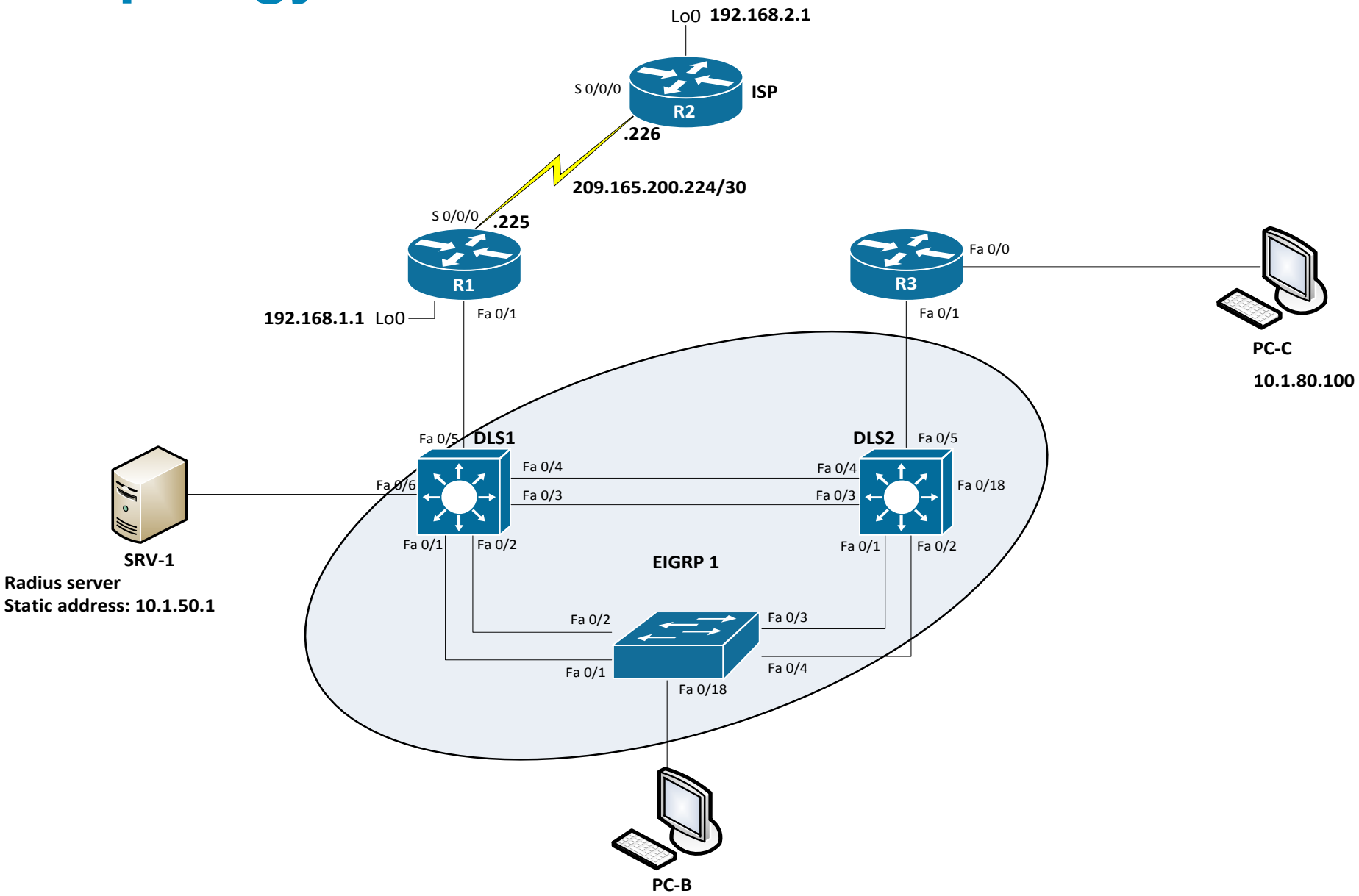
LAB: Module 9

Topology


Lo0 192.168.2.1
S 0/0/0
R2
ISP
.226
209.165.200.224/30
S 0/0/0
.225
R1
192.168.1.1 Lo0
Fa 0/1
R3
Fa 0/0
Fa 0/1
PC-C
10.1.80.100
Fa 0/5
DLS1
DLS2
Fa 0/5
Fa 0/4
Fa 0/4
Fa 0/6
Fa 0/3
Fa 0/3
Fa 0/18
Fa 0/1
Fa 0/2
Fa 0/1
Fa 0/2
EIGRP 1
SRV-1
Radius server
Static address: 10.1.50.1
Fa 0/2
Fa 0/3
Fa 0/1
Fa 0/4
Fa 0/18
PC-B

Tasks

- Prepare topology
- Start TFTP server on SRV-1 with config files
- Troubleshoot security issues

Trouble ticket Lab 9-1 TT-A

- Load appropriate config files: Lab91-%H-91-TT-A-Cfg
- %H: hostname e.g. R1
- As a security measure, your company has decided to implement centralized server-based AAA authentication for key network devices, such as routers and switches. The implementation plan specifies that RADIUS server software is to be installed on SRV1. As a pilot, Layer 3 core switch DLS1 is to be configured with AAA to access the RADIUS server for login authentication. The implementation plan specifies RADIUS as the primary method of authentication, with local authentication as the backup method.
- Your colleague has configured the RADIUS server on SRV1 and AAA login authentication on DLS1 but is having trouble accessing DLS1 when attempting to log in via Telnet from PC-B. On the RADIUS server, he has created a test username **raduser** with a password of **RadUserpass**.
- He has asked for your help in diagnosing and solving the problem.

Trouble ticket Lab 9-1 TT-B

- Load appropriate config files: Lab91-%H-91-TT-B-Cfg
  - %H: hostname e.g. R1
- As a further security measure, your company has decided to implement SSH and only allow vty access to key networking devices from specific management workstations. As a pilot, router R3 will be configured to allow SSH access from only PC-C (on the R3 LAN) and prevent remote access from any host other than PC-C. For testing purposes, host PC-C will be used as a management workstation and will be assigned a static address of 10.1.80.100. Login from PC-C to R3 must be authenticated by the RADIUS server running on SRV1. No other hosts in the network should be able to access R3 via SSH.
- A colleague of yours configured an ACL and SSH access on R3, but due to sporadic hardware issues with R3, she decided to replace R3 with a comparable router. She says that she backed up the configuration from the old router to a USB flash drive and loaded it into the new router. Now she is unable to connect to R3 using SSH from PC-C.
- On the RADIUS server, she created a test user named **raduser** with a password of **RadUserpass**. The implementation plan specifies RADIUS as the primary method of authentication with local authentication as the backup method.
- She has asked for your help in diagnosing and solving the problem.

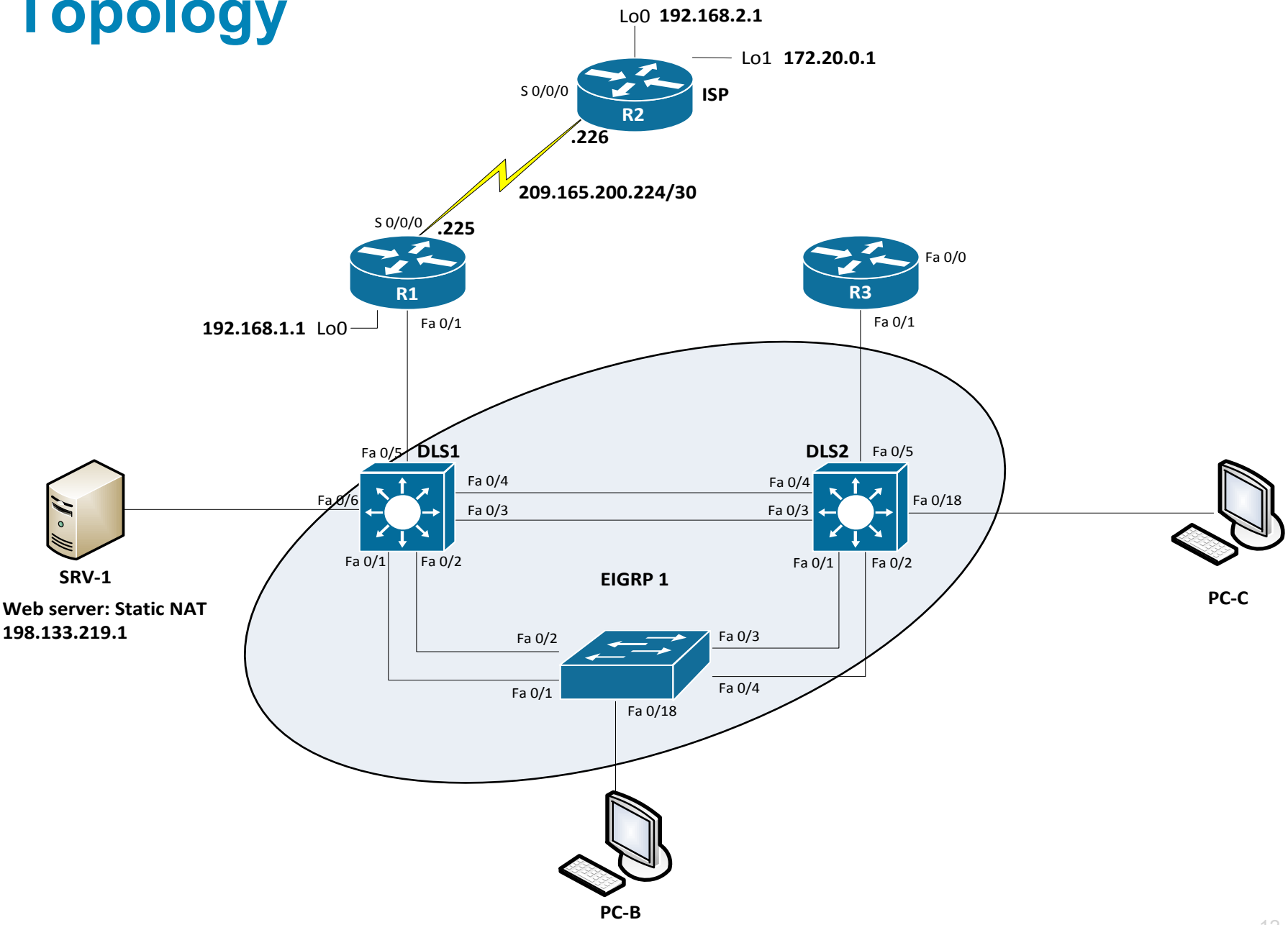
Trouble ticket Lab 9-2 TT-A

- Load appropriate config files: Lab92-%H-92-TT-A-Cfg
  - %H: hostname e.g. R1
- As a security measure, your company has decided to implement DHCP snooping on access switches to prevent DHCP spoofing by unauthorized DHCP servers. For the pilot, the implementation plan specifies that the user VLAN 10 (OFFICE VLAN) on ASL1 be configured for DHCP snooping, and DHCP client PC-B be used as a test station. The test plan requires that the redundant switch topology failover allows VLAN 10 users to obtain an IP address from the DHCP server (DLS1) if one of the trunk links from ALS1 to DLS1 or DLS2 goes down.
- Your colleague has configured DHCP snooping on ASL1, but now PC-B cannot access SRV1 or the Internet. He has asked for your help in diagnosing and solving the problem.

Trouble ticket Lab 9-2 TT-B

- Load appropriate config files: Lab92-%H-92-TT-B-Cfg
  - %H: hostname e.g. R1
- As another control plane security measure, your company has decided to implement MD5 authentication between EIGRP routers and Layer 3 switches. As a pilot, a colleague of yours configured MD5 authentication on Layer 3 switch DLS2 and router R3. Now branch office users on the R3 LAN (PC-C) cannot access SRV1 or the Internet.
- He has asked for your help in diagnosing and solving the problem.

Topology


Lo0 192.168.2.1
Lo1 172.20.0.1
S 0/0/0
R2
ISP
.226
209.165.200.224/30
S 0/0/0
.225
R1
R3
Fa 0/0
192.168.1.1 Lo0
Fa 0/1
Fa 0/1
Fa 0/5
DLS1
DLS2
Fa 0/5
Fa 0/4
Fa 0/4
Fa 0/6
Fa 0/3
Fa 0/3
Fa 0/18
Fa 0/1
Fa 0/2
Fa 0/1
Fa 0/2
EIGRP 1
SRV-1
Web server: Static NAT
198.133.219.1
Fa 0/2
Fa 0/3
Fa 0/1
Fa 0/4
Fa 0/18
PC-C
PC-B

Trouble ticket Lab 9-3 TT-A

- Load appropriate config files: Lab93-%H-93-TT-A-Cfg
  - %H: hostname e.g. R1
- As a security measure, your company has decided to implement stateful packet inspection using a Cisco IOS firewall on edge router R1. The firewall will allow traffic from external hosts only if it is a response to a legitimate request from an internal host. The only exception is that Internet access to the internal SRV1 web-based application will be allowed. Internal users should be able to access the Internet (simulated by Lo1 on R2) using various protocols, such as ICMP, FTP, Telnet, DNS, and HTTP. The firewall implementation must work in conjunction with the dynamic NAT currently being employed on R1. In addition, internal network devices must be able to obtain the correct time from the ISP (R2).
- You colleague has configured the firewall and the necessary access lists on R1. However, users on the office VLAN cannot access Internet websites, and remote users on the Internet cannot access the web-based application on SRV1. Your colleague has asked for your help in diagnosing and solving the problem.

Trouble ticket Lab 9-3 TT-B

- Load appropriate config files: Lab93-%H-93-TT-B-Cfg
  - %H: hostname e.g. R1
- In a continuing effort to improve network data plane security, your company has decided to limit access for users on the guest VLAN 30 subnet (10.1.30.0/24). Guest VLAN users should not have access to any Office VLAN 10 or Server VLAN 50 resources. In addition, it will be necessary to prevent guests from pinging internal network switches. Although they will not have access to internal resources, guest users must be able to access the Internet from VLAN 30. Guest user PCs are DHCP clients (simulated by PC-C) that connect to the network from Layer 3 core switch DLS2 and obtain their IP addresses from DLS1.
- Your colleague has configured a VLAN access control list (VACL) on DLS2 to limit guest access. After the VACL implementation, guests are prevented from accessing Office VLAN and Server VLAN resources, as expected. However, guest users are unable to access the Internet (simulated by R2 Lo1). Your colleague has asked for your help in diagnosing and solving the problem.

Lab created by Vladimír Veselý and Matěj Grégr for C3P

Last update: 2014-04-27