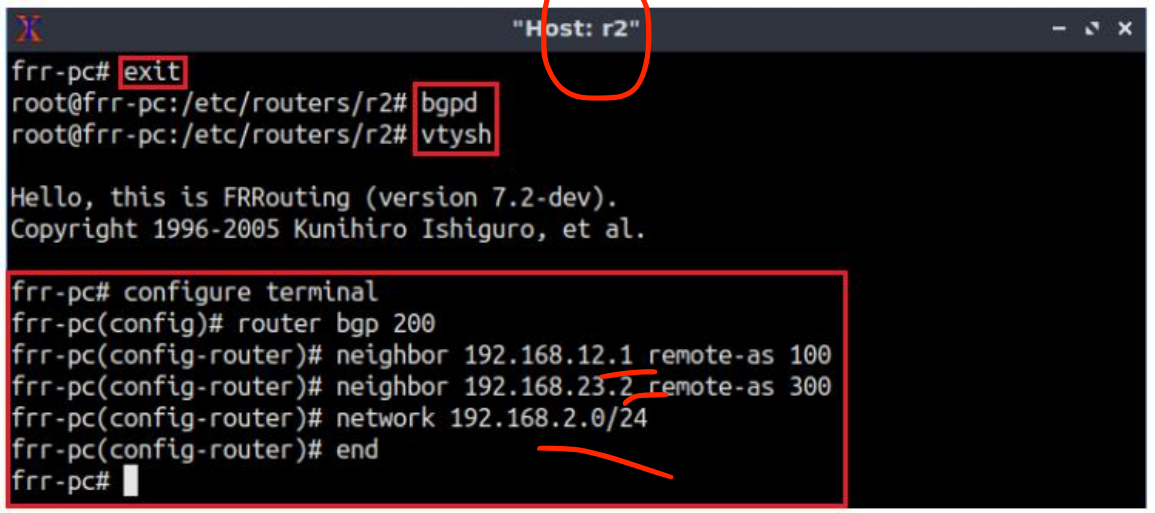
Example topology

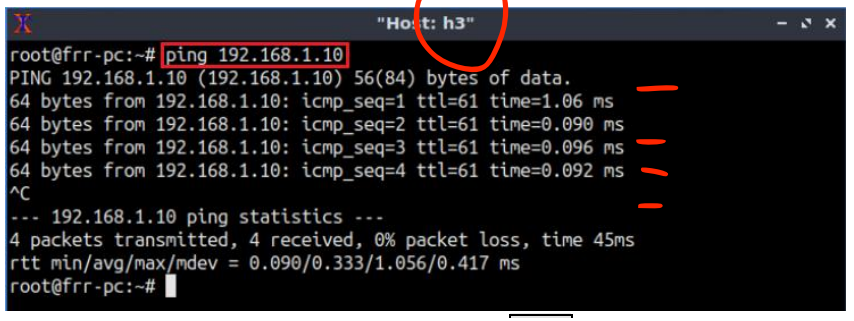




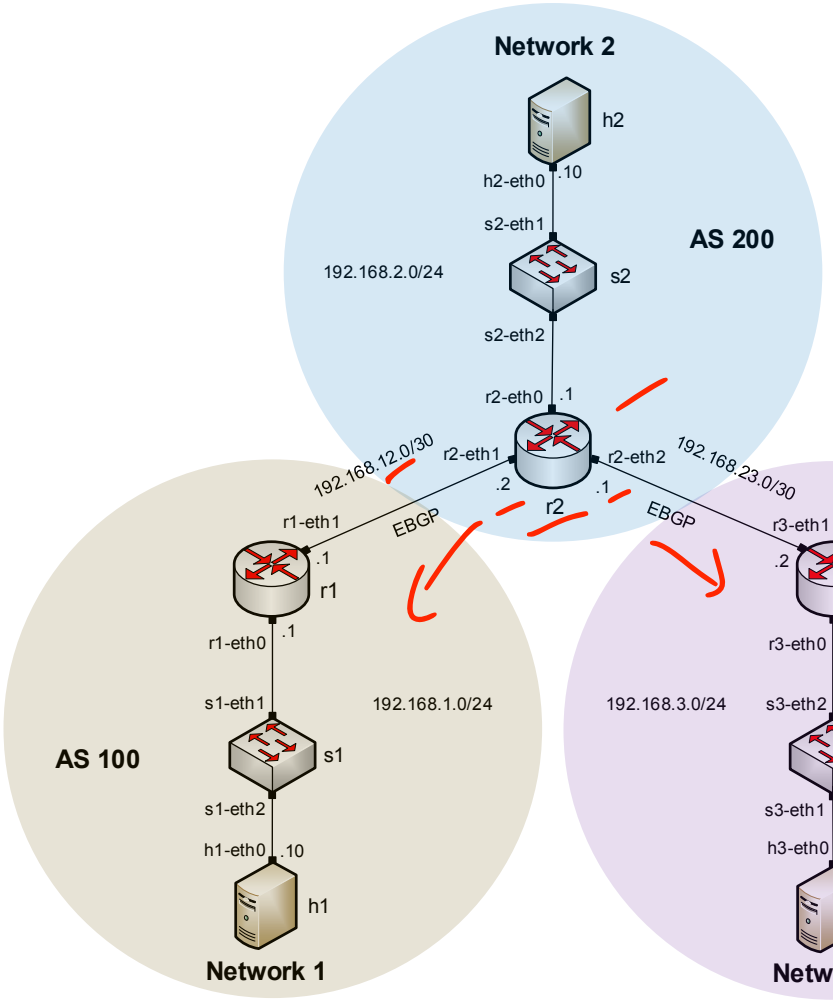
Example topology







Set up password

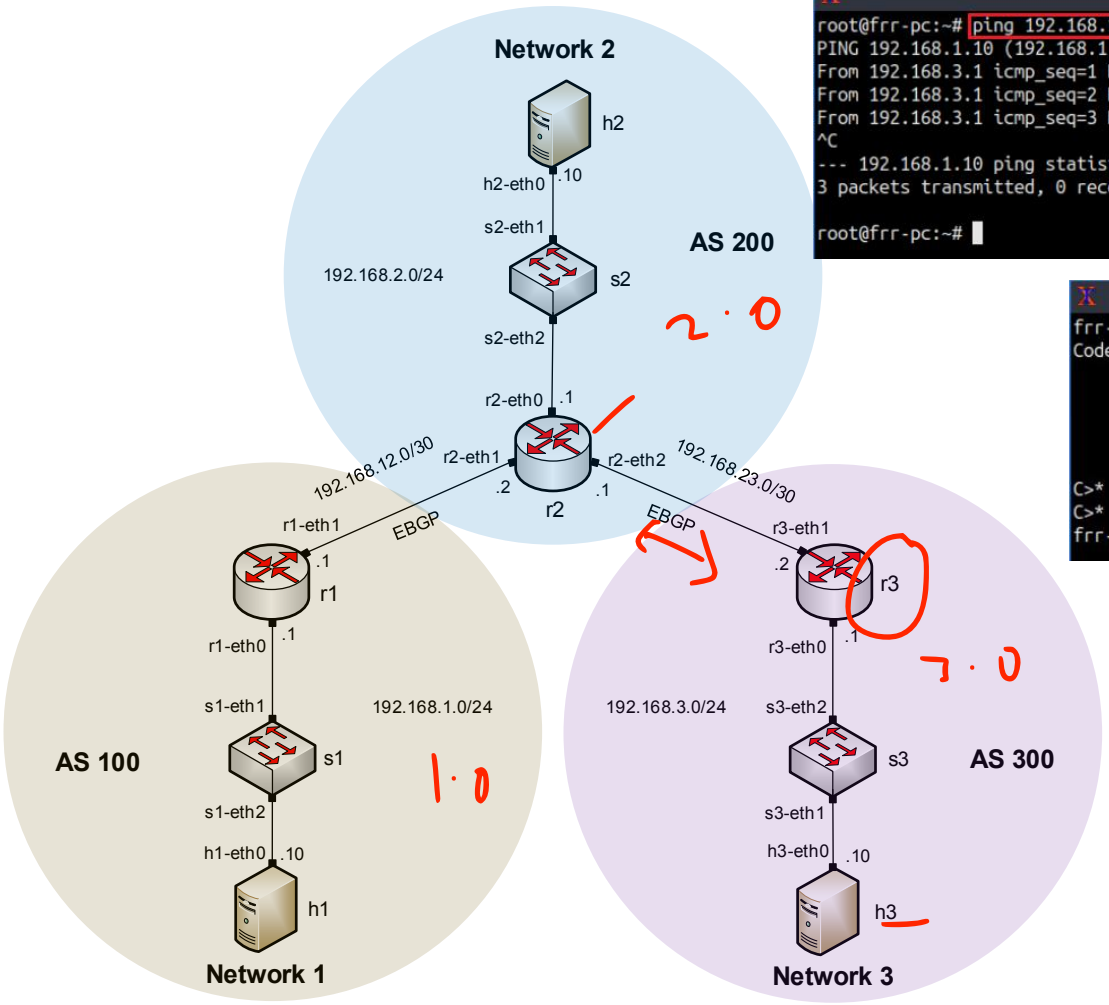


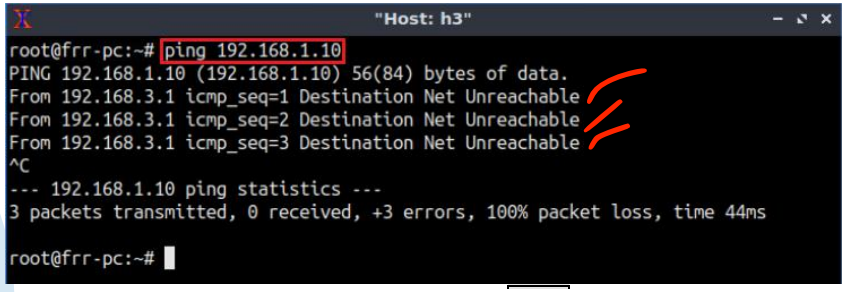

```
"Host: r1"
frr-pc# configure terminal
frr-pc(config)# router bgp 100
frr-pc(config-router)# neighbor 192.168.12.2 password 123
frr-pc(config-router)#
```

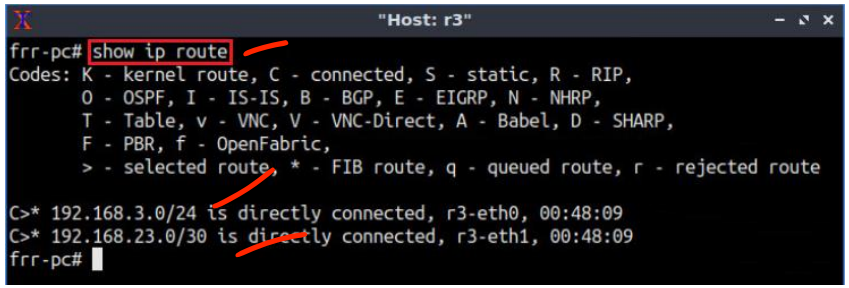
```
"Host: r2"
frr-pc# configure terminal
frr-pc(config)# router bgp 200
frr-pc(config-router)# neighbor 192.168.12.1 password 123
frr-pc(config-router)# neighbor 192.168.23.2 password 123
frr-pc(config-router)# end
frr-pc#
```

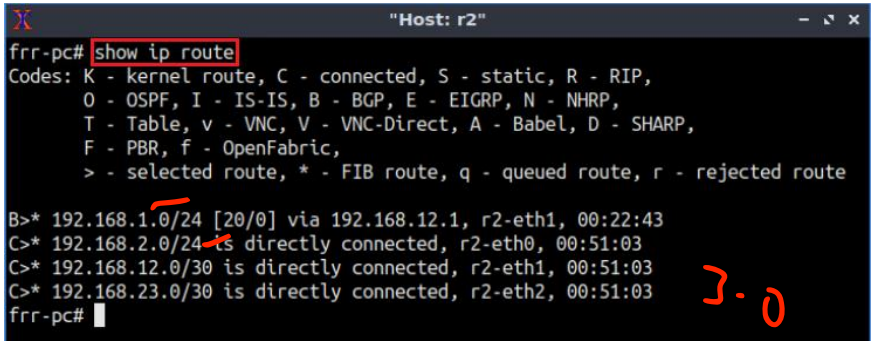
```
"Host: r3"
frr-pc# configure terminal
frr-pc(config)# router bgp 300
frr-pc(config-router)# neighbor 192.168.23.1 password 345
frr-pc(config-router)# end
frr-pc#
```

Verify MD5 authentication

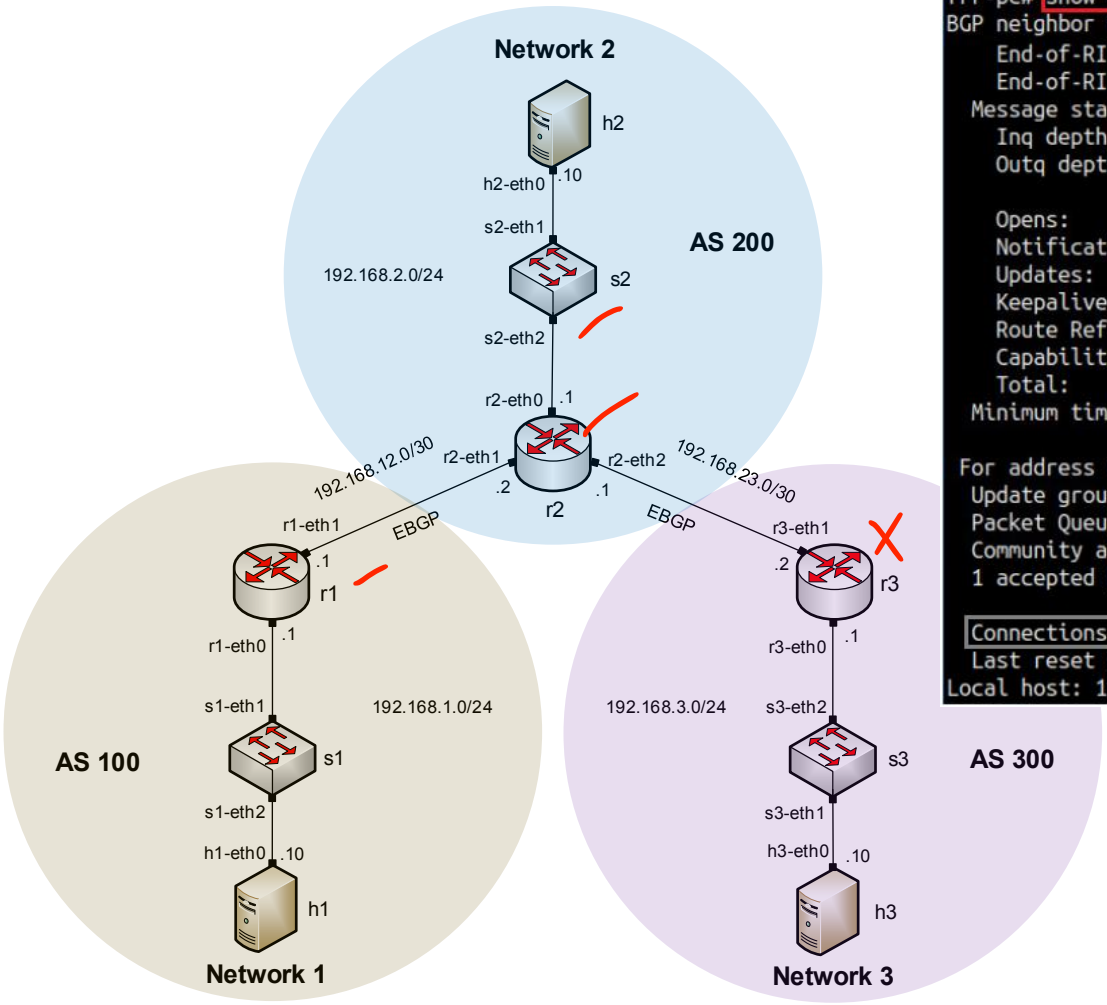








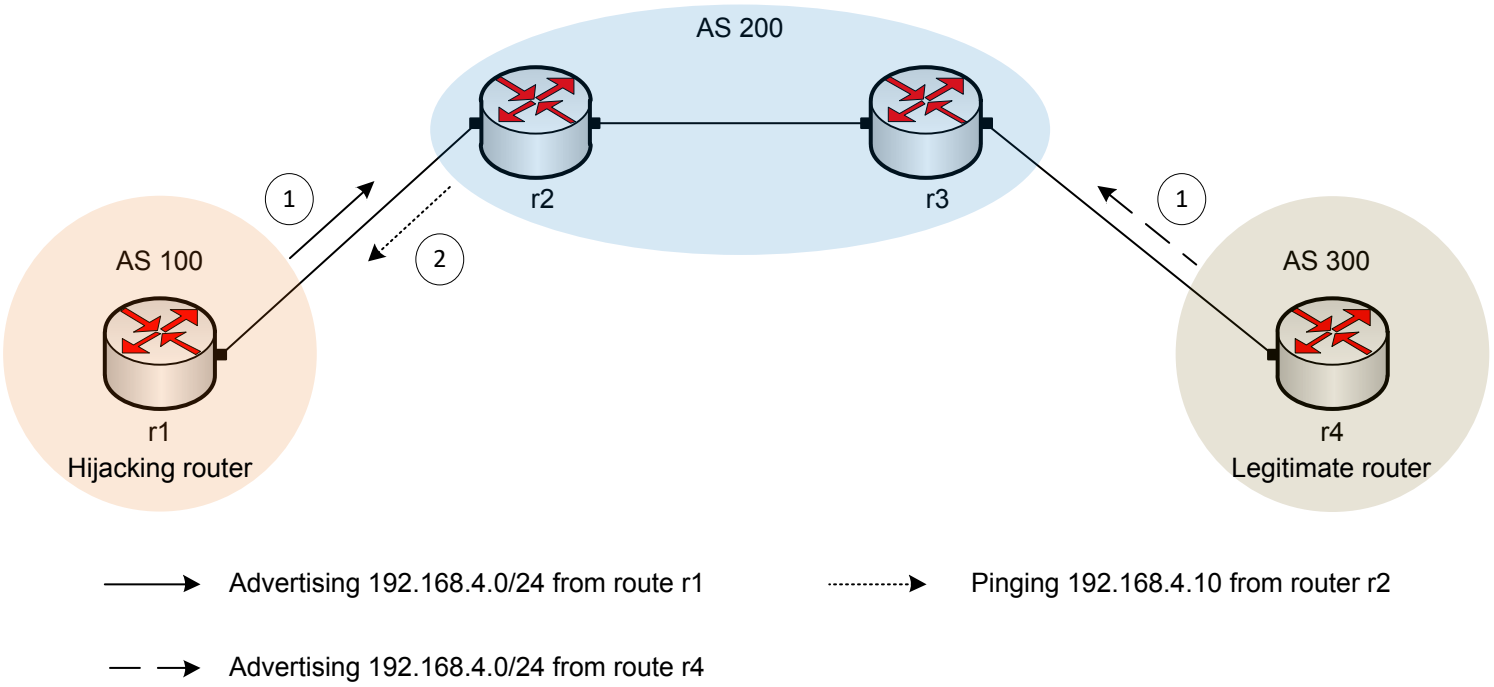
Verify MD5 authentication




```
"Host: r2"
frr-pc# show ip bgp neighbors
BGP neighbor is 192.168.12.1, remote AS 100, local AS 200, external link
    End-of-RIB send: IPv4 Unicast
    End-of-RIB received: IPv4 Unicast
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  2          2
    Notifications:          0          2
    Updates:                9          9
    Keepalives:            49         49
    Route Refresh:          0          0
    Capability:             0          0
    Total:                 60         62
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  1 accepted prefixes

  Connections established 2; dropped 1
  Last reset 00:28:03,   No AFI/SAFI activated for peer
Local host: 192.168.12.2, Local port: 179
```

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



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/

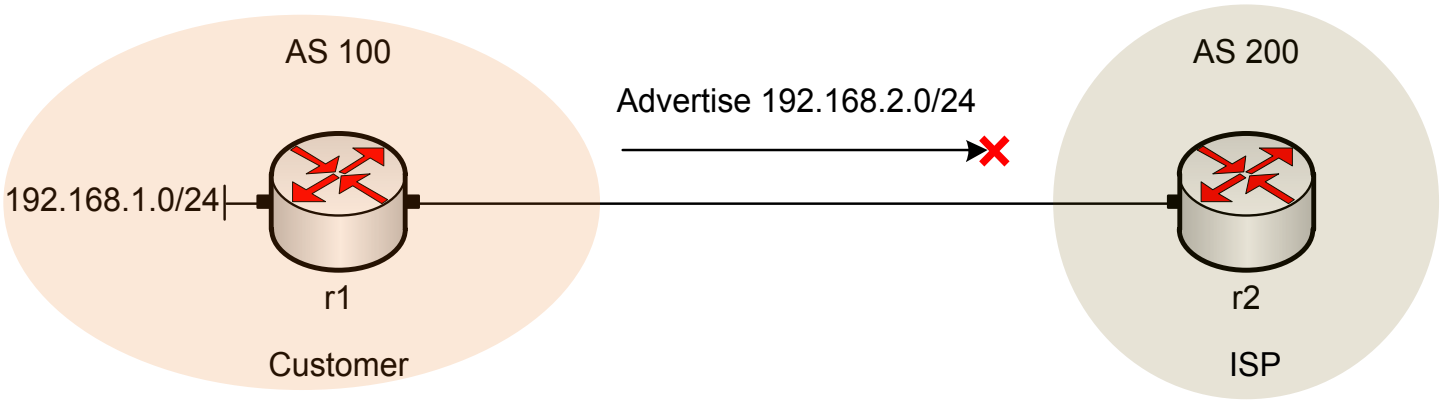
[2] Nichols Shaun, “AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet”,

[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/

Using IP Prefix Filters to Mitigate BGP Hijacking

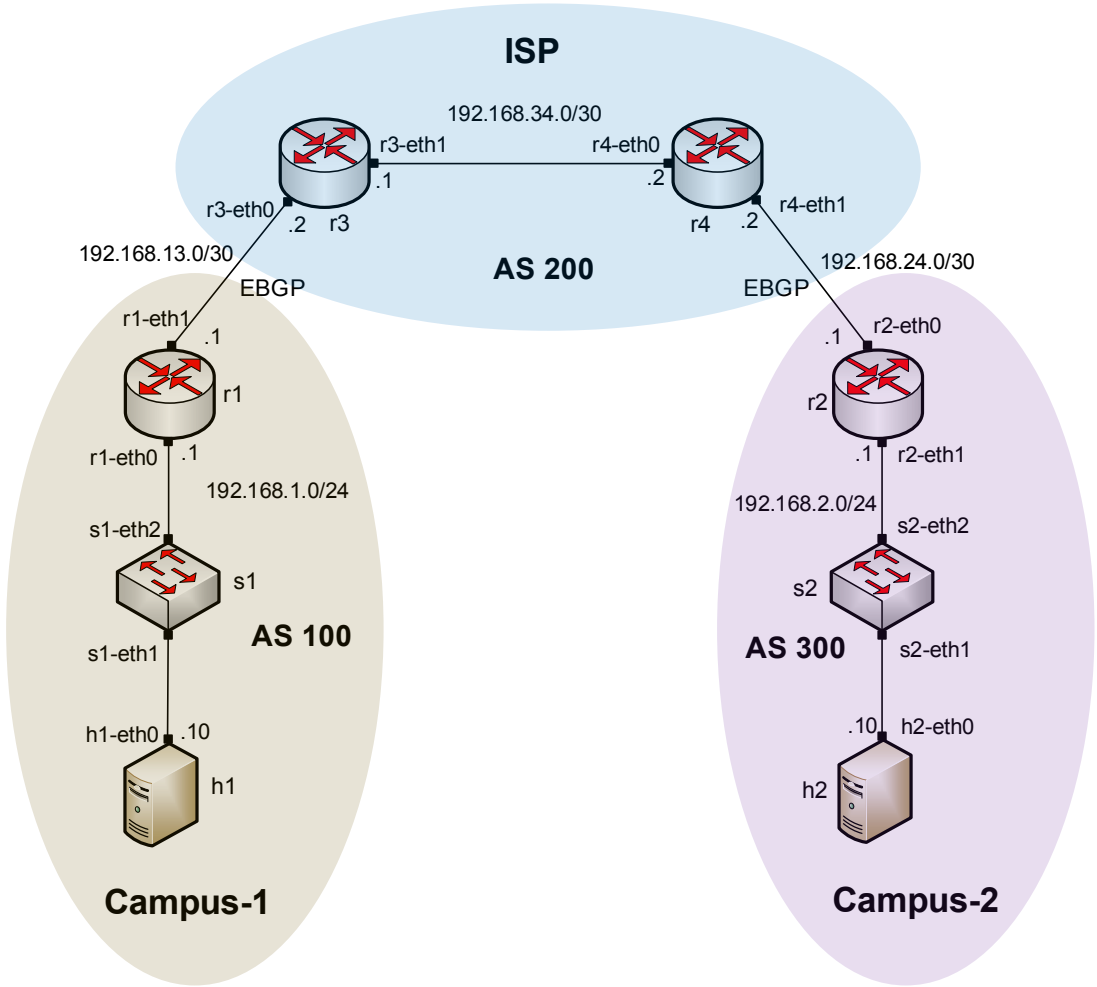
- A router can limit the number of BGP route advertisements by configuring IP prefix filters
- "Most important is to secure the inbound routing advertisements, particularly from customer networks, through the use of explicit prefix-level filters…"[1]



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

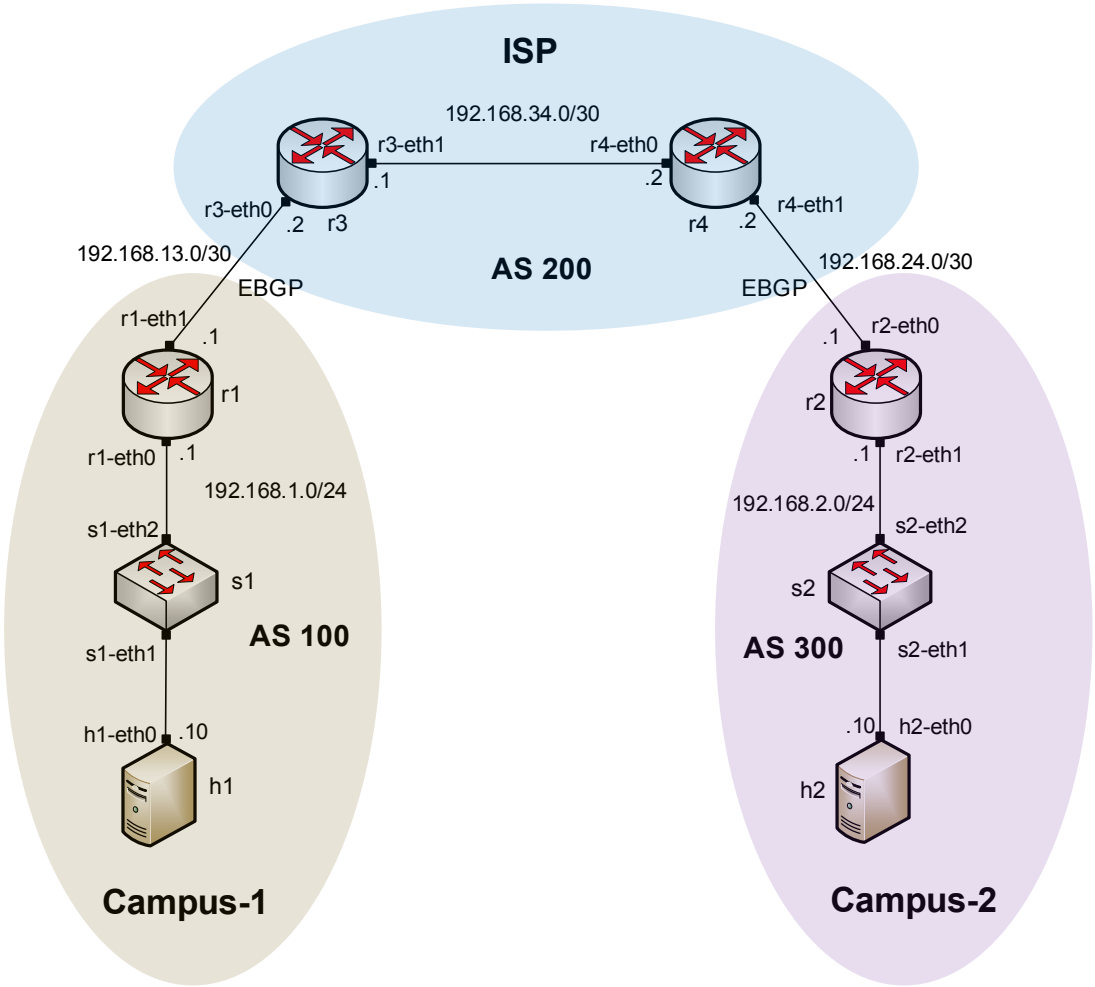
Lab 13 Topology

- Campus-1 hijacks Campus-2's prefixes



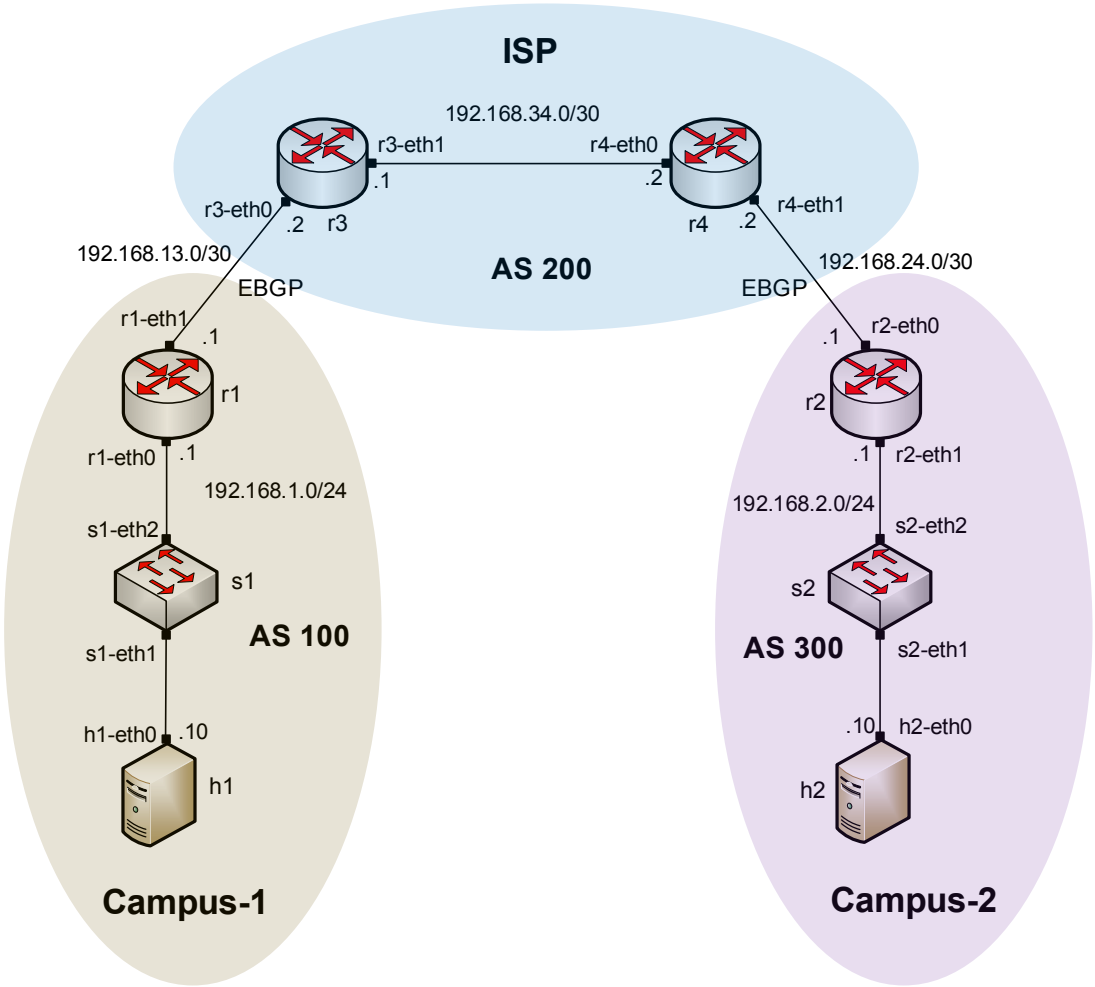
Lab 13 Topology

- Traffic to Campus-2 is redirected to Campus-1



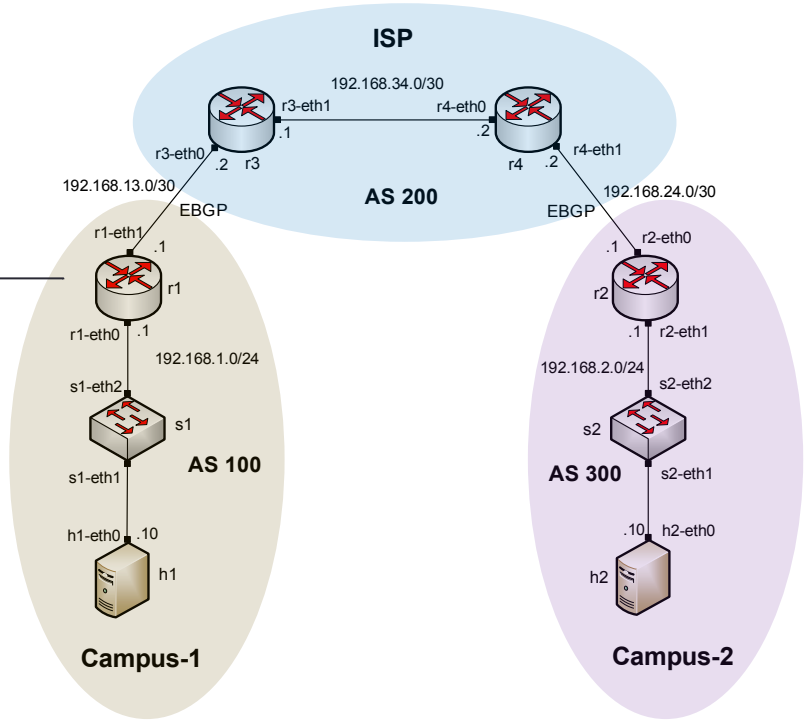
Lab 13 Topology

- The ISP configures IP prefix lists on both campuses to prevent BGP hijacking

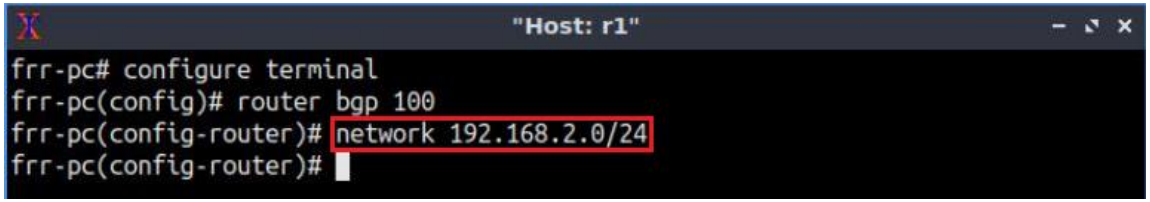


Lab 13 Configuration

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



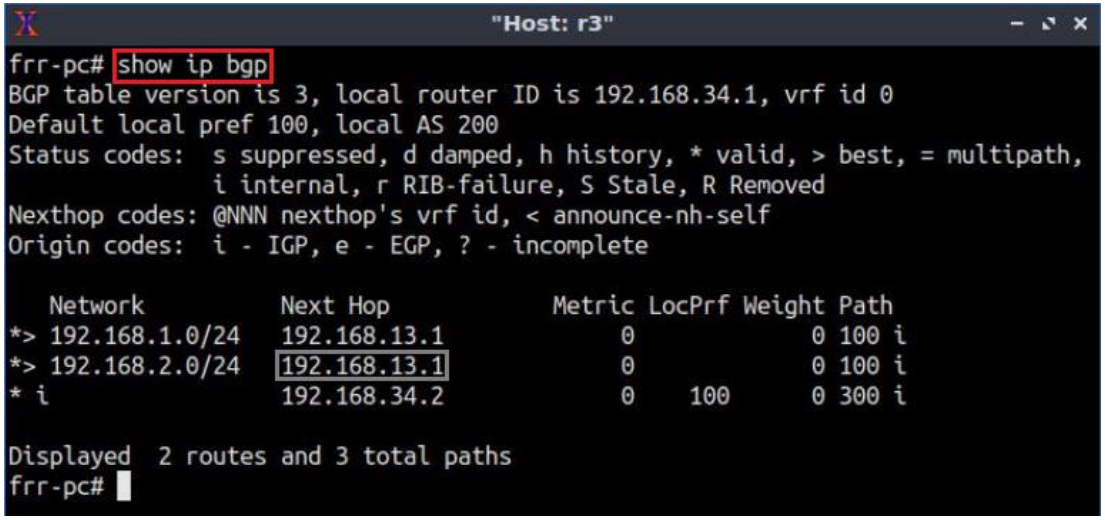
Router r1

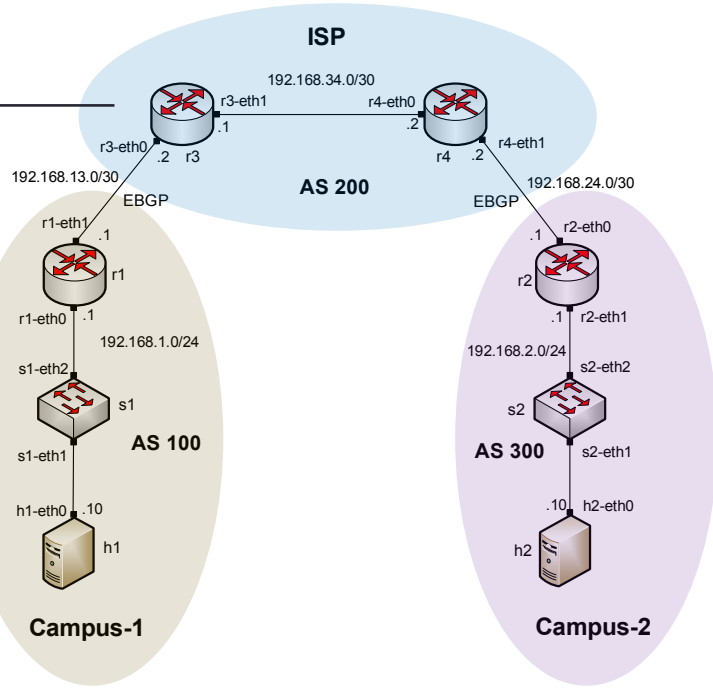


Lab 13 Configuration

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

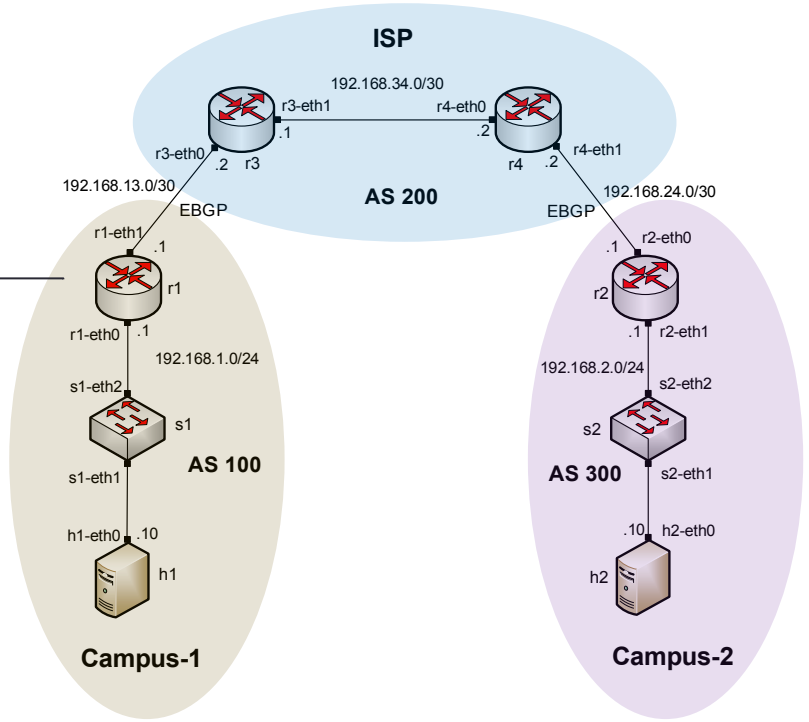
Router r3



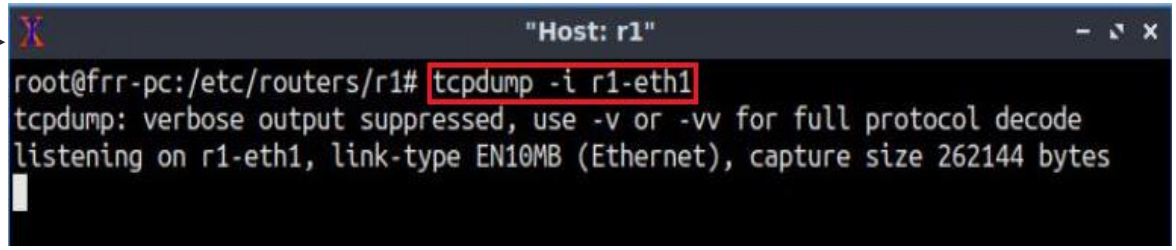


Lab 13 Configuration

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



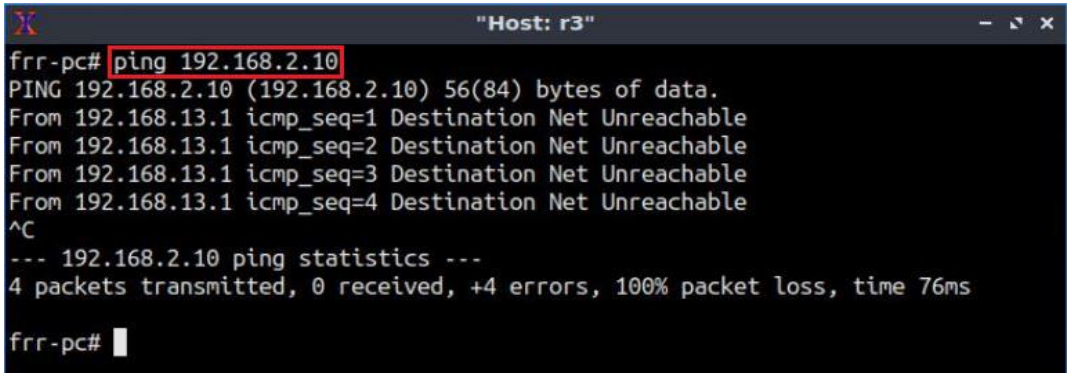
Router r1

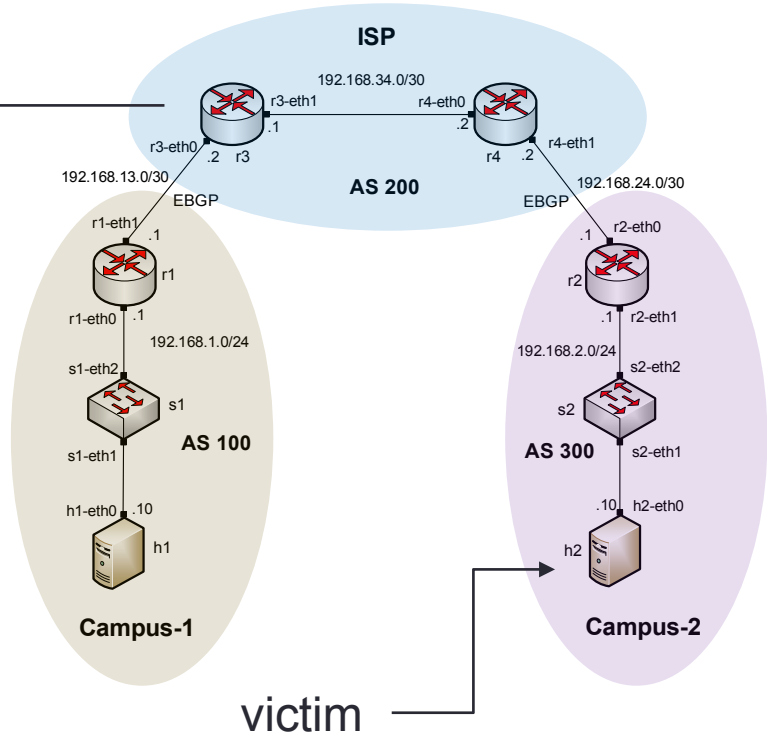


Lab 13 Configuration

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

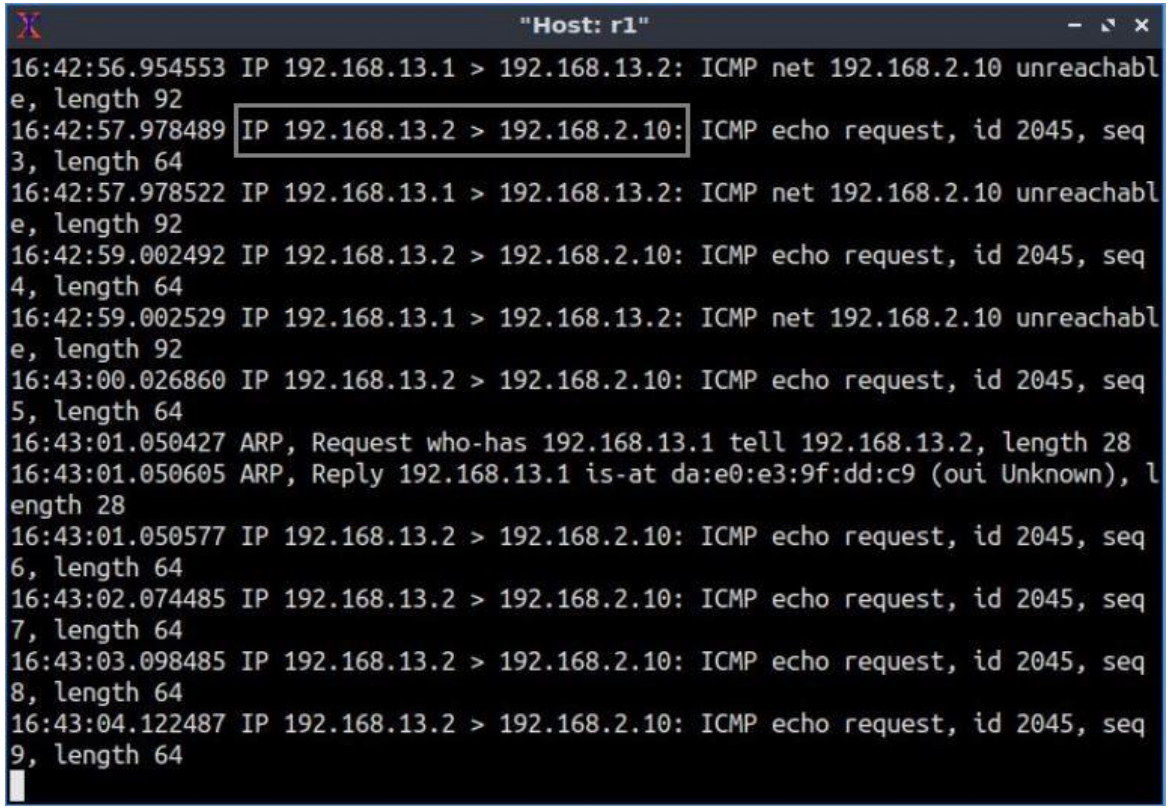
Router r3





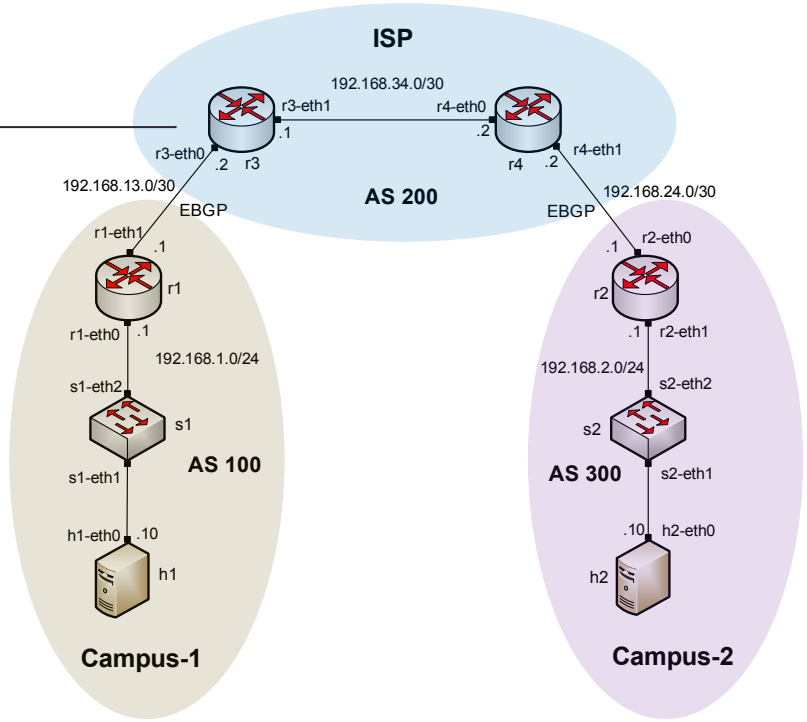
Lab 13 Configuration

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

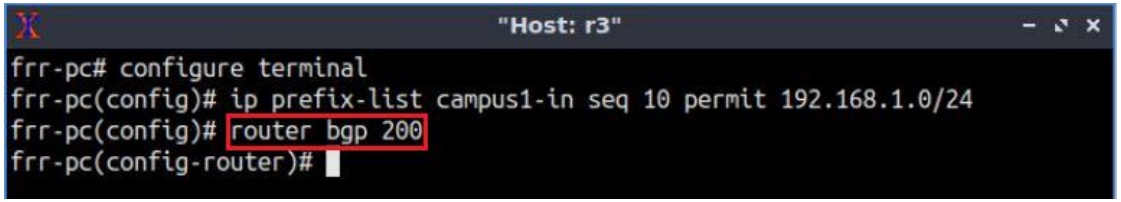


Lab 13 Configuration

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

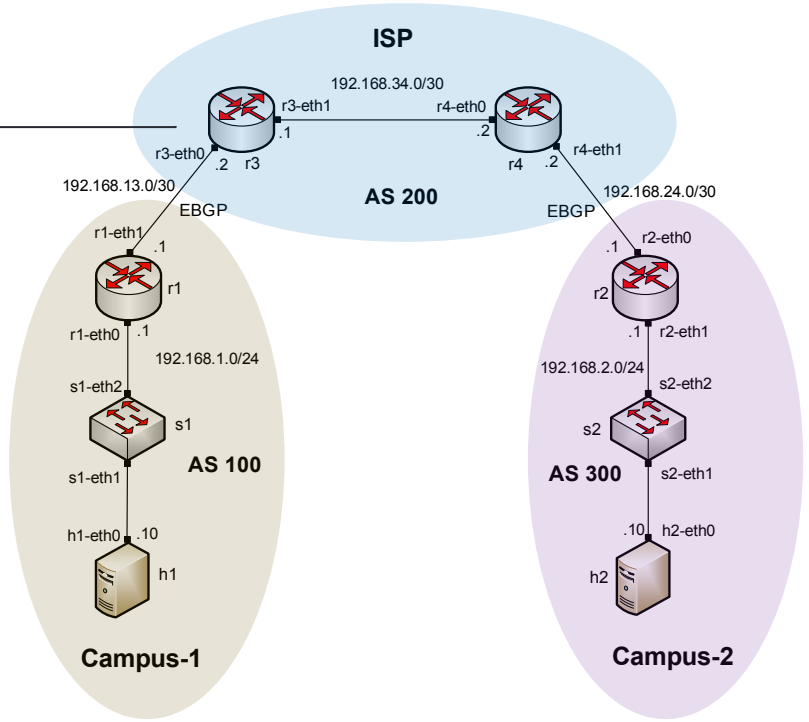


Router r3

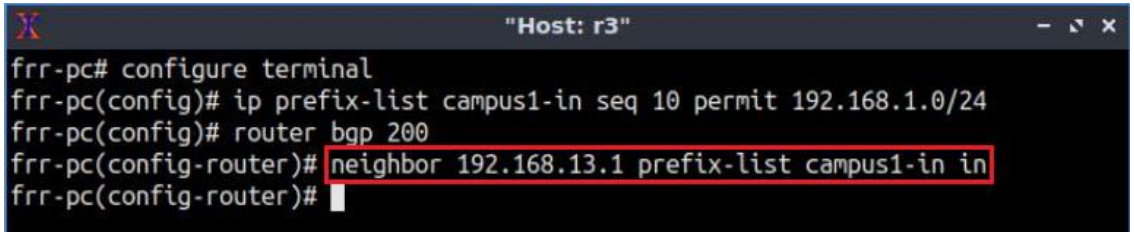


Lab 13 Configuration

- Apply the prefix list to router r3 neighbor



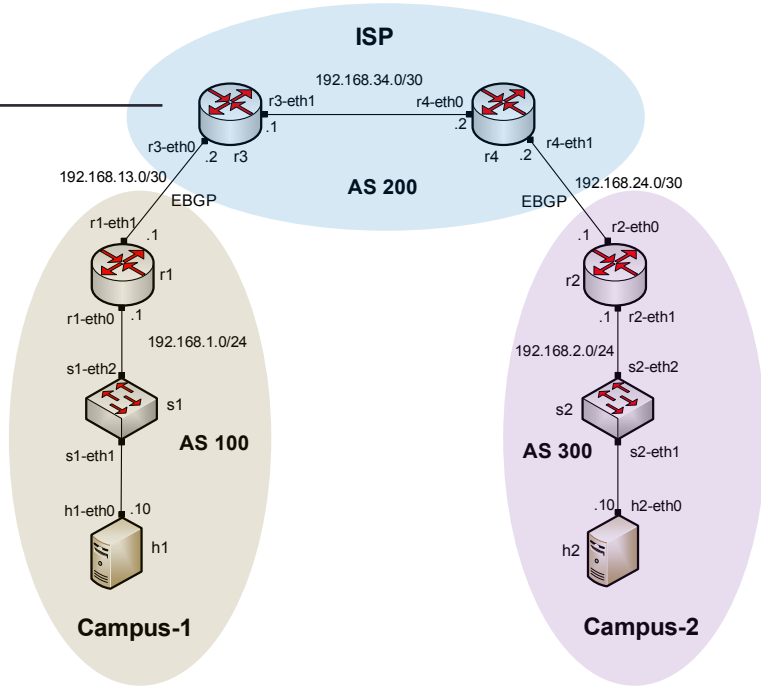
Router r3



Lab 13 Configuration

- Router r3 readjusts its BGP table back to normal

Router r3

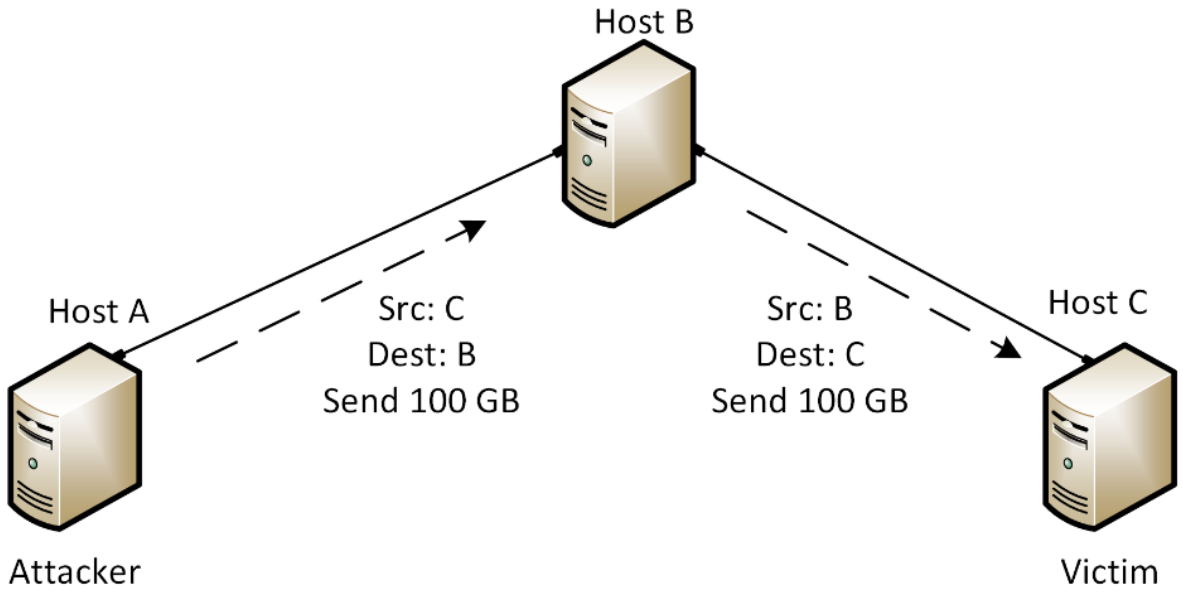


"Host: r3"

```
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#
```

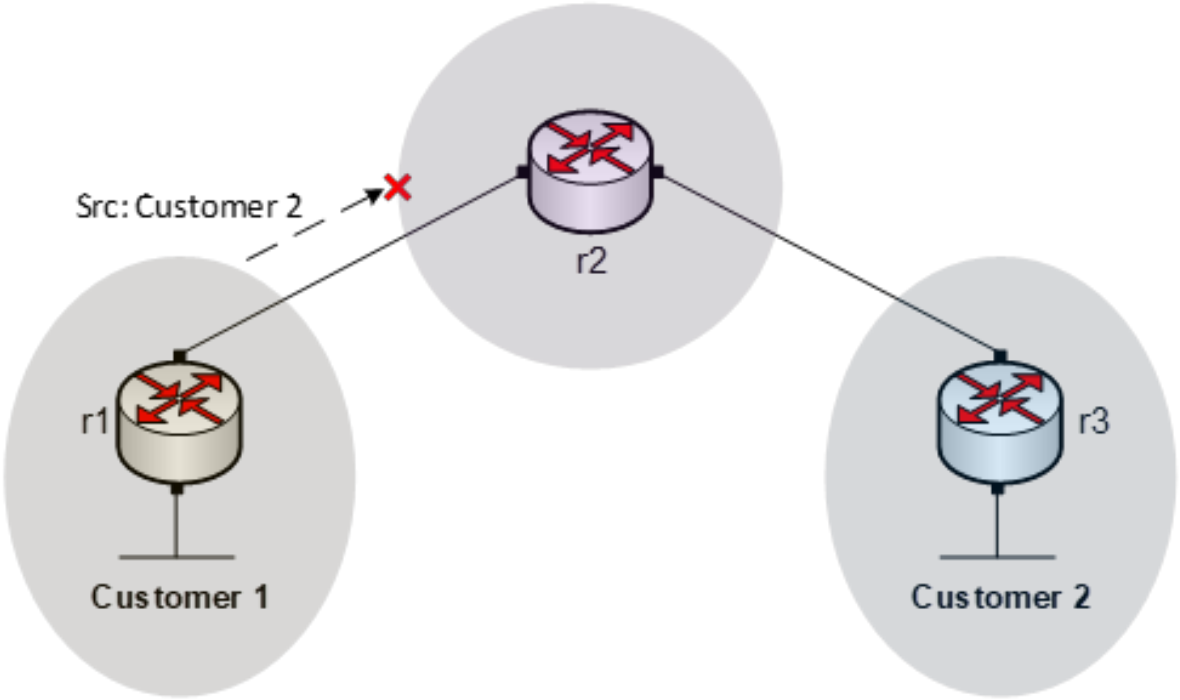
What is IP Spoofing?

- It is the process of originating IP packets with source addresses other than those assigned to the origin host.
- IP spoofing can be exploited in several ways, mainly to launch Denial of Service (DoS) attacks.



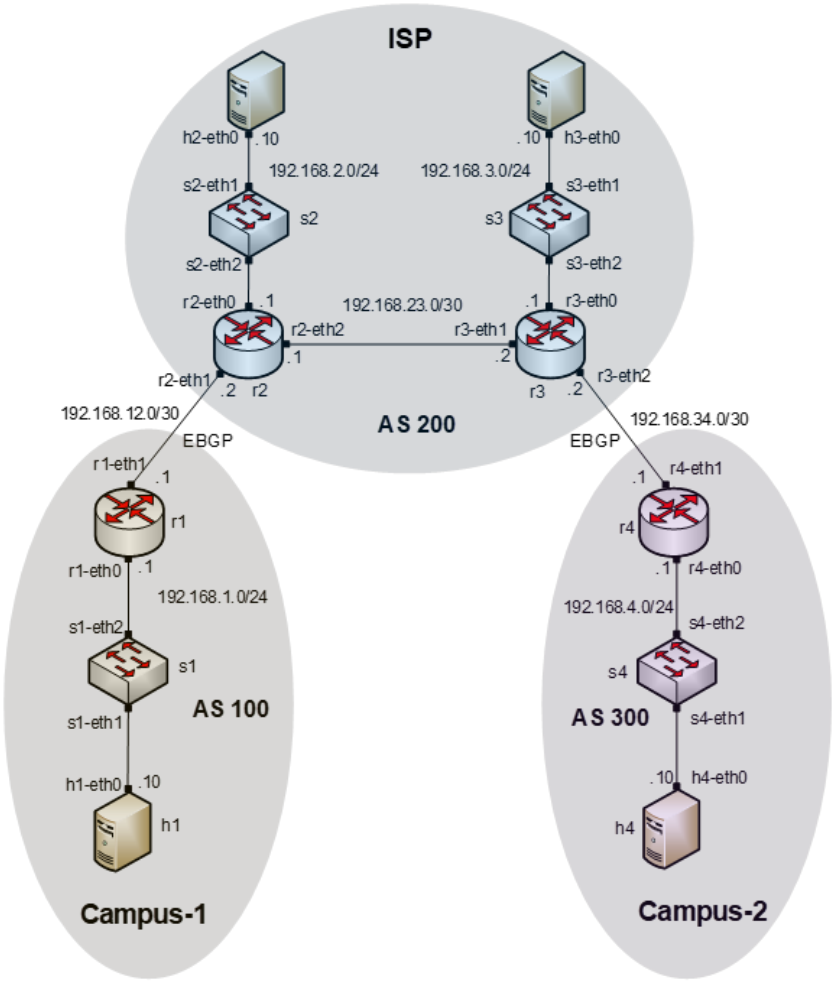
Anti-Spoofing Techniques – Route Filtering

- Route filtering is a method for selectively identifying routes that are advertised or received from neighbor routers.
- It can be used to manipulate traffic flows, reduce memory utilization, or to improve security



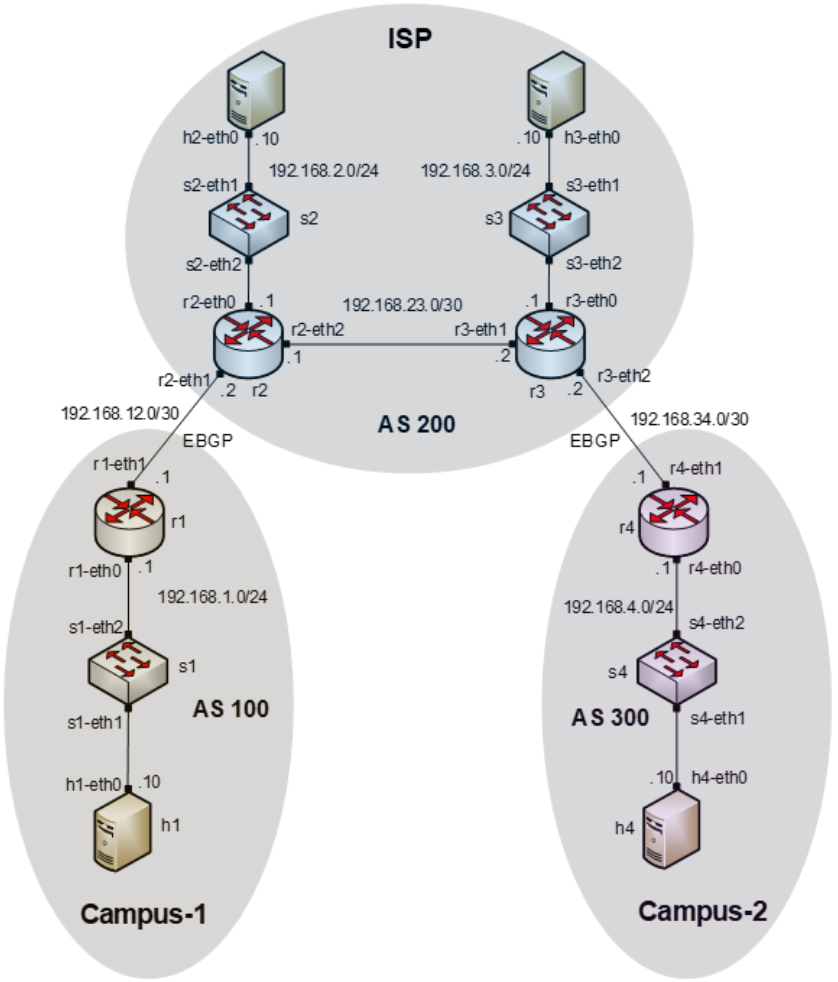
Lab 12 Topology

- Host h1 in Campus-1 spoofs the IP address of host h4 in Campus-2 and launches DoS attack.



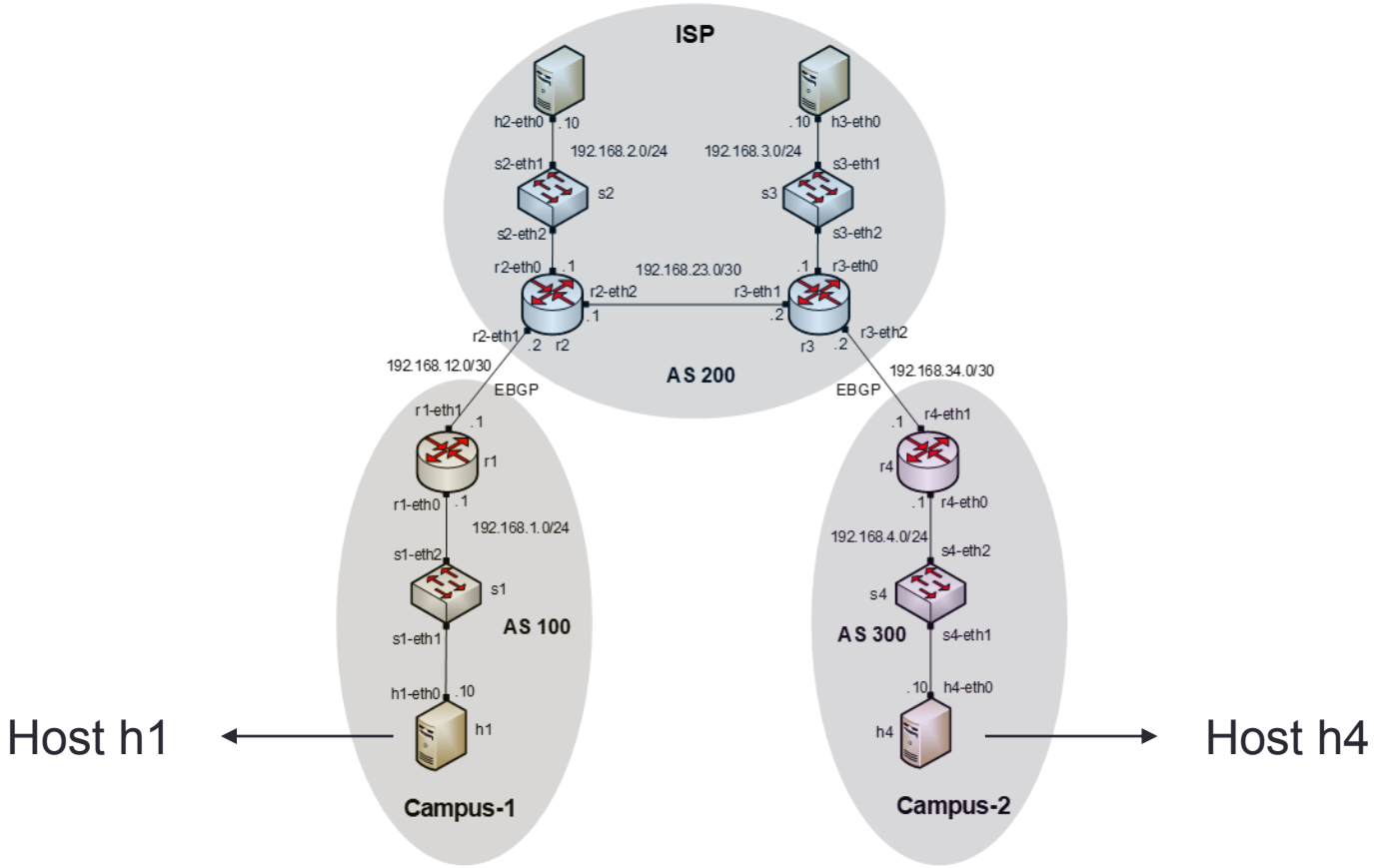
Lab 12 Topology

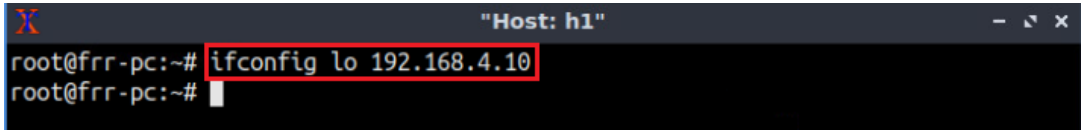
- The Internet Service Provider (ISP) applies the appropriate route filters to prevent IP spoofing



Lab 12 Configuration

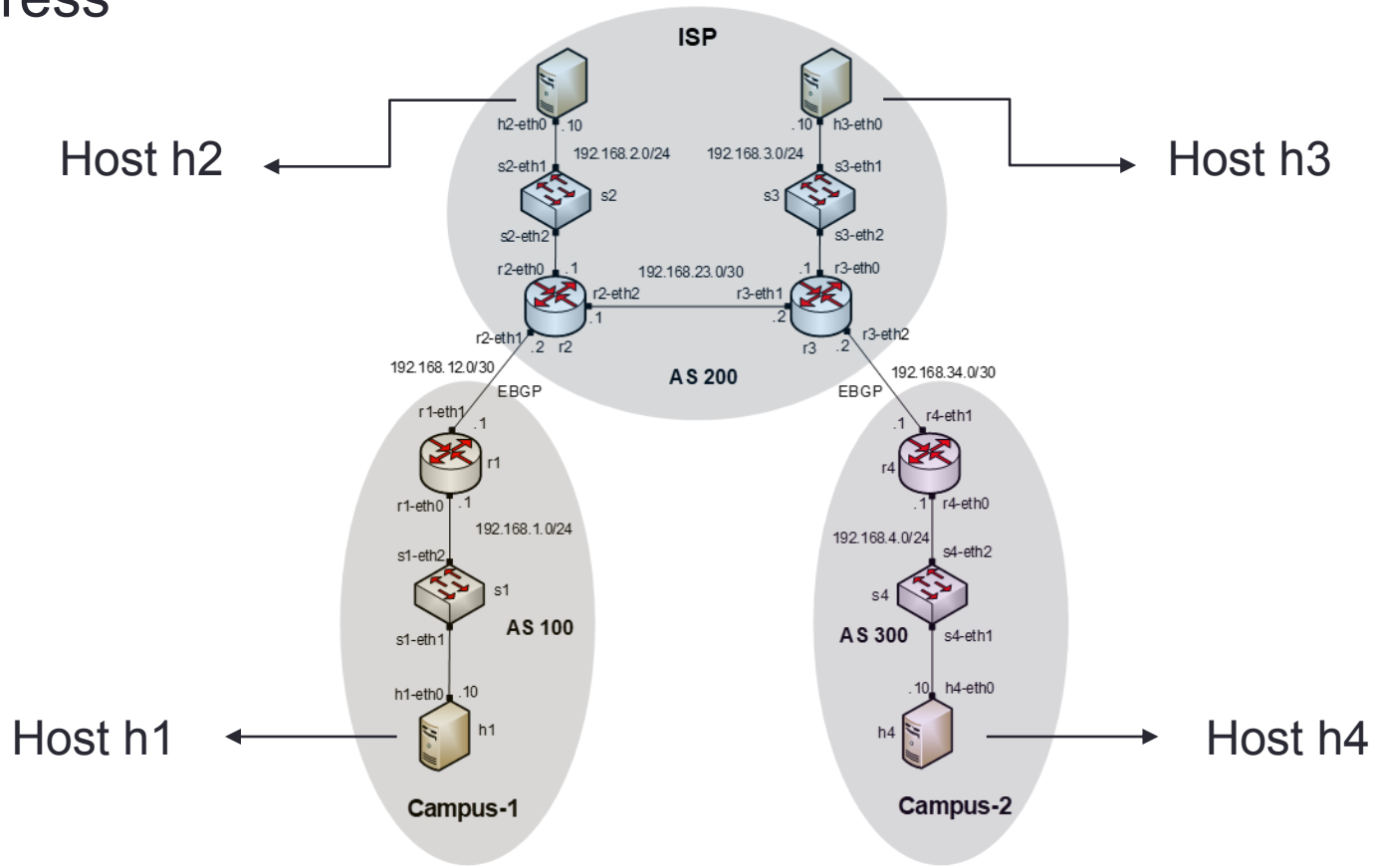
- Host h1 spoofs the IP address of host h4





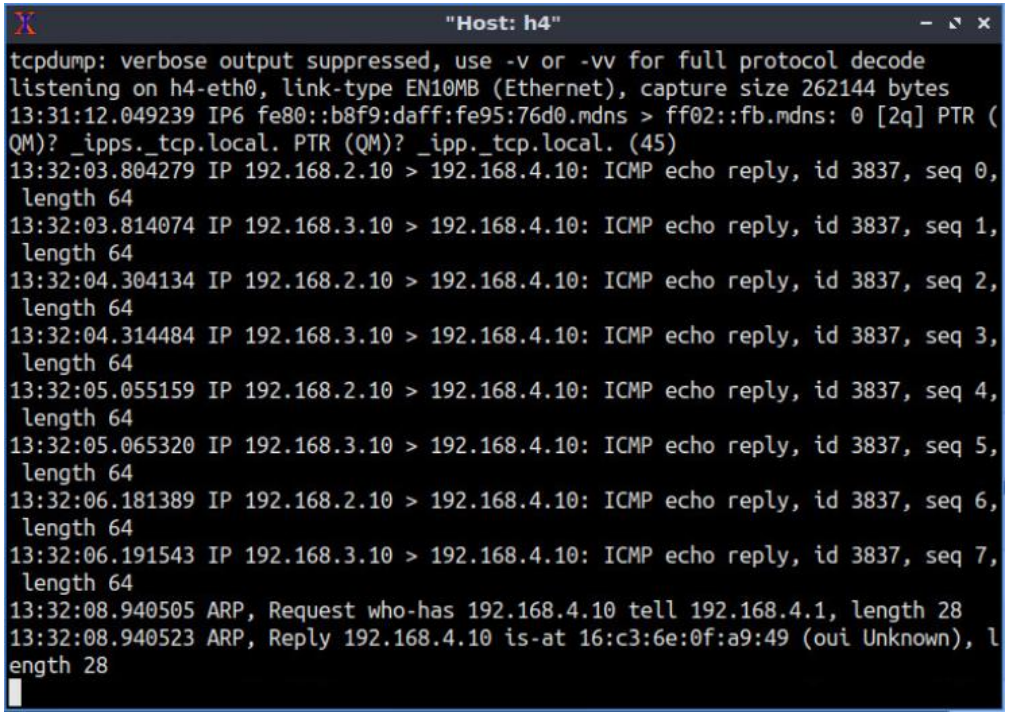
Lab 12 Configuration

- Host h1 pings hosts h2 and h3 using the spoofed source IP address



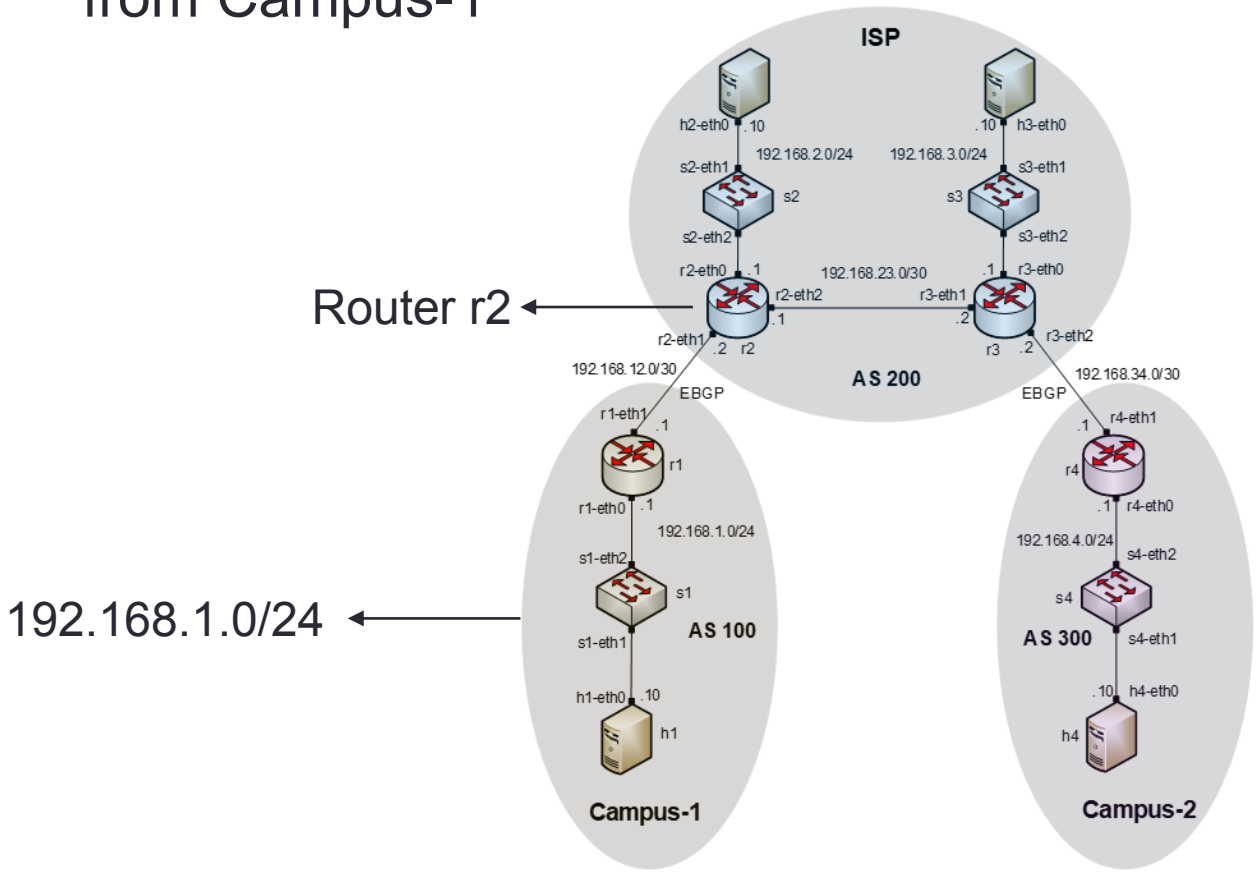
Lab 12 Configuration

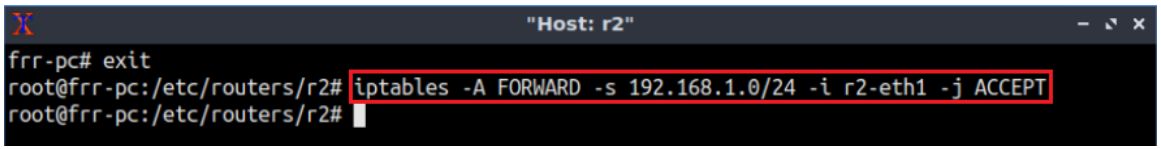
- Host h4 receives a reply messages from 192.168.2.10 and 192.168.3.10



Lab 12 Configuration

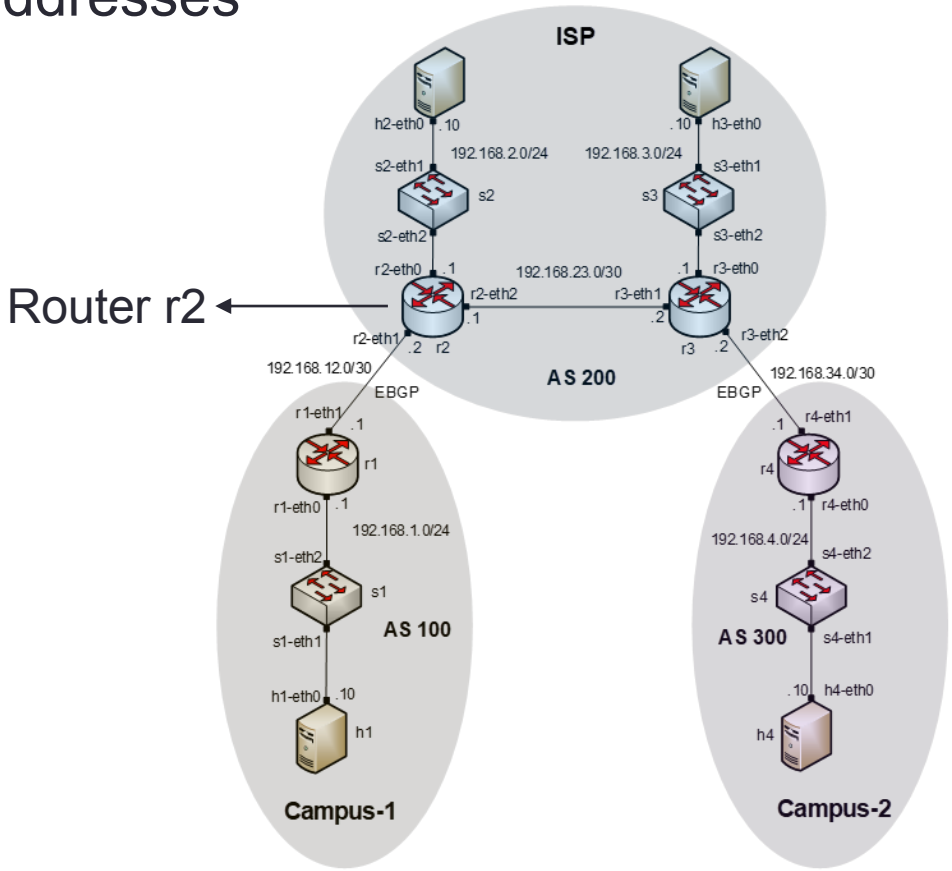
- Apply a filter on router r2 to accept IP source 192.168.1.0/24 from Campus-1

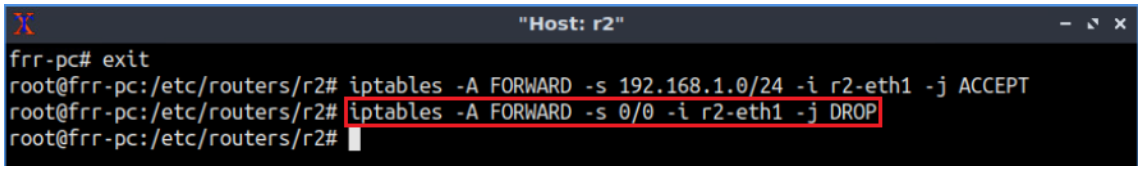




Lab 12 Configuration

- Apply another route filter on router r2 to reject all other IP source addresses





Lab 12 Configuration

- Perform DoS attack by host h1 on host h4

- Capture the network traffic on host h4