IP Networking Lab Assignment

Configuring Basic Aspects of MPLS

1 Purpose and Goals

This lab assignment will give you a hands-on experience in configuring basic MPLS using OSPF as an IGP routing protocol. You will prepare the lab session, perform the practical exercises, and write a lab report, which describes the whole lab, including planning, preparations, and results. You will work and hand in the report in groups of two students.

The lab report will be assessed; grading will be added to the total course score - check the course home page for details.

2 Overview

The Assignment is divided into preparation, practical part and documentation.

2.1 Preparations

The preparations are crucial to the successful execution of the main exercise. Without proper study there is no possibility to fulfil the requirements within the specified time; trial-and-error will not work!

The Appendix contains some basic information related to Cisco IOS software, that you should read and understand to follow the instructions provided in this document. However, during this phase it is advised to study the additional Cisco routers documentation available in the Internet if any additional explanations to relevant IOS commands are required. Finally, you should refresh and expand your knowledge on the topic of the lab exercise.

2.2 Lab Access and the Exercise

The main exercise is executed using the virtual lab that is accessible remotely from a computer of your choice via the Internet – you don't need to be present in the Lab room during the exercise. To access the lab you only need a PC with Internet access, an OpenVPN client installed (the app is freely available at: https://openvpn.net/community-downloads/) and a terminal client. For the latter we strongly recommend using MobaXTerm free application, available at https://mobaxterm.mobatek.net/download-home-edition.html, but you can use other similar applications (such as PuTTY), provided that they support the required functions (such as capturing the terminal text to the file in a well-readable format).

The lab environment emulates Cisco routers, and so the router operation system is IOS. The emulated network topology is fixed – changes can be only introduced by opening and closing individual router interfaces.

Before starting the main lab exercise, it is required to reserve the lab resources beforehand using the Resource Reservation system. Please refer to the *Resource Reservation User Guide* accessible at the relevant course home page. The lab can be booked for maximum of 4 hours (this is a total time assigned for completing the lab exercise). If you are well-prepared, this should be enough to execute the main exercise and gather information required to prepare the lab report.

To access the lab remotely, you first need to obtain the relevant OpenVPN certificate and then, at the reserved lab time, open the OpenVPN session. After successful login to the VPN network, the router consoles should be accessible via *telnet* sessions to the terminal server inside the VPN using the terminal client. For detailed instructions, please refer to the *Remote Access User Guide* accessible at the relevant course home page.

The tasks required to pass the exercise are described in detail in Section 3.

In case of any technical problems during the exercise (problems with remote access, access to router consoles, instability etc.) please contact the lab supervisor. The exercise can be repeated in cases justified by the observed technical problems.

Remark: do not use the `reload` command if you want to restore the initial state of the router during the exercise, or you will lose access to the router console. Use the procedure described in the Appendix instead, if necessary.

2.3 FINAL REPORT

The last phase consists of lab report preparation. You should plan the outline of the report in advance, during the preparation phase to be sure what input is necessary before attempting the main part of the exercise.

The report should contain the findings collected during the main practical part. This instruction will provide the questions and remarks (usually marked with different colour) as a guideline for the mandatory content of the report. Please make sure that you paste all required screenshots or text from terminal where asked and provide relevant explanations. The report should be clear, logical, concise, and formatted in a form that is typical for technical documents.

The final archive to be delivered as a result of the exercise should contain:

1. The report (in PDF format – all other formats will be rejected)
2. The file (or files) containing the text from all terminal windows where the router's consoles were accessed (the MobaXTerm software provides a very convenient way to save the content of the terminal window; the procedure is described in the *Remote Access User Guide*). **The archives without these files will be rejected.**

Please deliver the final report before the deadline announced for this exercise.

Note: If you find any errors or inconsistencies in this document and referenced manuals, please report them to the lab exercise supervisor(s). It will help to improve the lab exercise in the future.

3 LAB EXERCISE

The topology of the network emulated in the virtual environment is shown in Figure 1. All emulated routers are Cisco 3600. The experience of configuring the routers running within the virtual environment is indistinguishable from configuration of actual devices via typical ssh console access.

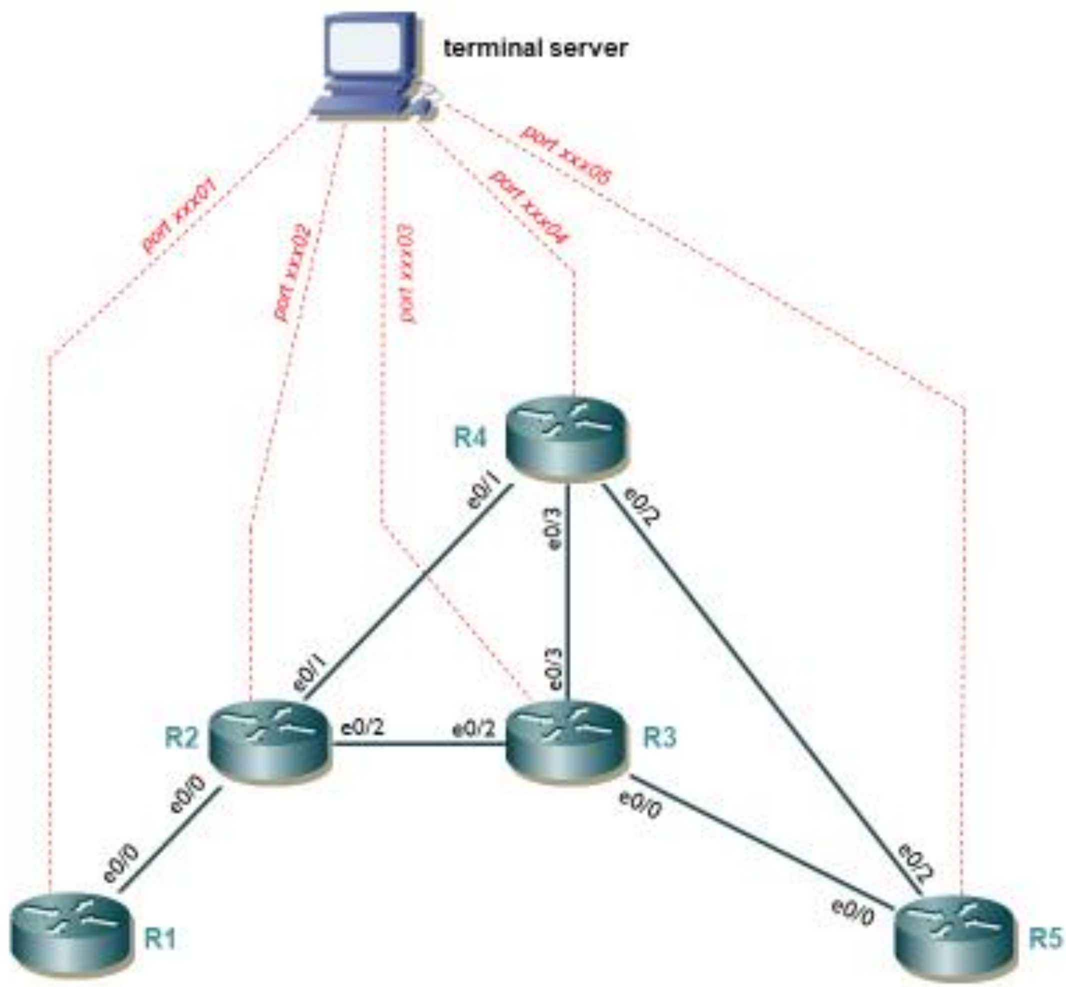

Figure 1. Router Lab topology

The lab exercise is divided into two main parts:

- basic MPLS configuration using LDP protocol,
- traffic engineering with MPLS using RSVP-TE protocol.

The remainder of this section covers all practical tasks that constitute the scope of this exercise.

3A. ADDRESS ASSIGNMENT

Start this lab assignment with allocating appropriate IP addresses to all routers' interfaces, in accordance with the lab topology presented in Fig. 1, and the information provided in Table 1. Remember that each router interface must have a unique IP address on the subnet that it belongs to. Remember to configure loopback interfaces.

Note: The MPLS LSRs must have (up) Loopback interfaces with an address mask of 32 bits and these interfaces must be reachable with the global IP routing table.

Subnet	Subnet address
R1-R2	10.0.12.0/30
R2-R4	10.0.24.0/30
R3-R4	10.0.34.0/30
R3-R5	10.0.35.0/30
R4-R5	10.0.45.0/30
R2-R3	10.0.23.0/30
Router	Loopback Address
R1	1.1.1.1/32
R2	2.2.2.2/32
R3	3.3.3.3/32
R4	4.4.4.4/32
R5	5.5.5.5/32

Table 1. Addressing plan

Configure IP addresses of all interfaces. Use CDP and check your configuration (use the following commands):

```
#show cdp neighbour,
#show cdp neighbour <interface> detail
```

Place the details of the addressing plan in the report.

3B. RUNNING OSPF

Before you can configure MPLS you must have routing protocol (OSPF in our case) up and running in the network. Enabling OSPF is required to compute routing tables of the different LSRs (Label Switching Routers). A label distribution protocol (LDP) advertises the bindings between routes and labels. These bindings are then checked against the routing table. If the route (prefix/mask and next hop) learned from the LDP matches the route learned from OSPF in the routing table, an entry is created in the Label Forwarding Information Base (LFIB) on the LSR.

In the config mode, initiate OSPF on every router, and add interfaces (<u>including loopbacks</u>) to the OSPF:

```
#router ospf 1
#network <X.X.X.X> <Y.Y.Y.Y> area 0
X.X.X.X – IP network prefix
Y.Y.Y.Y – wildcard mask
```

All interfaces (except loopbacks) should run OSPF in point-to-point mode – set this mode if necessary using **ip ospf network point-to-point** command in the context of the selected interface.

Check the routing information and routing table in all routers. Ensure that OSPF protocol works properly (ping each router from any other to verify).

Check OSPF metric (link cost) for all network links. You can use **show ip ospf interface brief** command, or the more advanced **show ip ospf interface | include protocol|Cost**

For the needs of the exercise, all link costs should be set to the value of 10, except the link between the routers R2 and R3, where the cost should be set to 100 (this is to simplify the output of *traceroute* command in case of equal cost paths). Use the following command in the interface configuration mode to change the link costs if required (set the metric on both sides of the link, if necessary).

#ip ospf cost <your cost>

Verify via the *traceroute* command between R1 and R5 what is the effect of cost differentiation on R2-R3 link. *Copy/paste the output of this command into the report and explain the content.*

3C. BASIC MPLS CONFIGURATION

Configure MPLS protocol in the network. For better performances enable *ip cef* (use *ip cef distributed* when available) in the general configuration mode. You must enable MPLS both on the router and on the specific interfaces you want to add to MPLS.

Enable MPLS and LDP protocols on each router (in global configuration mode):

#ip cef (enable cef mode if not already enabled)
#mpls ip

To run MPLS on a given interface you must explicitly enable MPLS on that interface:

```
#interface e0/1
#mpls ip
#exit
```

Study the appropriate documentation to extend your knowledge about MPLS configuration if needed.

3D. VERIFY MPLS/LDP SETUP

Analyze *show* command output for selected router. Short summary of *show* command functionality that can be used to verify MPLS configuration is provided below.

Information about interfaces added to the MPLS process.
#show mpls interfaces

Information about LDP neighbors.
#show mpls ldp neighbor

LIB (MPLS equivalent of the Routing Information Base) data:
#show mpls ldp binding

LFIB (MPLS equivalent of the IP routing table); contains inbound and outbound labels and descriptions of the packets:

```
#show mpls forwarding-table
```

MPLS forwarding table details (if <prefix> is given, only one entry is shown):

```
#show mpls forwarding-table <prefix> detail
```

Copy-paste the outputs of the above commands from router R2 into the report and explain briefly.

3E. CHECK PATHS

Now that you have MPLS running in your network you can check if packets are forwarded using the expected paths. You shall compare the MPLS forwarding table of R1 and the result of a *traceroute*.

- From the forwarding table in router R1 find the path to the loopback interface of router R5. Do *a traceroute* to this interface (from R1). *Add the output from this command to the report and explain it. Did the packets take the expected path?*
- Use the appropriate commands to check what label numbers are used on each router for the above IP flow. *Present this information in the report.*

3F. CONFIGURE BASIC TRAFFIC ENGINEERING

This part of the exercise explains the basics of implementing traffic engineering (TE) on top of an existing MPLS configuration using OSPF routing protocol. MPLS TE uses an extension to existing OSPF protocol to calculate and establish unidirectional tunnels that are set according to the specific constraints. For setting and maintaining tunnels based on the calculated path the RSVP-TE protocol is used (PATH and RESV messages). The typical RSVP capabilities are extended to allow it to distribute label information.

I. Enable traffic engineering for the routing protocol

First, you must enable MPLS TE for a given routing protocol and set the loopback interface as MPLS router id. In the routing protocol configuration mode (use *router ospf 1*) enter the following commands:

```
mpls traffic-eng area 0
mpls traffic-eng router-id loopback0
```

II. Enable traffic engineering capabilities on the router and router interfaces

You must enable MPLS traffic engineering both on the router and on each concerned interface. In the global configuration mode as well as in the interface configuration mode enter the following command (hint: enter this command in the global configuration mode first):

```
mpls traffic-eng tunnels
```

III. Enable RSVP

This can be done by entering **ip rsvp bandwidth XXX** on each concerned interface. Limit RSVP bandwidth to very low value on the link between routers **R2 and R4** (setup some small value like 64 kbps on both ends). Setup higher bandwidth for other interfaces (e.g. 512 kbps). Use the following command:

```
ip rsvp bandwidth 512
```

IV. Set up RSVP TE (Traffic Engineering) tunnel

Now you can define MPLS tunnels with specific traffic engineering parameters between routers. First set up dynamic tunnel between routers R1 and R5 with specific bandwidth demand. On router R1 and R5 define the tunnel interfaces. To do this enter the interface configuration mode giving the tunnel name as the interface (e.g. **`interface tunnel1`**). This will create the tunnel interface with the specified name on the router. Next, issue the following commands:

```
mpls ip
ip unnumbered loopback0
no ip directed-broadcast
tunnel destination y.y.y.y
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 5
tunnel mpls traffic-eng bandwidth 256
tunnel mpls traffic-eng path-option 2 dynamic
```

The *tunnel mode mpls traffic−eng* command is mandatory. The *tunnel mpls traffic−eng autoroute announce* command announces the presence of the tunnel by the routing protocol. Note: Do not forget to use *ip unnumbered loopback0* for the IP address of the tunnel interfaces. As destination address use the loopback address of the destination router.

- From R1, find the route calculated for the created MPLS traffic engineering tunnel (tunnel1) using command: **`show mpls traffic-eng tunnels`**. *Add the output from this command to the report.*
- Confirm that the packets sent to loopback interface of R5 take the tunnel by analyzing the OSPF and MPLS forwarding tables in the appropriate routers. *Note the route in the report and explain the difference between current route and route from section E, if any.*
- Do *a traceroute* to this interface from R1. *Add the output from this command to the report and explain it.*

Next, restore the RSVP bandwidth limit on the link between router R2 and R4 to normal value (eg. 512 kbps) and set the RSVP bandwidth limit to 64 kbps on the link between R2 and R3.

- From router R1 find the route calculated for *tunnel1* and compare with previous result. *Note the findings in the report and explain the difference.*

V. Set up explicit path tunnel

Make sure that the RSVP bandwidth limit is set to the same value on all links. Shutdown the tunnel1 (using the *configure interface* context). Traceroute the loopback interface of router R5 from R1, observe and explain the result.

Next, Set up explicit MPLS path from R1 to R5, traversing routers R2, R3 and R4. Add second tunnel interface for this path (e.g. **`interface tunnel2`**) and use the following commands :

```
mpls ip
ip unnumbered loopback0
tunnel destination y.y.y.y
```

```
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 2
tunnel mpls traffic-eng bandwidth 256
tunnel mpls traffic-eng path-option 1 explicit name MyPath
```

The explicit path between R1 and R5 can be defined (in the general config context mode) as follows *(study the CISCO documentation if required).*

```
ip explicit-path name MyPath enable
next-address z.z.z.z
...
```

Check how packets are routed between R1 and R5, *prove that the explicit tunnel is utilized and place this information in the report.*

VI. OSPF-TE (OPTIONAL)

The following commands are specific to MPLS TE with OSPF:

```
show ip ospf mpls traffic-eng link
show ip ospf database opaque-area
```

You can use the **`show ip ospf mpls traffic-eng link`** command to see what will be advertised by OSPF at a given router.

The **`show ip ospf database opaque-area`** restrains the output to Type 10 LSAs and shows the content of the TED database that is used by the MPLS TE process to calculate the best route for dynamic tunnels.

*Execute **the first command** on R2, copy/paste the output to the report and explain the content.*

3G. CLOSING REMARKS

Before exiting the lab environment, you are required to do the following:

1. Run "show running-config" command on each router console
2. Save the terminal text for each router console and attach the saved files to the zip archive containing the report.

The reports that do not fulfill the above requirements will be rejected.

Do not forget to list the authors' names on the first page of the report and use the following template for archive naming: **COURSE_Semester_FirstAuthorSurname.zip** (example: DT_2021Z_Kowalski.zip).

4 DOCUMENTATION

At the course page you should have access to the following two complementary documents:

- *Resource Reservation User Guide*
- *Remote Access User Guide*