Advanced Networking 2018

Lab #2: COS and DSCP
Total points: 15 pts

Assignment
Lab date: February 20 and February 23, 2018
Submission date: February 23, 2018 at 12.00 CET

Author: Arno Bakker, Ralph Koning and Paola Grosso
Email: arno.bakker@os3.nl, R.Koning@uva.nl, p.grosso@uva.nl
University of Amsterdam

Abstract

The first goal of this assignment is to let you familiarize with the basic configuration of an Ethernet switch; the second goal is to be able to configure basic QoS, by using CoS and DSCP.

Preparation

Work in groups of 2 or 3 people. You can choose your mates according to the instructions given during the lecture. You will be configuring Cisco 3750 switches. The user documentation is available at http://software.os3.nl/AdvancedNetworking/ (available only from the OS3 network). You might find it useful to refer to the following:

- QoS Configuration Examples (esp. Egress QoS Features) http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/91862-cat3750-qos-config.html#topic3
- Configuring QoS Guide (http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_52_se/configuration/guide/3750scg/swqos.html)

There are two serial console servers, serialserv3 and serialserv4 located near the Cisco switches. You can use these to connect to the switches' serial ports for configuration as follows. First, connect one of your machines via UTP to one of the switches labeled "Mgmt" (Nortel 5510s or Dell 5524). These Mgmt switches form a management network for this and other labs, and are located near your servers. Next, assign your machine an IP address in the range 10.0.1.63-254. Then, ssh into the serial server (10.0.1.3 and 10.0.1.4, resp.) using the following credentials:

Username is: dialout
Password: os3xsjun

Once logged in, you can access the four serial ports via

```
minicom -b 9600 -D /dev/ttyUSBz
```

where z is 0...3. Port 0 is the leftmost serial port, port 3 the rightmost. Coordinate with your fellow students who uses which port. Finally, use a serial cable (e.g. light blue with RJ45 for Cisco) to connect to the switch's console (located at the back of the switch for Cisco).

Task 1: Connection to the switch

1. Connect to the serial console of the switch (directly, or via the serial servers).
2. Assign a private IP address to the switch for its management.
3. Every group member should connect his/her server to the switch and configure the appropriate IP addresses on their server. Verify connectivity to each other.
4. Create user accounts for each group member and set password for SSH and console login on the switch. Disable Telnet, HTTP and HTTPS connections if possible.

At the end of this task you should all be able to connect to the switch from your server using your own account.

Notes:

- Remember to regularly save your running configuration to the startup configuration; you might consider copying also your configuration to an TFTP server you have set up for this purpose.

Task 2: Data transfer without and with CoS configuration (10 points)

In this task you are asked to perform data transfers between the nodes connected to the switch.

1. User *iperf* or another data transfer application of your choice to transfer data between a pair of nodes. Tune the data transfer to achieve maximum throughput.
2. Define a number of scenarios where the data transfers interfere with each other. Use your imagination!
    - One basic scenario could be the one in which multiple nodes and applications are trying to communicate with one node; think, for example, having iperf streams mixed with other applications. If you can think of more complex scenarios you are welcome!
    - Alternatively you can run multiple connections in parallel and decide which ones are to be prioritized.
    - You are welcome to think of different scenarios. For example, using VoIP.

Now you have to overcome the interference by applying CoS. You will try to improve the performance of the communication by starting from the degraded scenarios above. `Hint: mls qos trust cos`

- Configure CoS marking the switch ports and try to achieve desired behaviour by manipulating the mapping between class of service and the available input/output queues.
- Show what the difference is between SRR shape and share modes.

Task 4: DSCP (3 points)

1. Mark your outgoing packets using iptables.
2. Show that the packets are marked (with Wireshark).
3. Show how DSCP marking improves traffic performance.

`Hint: mls qos trust dscp`

Task 5: Monitoring (2 points)

1. Enable logging of events (syslog) to an external server.
2. Monitor your switch so that its statistics can be viewed online. This requires to poll via SNMP. Possible tools (you can choose) you might consider:
   - MRTG: http://oss.oetiker.ch/mrtg/
   - Cacti and Nagios: http://www.cacti.net/
   - Cricket: http://cricket.sourceforge.net/
   - NetDisco: http://www.netdisco.org/
3. Monitor also your servers via the IF-MIB from RFC2863.
4. Start a webserver on one of the group's servers and make sure it can be accessed from within OS3. Monitoring must still be live at the time the exercises get corrected (in the week of February 26 and March 05 2018)! The monitoring pages should still clearly show the test you made and the traffic through the switch. Historical data is fine, as the Cisco switches will be reused for the next lab.

Submission

The submission must contain following:

- The final switch configuration (DUMP file and txt).
- PDF document containing:
  1. Configuration explanation.
  2. Results of the data transfer tests:
     (a) Without CoS/DSCP (Task 2) : describe the scenarios you have defined and show the transfer results;
     (b) With CoS (Task 3): explain if the results are the one you expected given the CoS configuration;
     (c) With DSCP (Task 4): Show marking and explain if and how DSCP has improved the situation.
  3. Link to the monitoring server (the data transfers need to be visible on the monitoring site!)