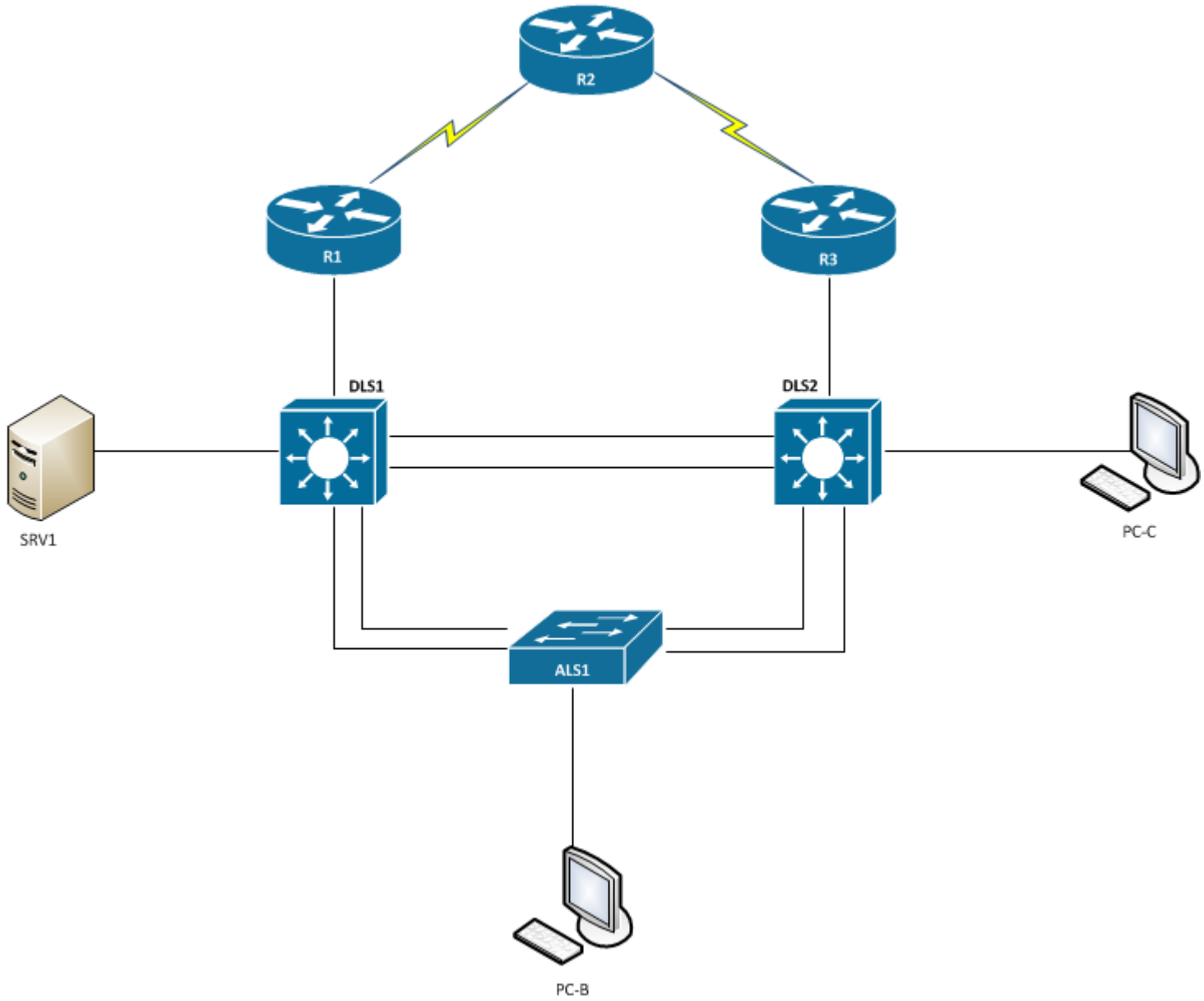
LAB: SRV-1 services

Topology



Tasks

Configure necessary services on SRV1

1. tftp-server
2. Syslog
3. NetFlow collector

A few useful commands

- Check which services are listening on which port

```
# nestat -tlnp
```

- Show firewall rules

```
# iptables -L --line-numbers
```

- Insert firewall rule on specific position in a chain to allow communication on a port

```
# iptables -I INPUT 4 -p udp --dport 514 -j ACCEPT
```

  - `INPUT` chain
  - `4` position of the rule in the chain
  - `-p` protocol type
  - `-j` policy

A few useful commands

- Save iptables rules

```
# service iptables save
```

- Check which services are running in which runlevel

```
# service name start | stop | restart | status
```

- Start, stop, restart a service with init skript

```
# chkconfig --list
```

- Print appended data as the file grows

```
# tail -f /var/log/messages
```

Task 1

- Check if tftp-server is installed and running

```
# service xinetd status | start | stop
```

- Check the settings in `/etc/xinet.d/tftp`
  - `server_args = -s -c /var/lib/tftpboot`
  - **`-c`** flag allows tftpd to create a file, otherwise, the file must be created first on the tftp server and after that uploaded by a client
- Check if port is allowed on firewall
- Check if tftp-server is operated correctly

```
ALS1# copy running-config tftp://10.1.50.1/ALS1-DDMMYY-cfg.txt
```

Task 2

- Check if syslog is installed and running

```
# service rsyslog status | start | stop
```

- Check the settings in `/etc/rsyslogd.conf`
  - Cisco devices use local7 facility by default
  - Create directory `/var/log/tshoot/`
  - `local7.*  "/var/log/tshoot/%fromhost%.log"`
  - Reload config
- Check, if syslog is listening on port 514

```
# netstat -ulnp
```

- Check if port is allowed on firewal

Task 3

- Check if nfdump is installed

```
# which nfdump
```

- Create user accounts to run the daemon:

```
# useradd -r -s /sbin/nologin -d /var/cache/nfdump netflow
# mkdir -p /var/cache/nfdump
# chown netflow:netflow /var/cache/nfdump
```

- Capture NetFlow data on port 9996:

```
# nfcapd -D -l /var/cache/nfdump -w -S 2 -z -u netflow -g
netflow -p 9996
```

Task 3

- Capture NetFlow data on port 9996:

```
# nfcapd -D -l /var/cache/nfdump -w -S 1 -z -u netflow -g
netflow -p 9996
```

- `-l` – base directory to store netflow data
- `-w` – rotate the files (5 min by default)
- `-S` – `%Y/%m/%d` directory sub hierarchy
- Check, if the port is allowed on the firewall
- Print the NetFlow data using nfdump

```
# nfdump -R /var/cache/nfdump/2014/02/01/
```

Lab created by Vladimír Veselý and Matěj Grégr for C3P

Last update: 2014-01-09