"HANDS-ON SESSION BORDER GATEWAY PROTOCOL"

Ali AlSabeh, J. Crichigno
Department of Integrated Information Technology
University of South Carolina

NSF Award 1829698
"CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers"

LAB SERIES:
BORDER GATEWAY PROTOCOL

Lab Series: Border Gateway Protocol

- Lab 1: Introduction to Mininet
- Lab 2: Introduction to Free Range Routing (FRR)
- Lab 3: Introduction to BGP
- Lab 4: Configure and verify EBGP
- Lab 5: BGP Authentication
- Lab 6: Configure BGP with Default Route
- Lab 7: Using AS_PATH BGP Attribute
- Lab 8: Configuring IBGP and EBGP Sessions, Local Preference, and MED
- Lab 9: IBGP, Next Hop and Full Mesh Topology
- Lab 10: BGP Route Reflection
- Lab 11: Configuring Multiprotocol BGP
- **Lab 12: IP Spoofing and Mitigation Techniques**
- **Lab 13: BGP Hijacking**

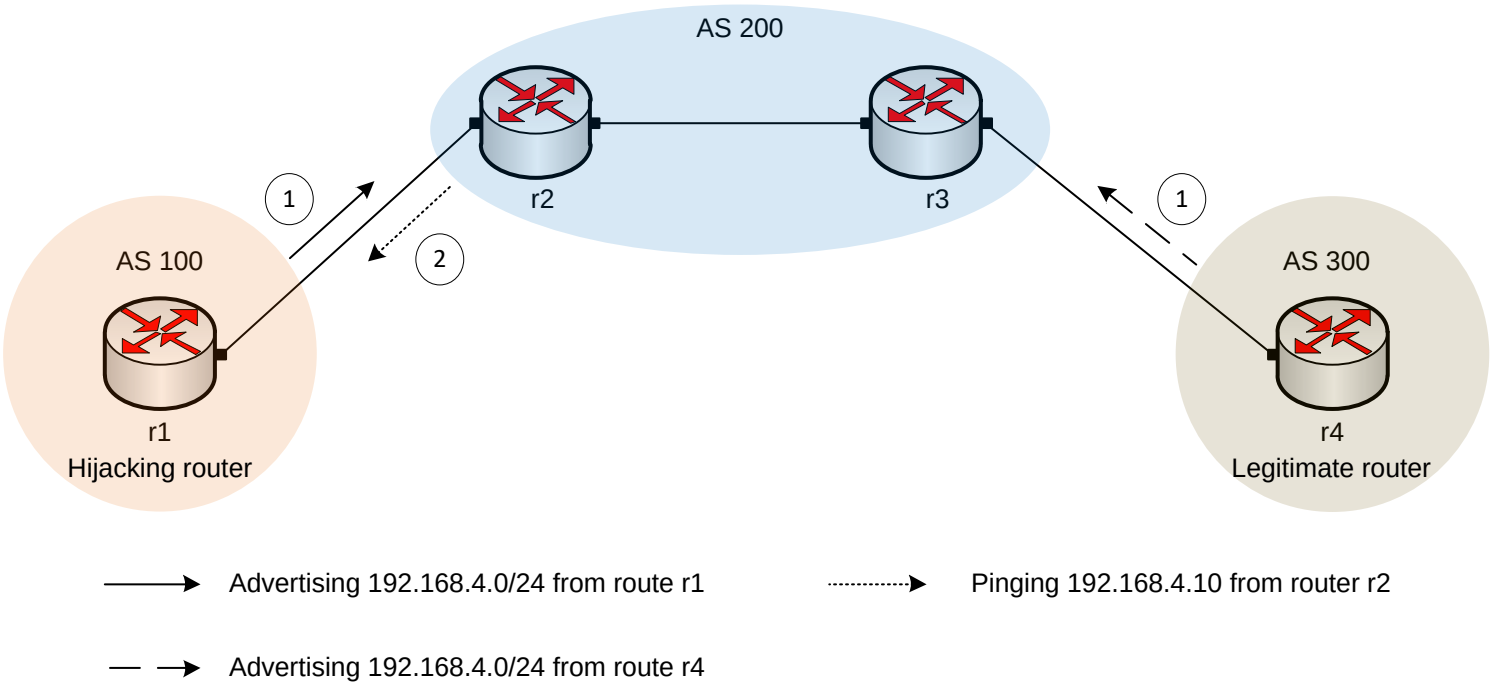
Organization of Lab Manuals

- Each lab starts with a section *Overview*
  - Objectives
  - Lab settings: passwords, device names
  - Roadmap: organization of the lab
- *Section 1*
  - Background information of the topic being covered (e.g., BGP hijacking)
  - Section 1 is optional (i.e., the reader can skip this section and move to lab directions)
- *Section 2… n*
  - Step-by-step directions

LAB 13: BGP HIJACKING

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/

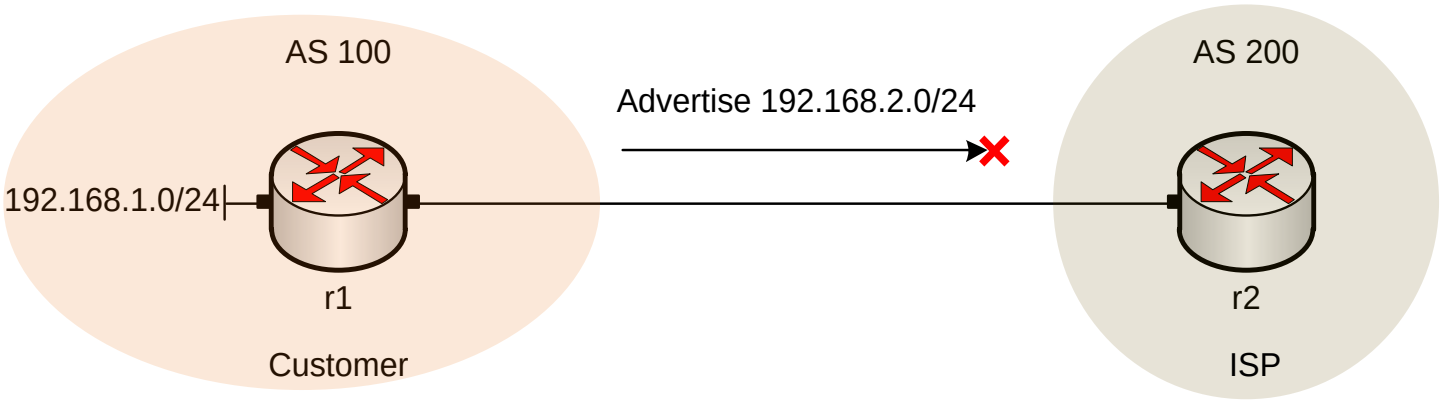
[2] Nichols Shaun, “AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet”,

[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

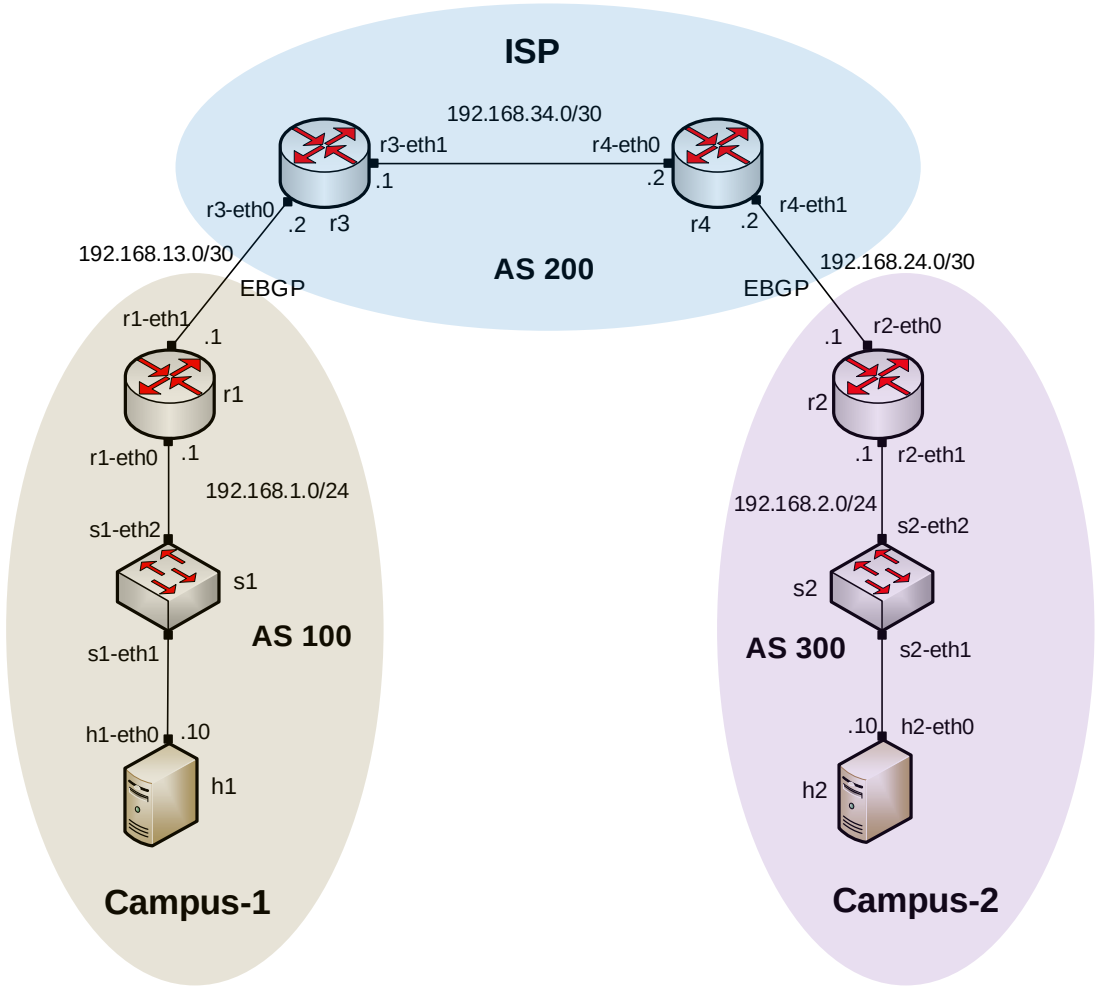
- A router can limit the number of BGP route advertisements by configuring IP prefix filters
- “Most important is to secure the inbound routing advertisements, particularly from customer networks, through the use of explicit prefix-level filters…”[1]



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

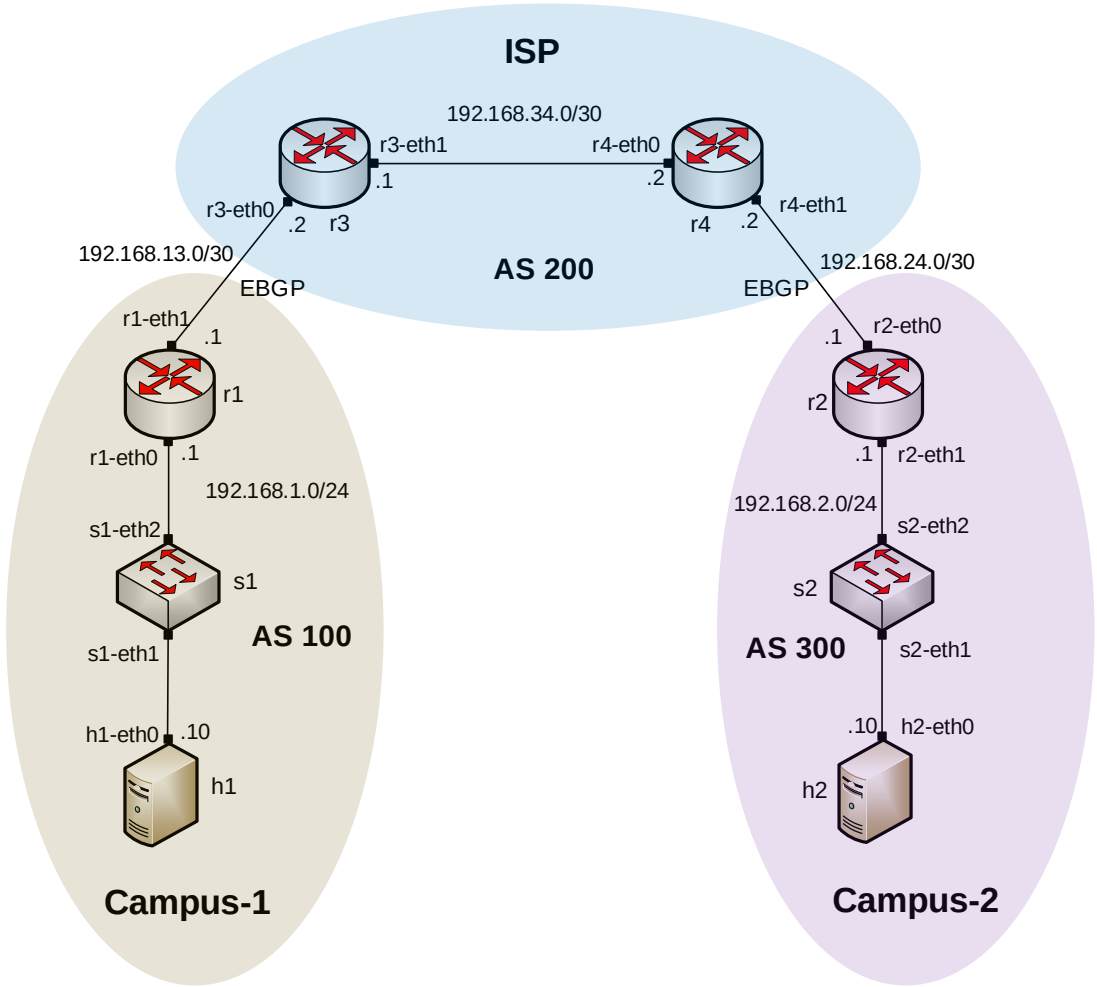
Lab 13 Topology

- Campus-1 hijacks Campus-2's prefixes



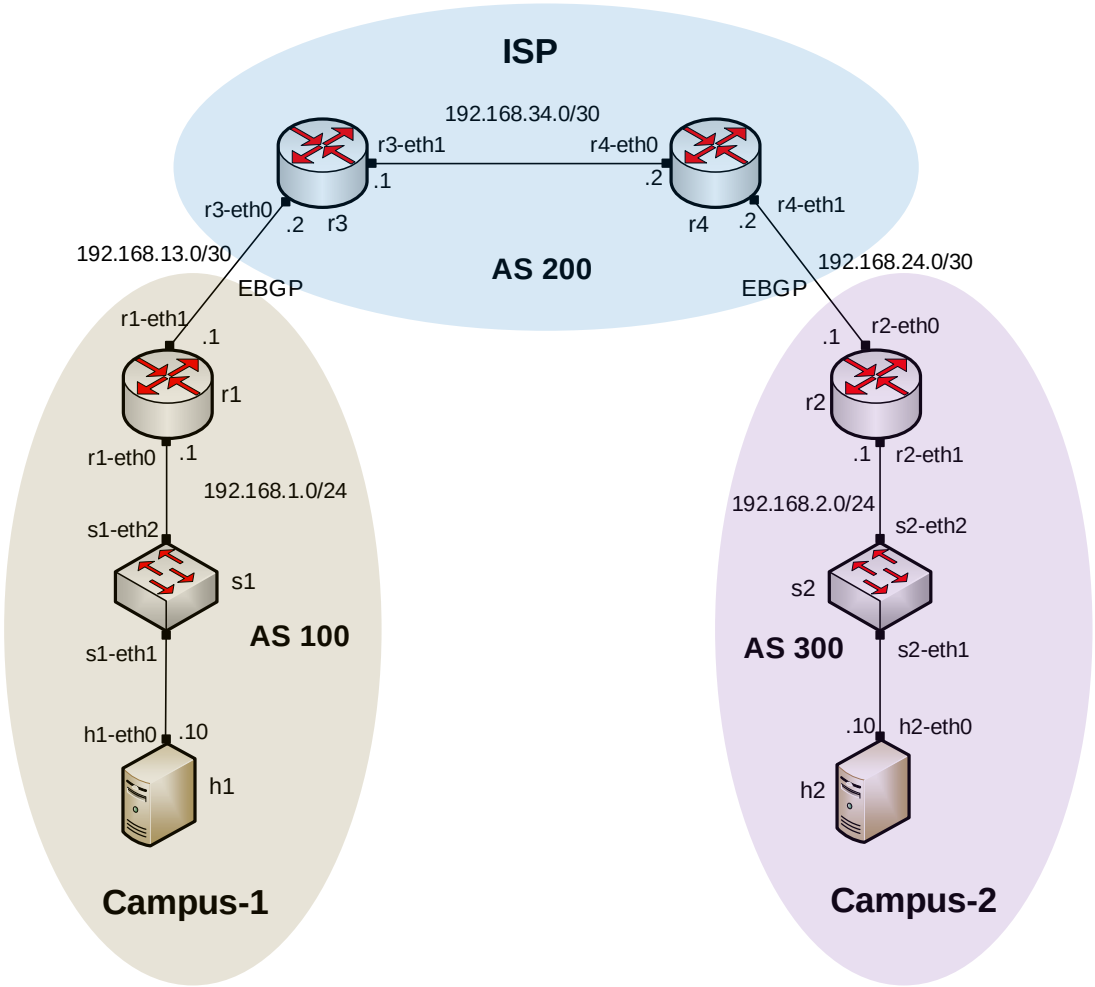
Lab 13 Topology

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



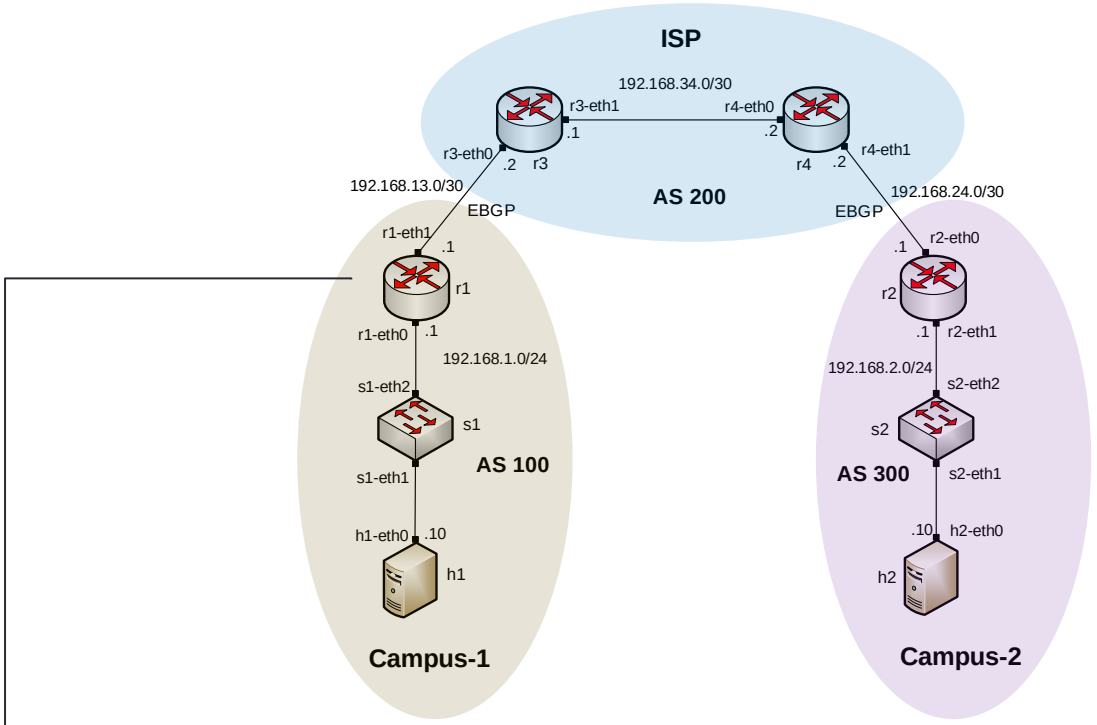
Lab 13 Topology

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

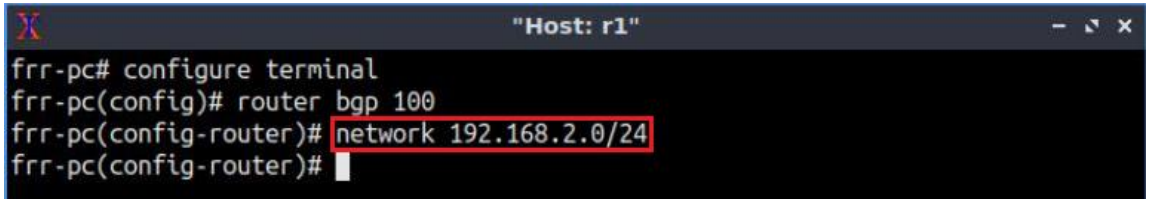


Lab 13 Configuration

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



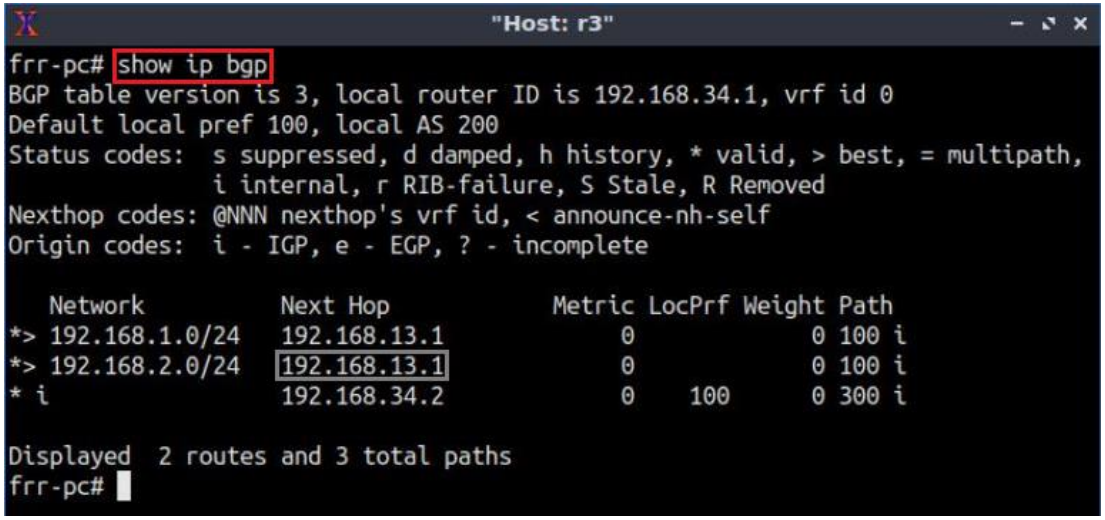
Router r1

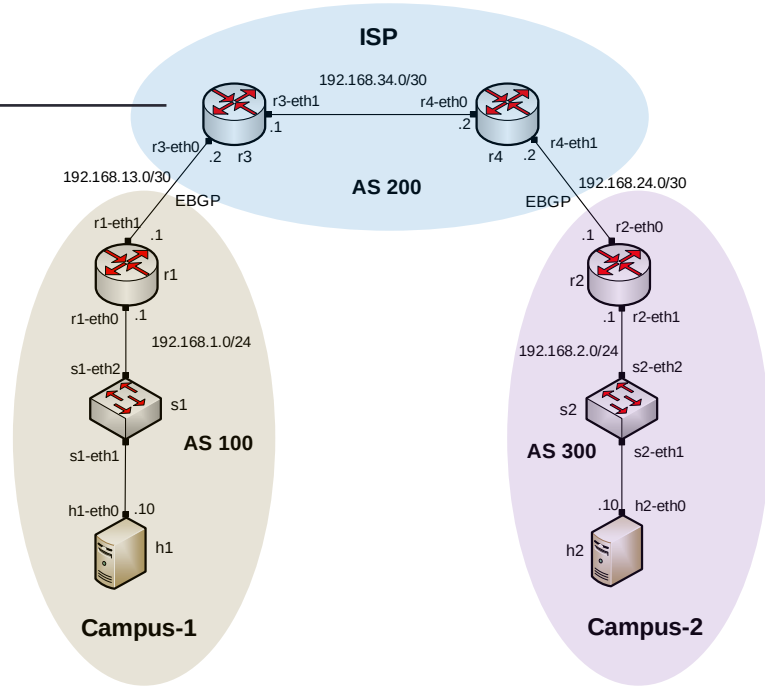


Lab 13 Configuration

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

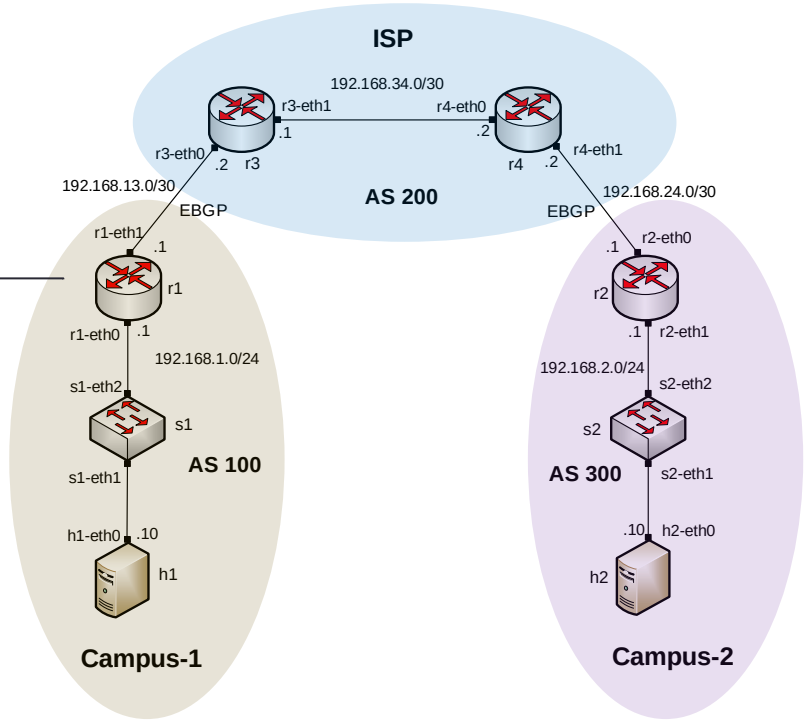
Router r3



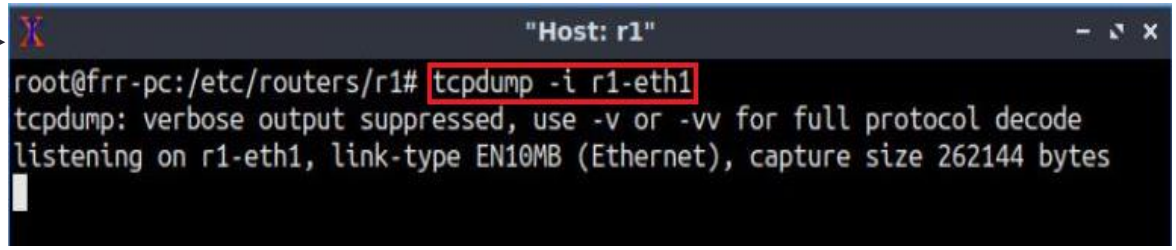


Lab 13 Configuration

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



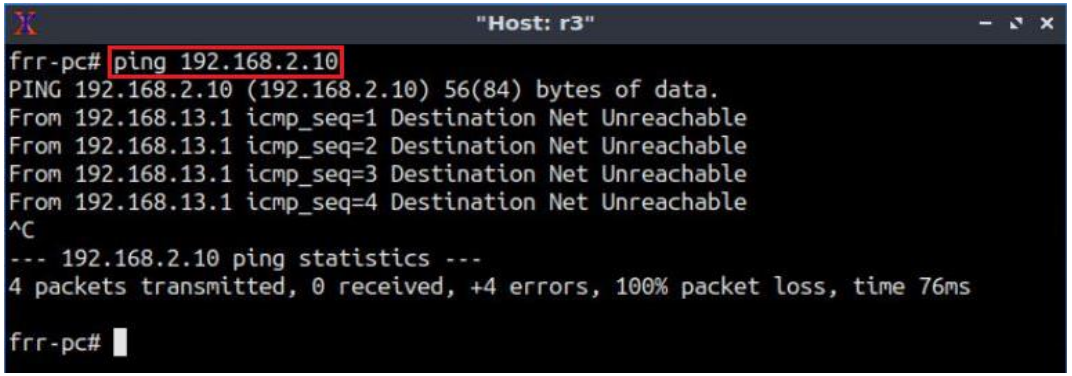
Router r1

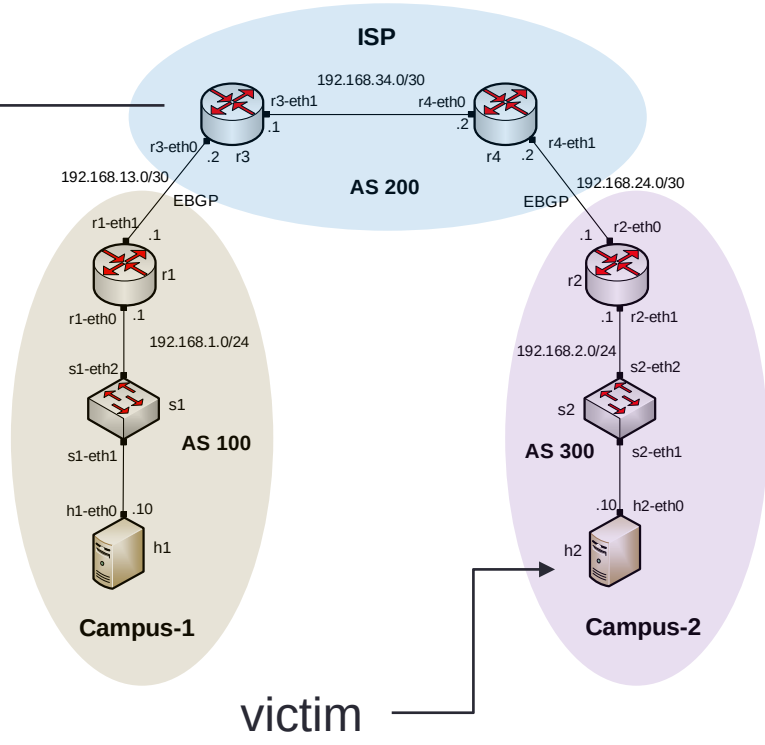


Lab 13 Configuration

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

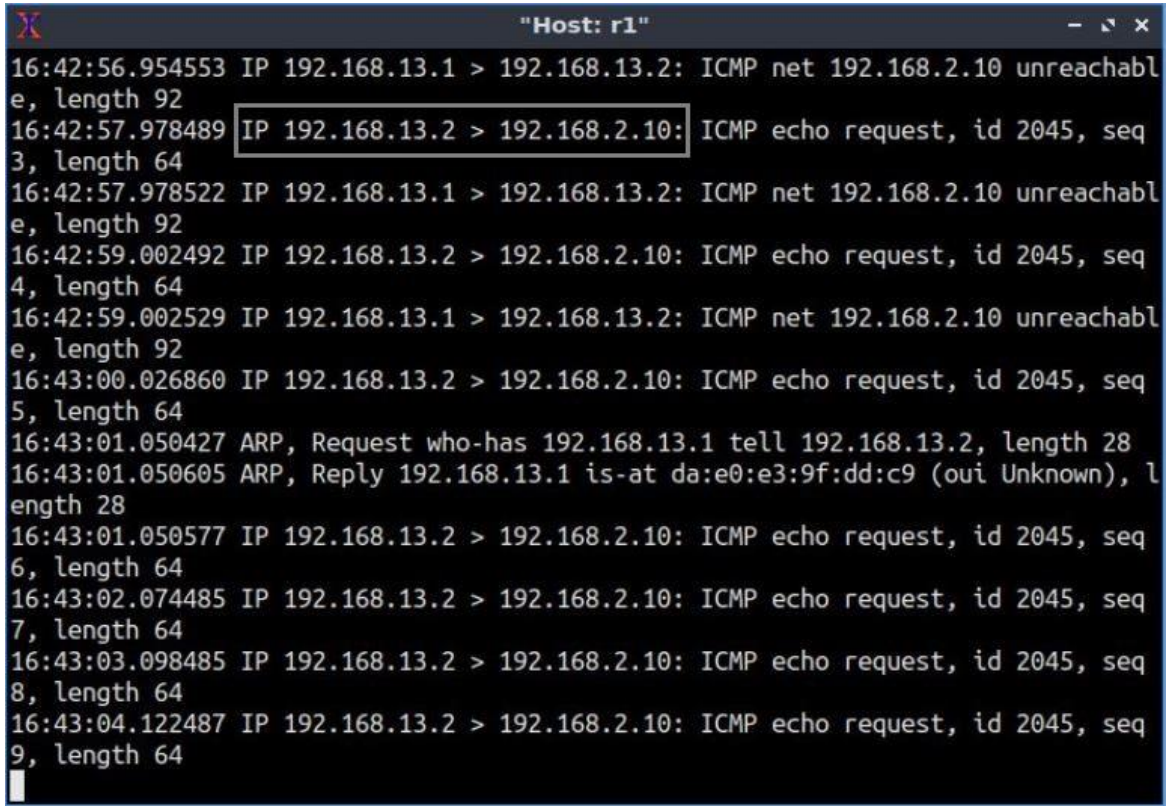
Router r3





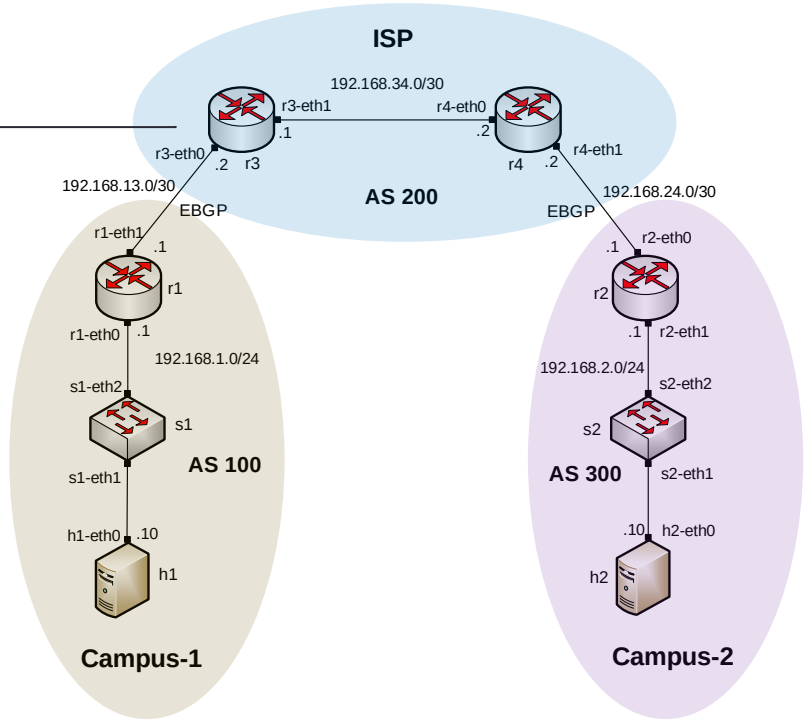
Lab 13 Configuration

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

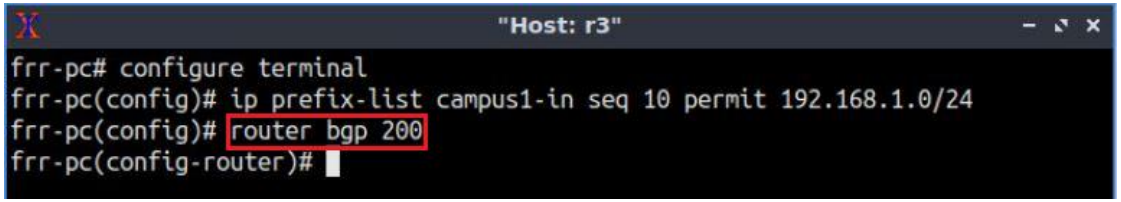


Lab 13 Configuration

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

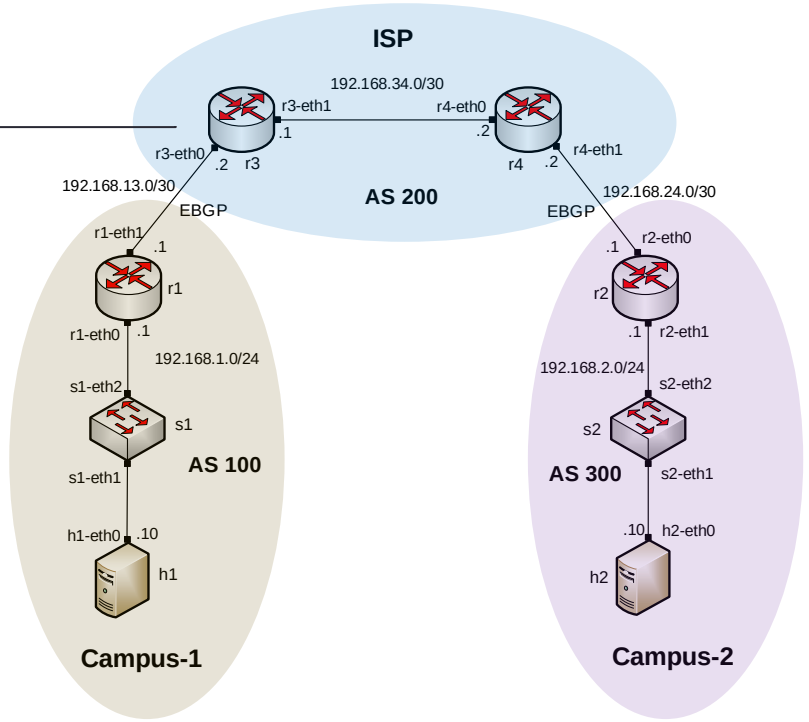


Router r3

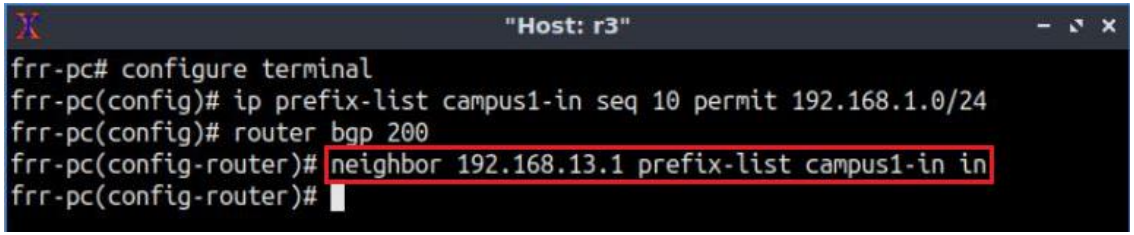


Lab 13 Configuration

- Apply the prefix list to router r3 neighbor



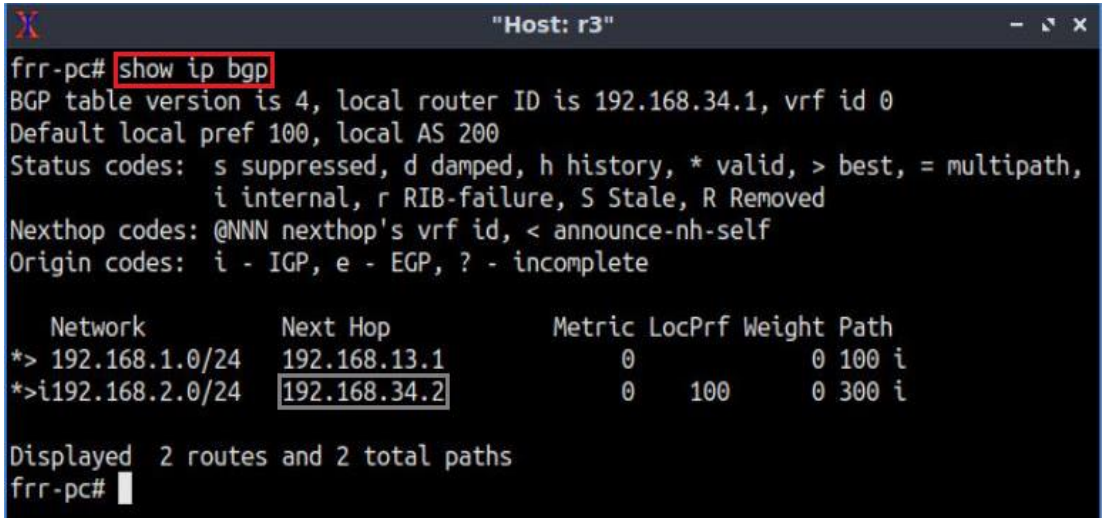
Router r3

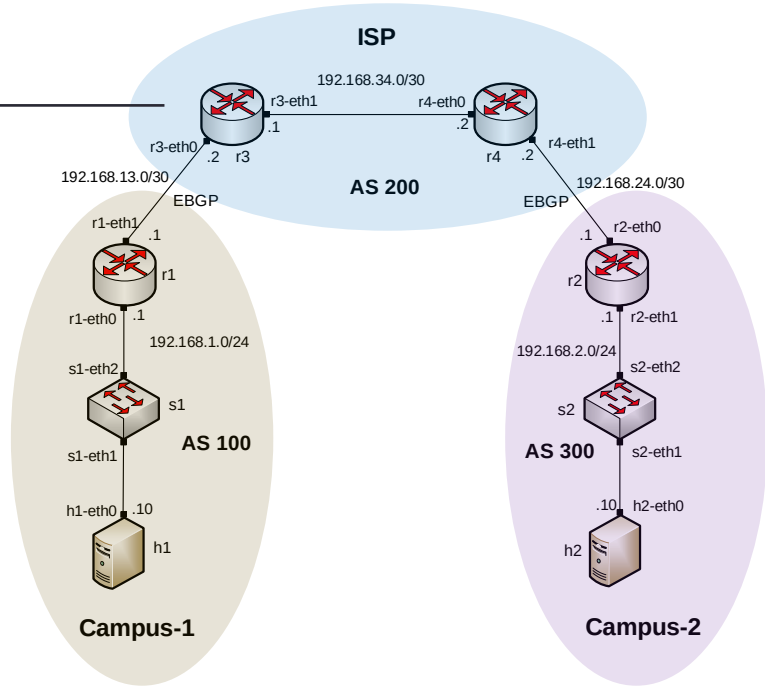


Lab 13 Configuration

- Router r3 readjusts its BGP table back to normal

Router r3

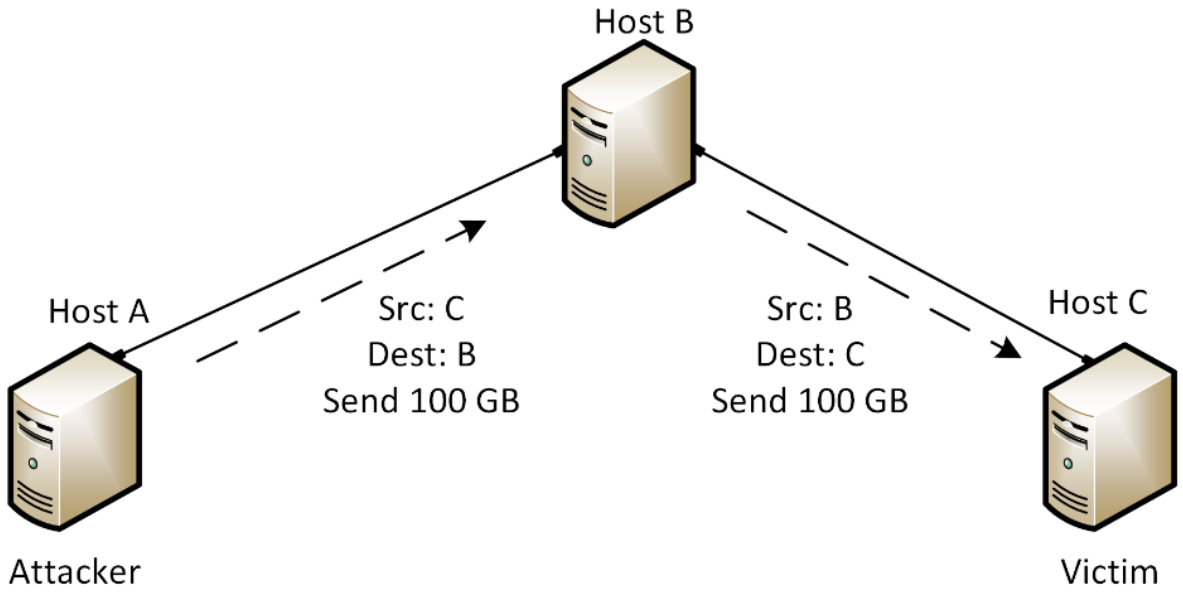




LAB 12: IP SPOOFING AND MITIGATION TECHNIQUES

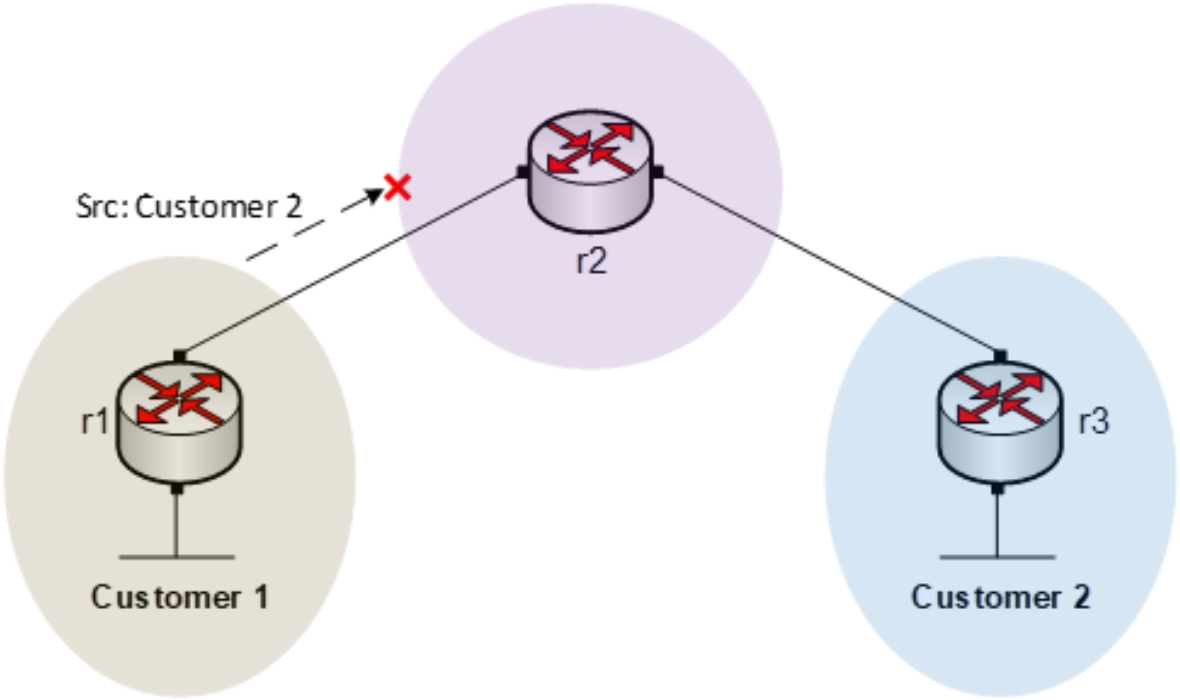
What is IP Spoofing?

- 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.



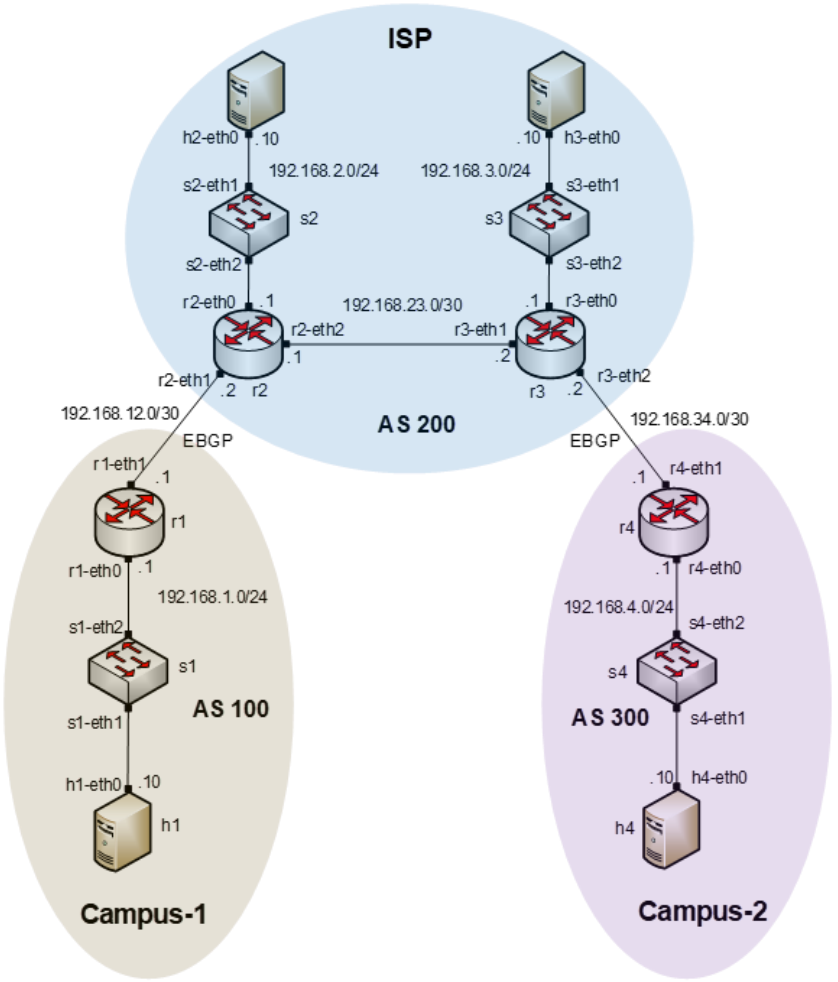
Anti-Spoofing Techniques – Route Filtering

- 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



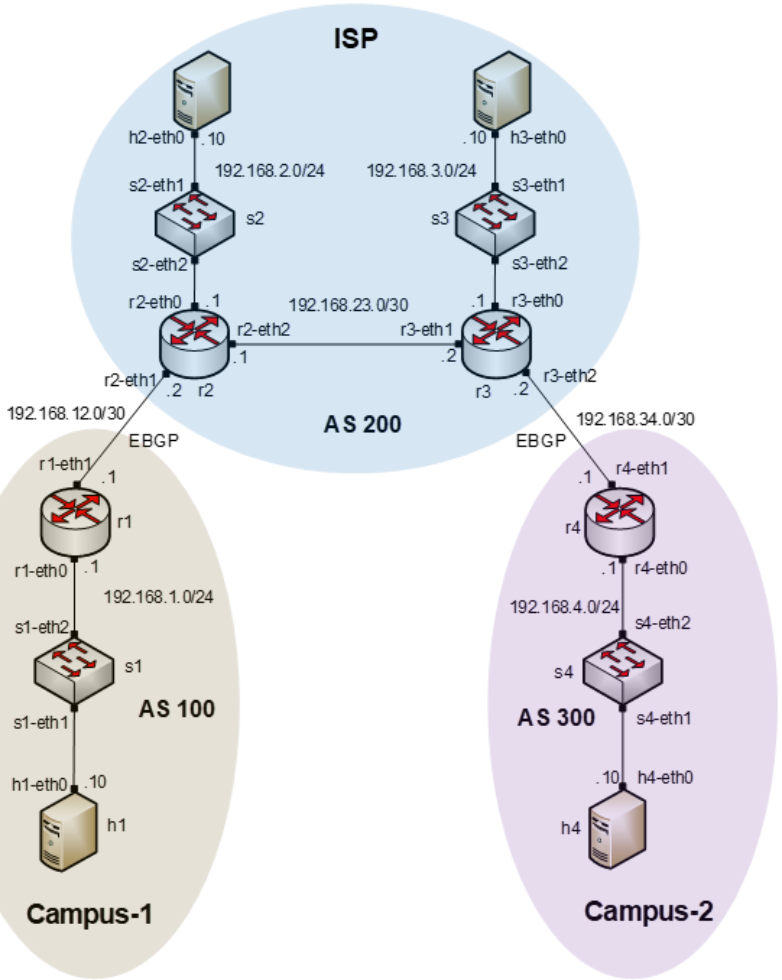
Lab 12 Topology

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



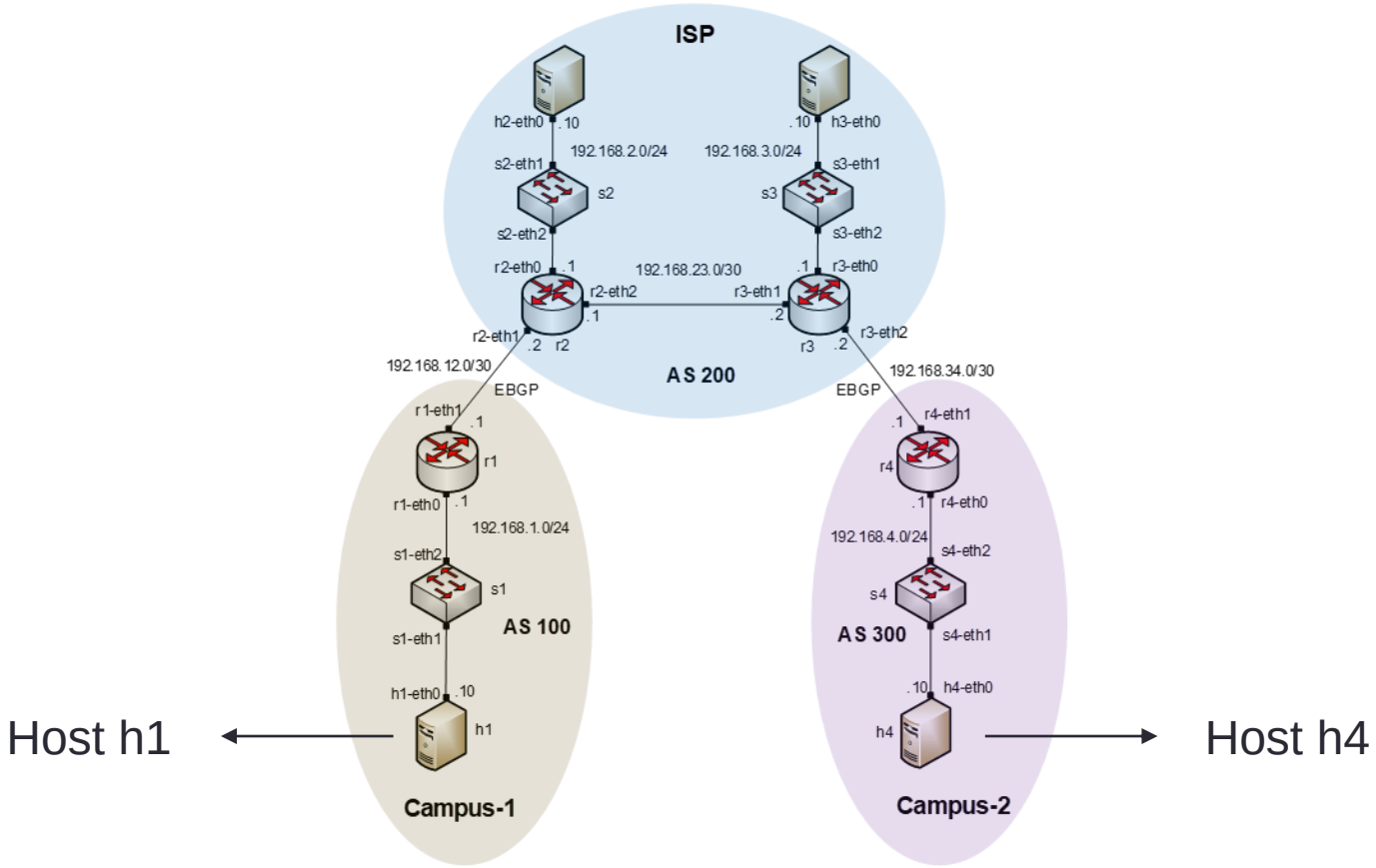
Lab 12 Topology

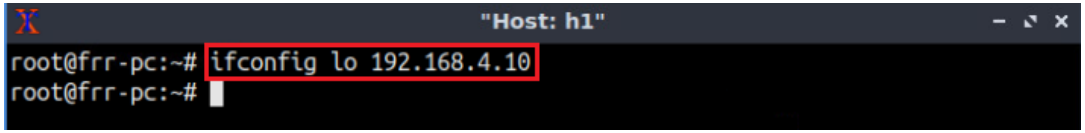
- The Internet Service Provider (ISP) applies the appropriate route filters to prevent IP spoofing



Lab 12 Configuration

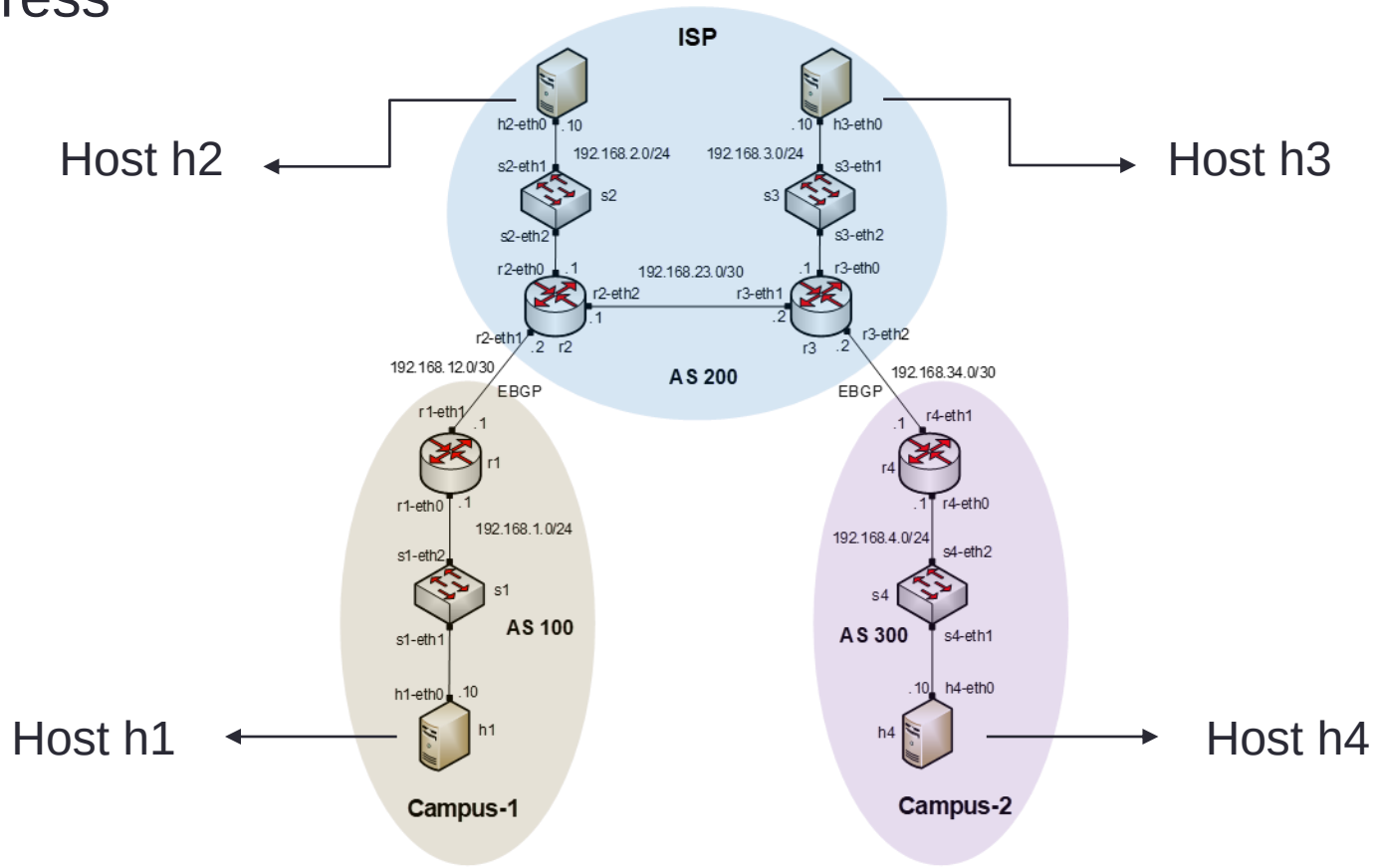
- Host h1 spoofs the IP address of host h4





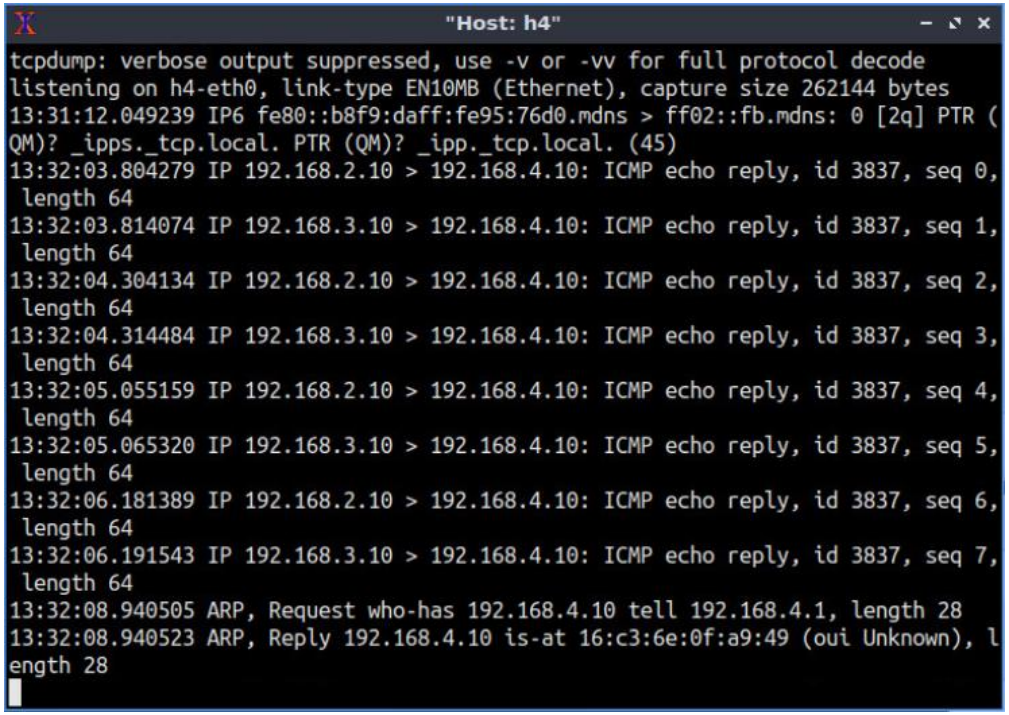
Lab 12 Configuration

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



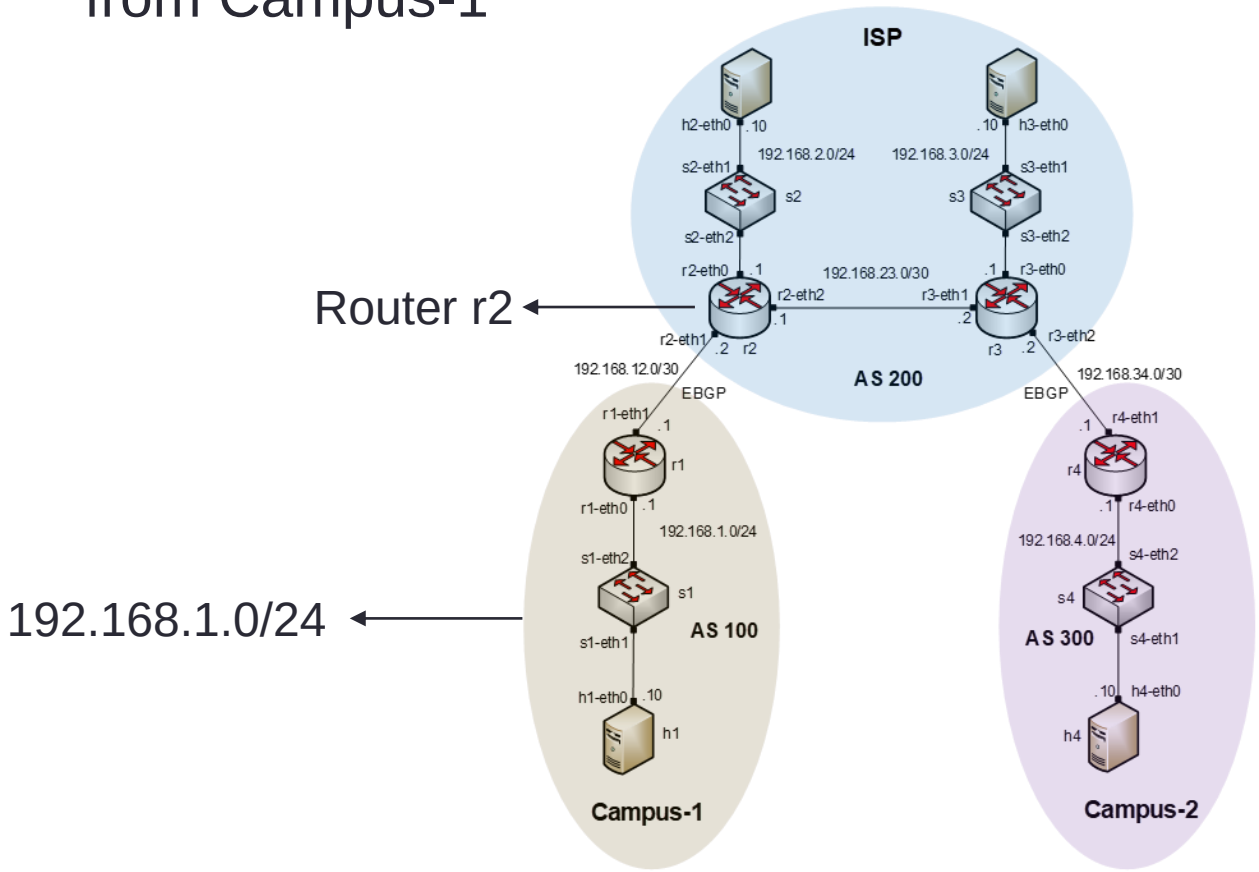
Lab 12 Configuration

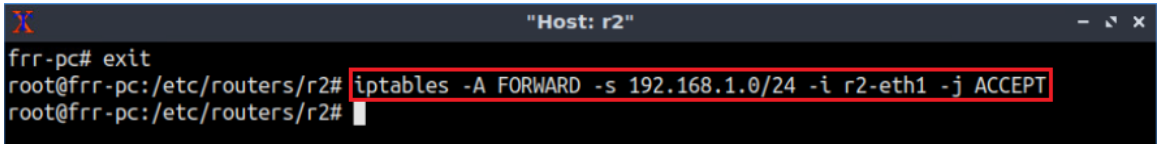
- Host h4 receives a reply messages from 192.168.2.10 and 192.168.3.10



Lab 12 Configuration

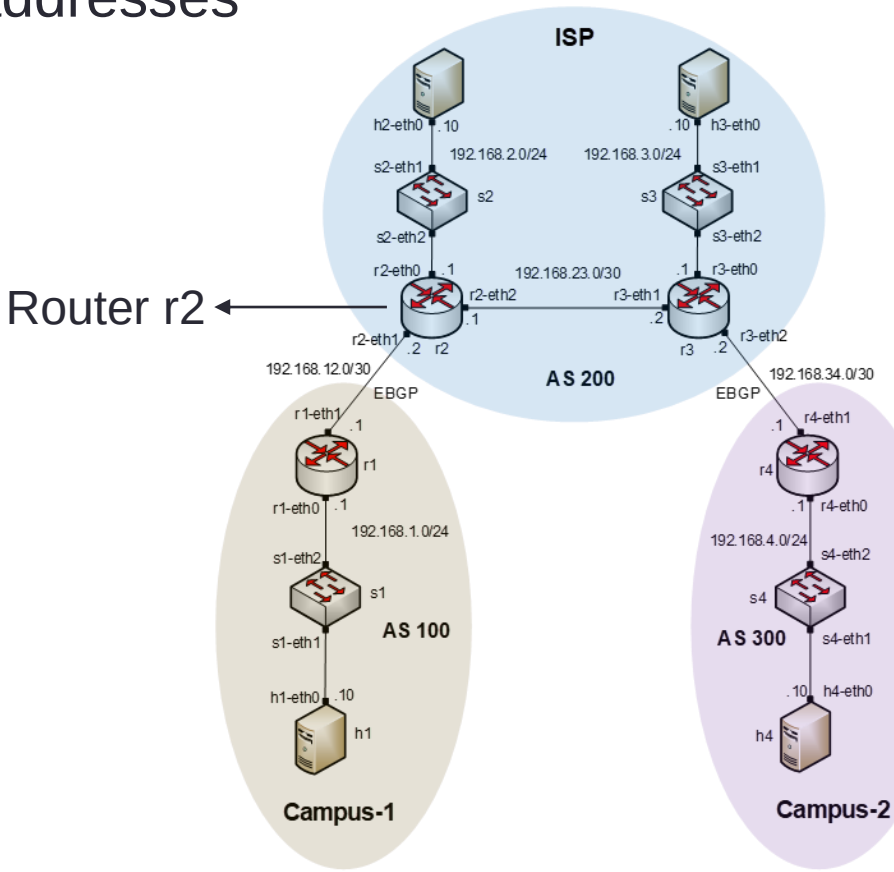
- Apply a filter on router r2 to accept IP source 192.168.1.0/24 from Campus-1

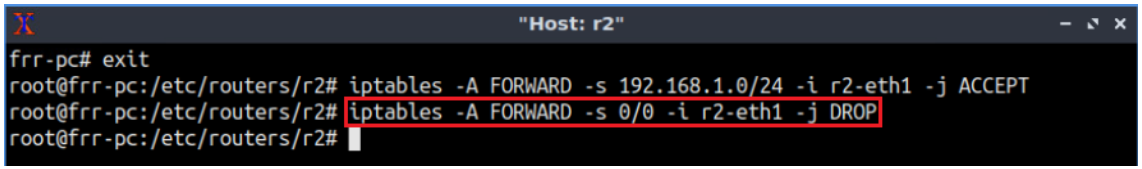




Lab 12 Configuration

- 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