IP Networking Lab Assignment

Configuring Basic Aspects of BGP Routing Protocol

1 Purpose and Goals

The BGP is used for inter-domain routing, and it is the only routing protocol used in the Internet to route IP packets between the networks of different ISPs.

This lab assignment will give you a hands-on experience in configuring basic aspects of the BGP. 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!

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.

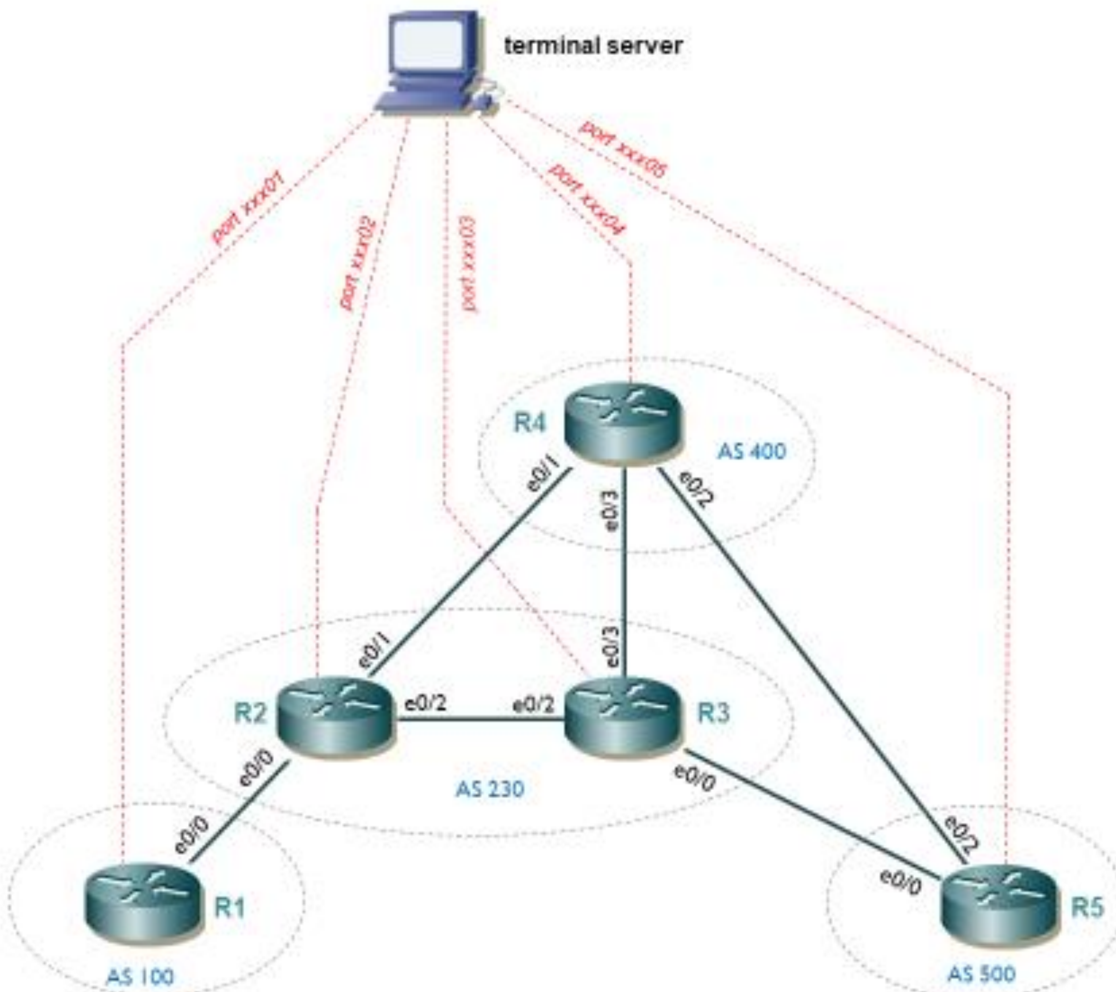

Figure 1. Router Lab topology

The lab exercise is divided into four main parts:

- Preparation of IP address assignment for the network
- Configuration of OSPF protocol between R2 and R3
- Basic configuration of BGP peering
- Advanced configuration of BGP protocol

Before you start, it should be mentioned that when you make changes to the BGP configuration, it usually takes some time before the changes are propagated throughout the network. To force the routers to exchange updates you can:

a) clear the BGP routing table on the router using the `clear ip bgp *` command; this command tears down all the BGP sessions on the router and is safe in the lab environment, however the much better method is:

b) to perform the route-refresh by soft reset, using:

```
clear ip bgp <neighbor address> soft
```

this method is selective, and keeps the TCP session up and just refreshes any routing changes.

3A. IP ADDRESS ASSIGNMENT

In this exercise, you configure the BGP protocol between lab routers. Each router, except R2 and R3, represents a single AS (autonomous system). Routers R2 and R3 belong to the same AS.

Your first task is to configure network addresses of the router interfaces. Allocate appropriate network addresses considering configuration information provided in Table 1 (use the subnet or IP addresses as specified in the 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	AS	Interface	Address
R1	AS100	L0	1.1.1.1/32
		L1	192.168.11.1/24
R4	AS400	L0	4.4.4.4/32
		L1	192.168.41.1/24
		L2	192.168.42.1/24
		L3	192.168.43.1/24
R5	AS500	L0	5.5.5.5/32
		L1	192.168.51.1/24
		L2	192.168.52.1/24
R2	AS230	L0	2.2.2.2/32
		L1	192.168.21.1/24
R3	AS230	L0	3.3.3.3/32
		L1	192.168.31.1/24

Table 1. Addressing plan

Place the addressing scheme at the beginning of the report (preferably in a form of table or picture). You should plan the addressing scheme during preparation phase.

Remember that each router interface must have a unique IP address on the subnet that it belongs to.

Use the following command to configure the IP address of an interface:

```
ip address <ip address> <mask>
```

You should end this step with IP addresses configured on all routers' interfaces. Check your IP address assignment. You should be able to ping the other end of the directly connected subnets (the other end of the Ethernet link) from each router. Note that you will not be able to ping IP address from the subnets that are not directly connected.

Note also that the additional loopback interfaces (L1, …) will in this exercise emulate the customer networks attached to the routers, and are all intended to be advertised between all Autonomous Systems using BGP.

3B. OSFP CONFIGURATION IN AS 230

The routers R2 and R3 both belong to the same Autonomous System, and so you need to configure an IGP routing protocol (OSPF in our case) that will allow them to communicate. This step is mandatory for execution of all subsequent tasks related to BGP configuration.

You can initiate OSPF on the routers using **`router ospf`** command (with a selected process ID). After that you should add the subnet R2-R3 and loopback 0 interfaces of R2 and R3 to OSPF routing process (using a **`network`** sub-mode command with appropriate attributes).

After doing this, you should check if the OSPF is configured and runs properly, by analysing the routing table entries on R2 and R3, and pinging the loopback interface of R3 from R2, and vice versa. Place the output of ping command in the report.

3C. BASIC BGP CONFIGURATION (STEP-BY-STEP)

Before getting to configuration tasks, a short refresher on configuring the BGP.

The first step in configuring BGP protocol is to enter the router's BGP configuration sub-mode using the following command:

```
router bgp <AS number>
```

The above command starts the routing process for the given autonomous system (as specified by the <AS number> parameter). The suggested AS numbers are given in Table 1.

Next step in configuring BGP protocol is to setup BGP neighbors. Notice that there is no automatic discovery of the neighbor routers in the BGP protocol. Neighbors must be configured manually by the network administrator. You can configure the BGP neighbor using the following command in BGP sub-mode:

```
neighbor <ip address> remote-as <AS number>
```

The first parameter above is the IP address of the neighbor router's interface. The second parameter is the AS number of the neighbor router (the AS system to which the neighbor router belongs). In case of the iBGP session, the <AS number> parameter is the same as the AS number of the router for which we are configuring neighbor. In case of the eBGP, this parameter is the AS number of the remote system.

In case of eBGP, the session is usually set using the address of the remote end of the interface connecting the peer with a neighbor. For iBGP, it is advised to use the loopback address to define the BGP neighbor. However, by default, the BGP session uses the outgoing interface address as the source IP address for establishing the TCP connection with the neighbor. You can change this by explicitly defining the interface that should be used as the source IP address for the BGP session using the following command:

```
neighbor <ip address> update-source <interface>
```

The <ip address> parameter is the address of the neighbor router while the <interface> parameter specifies the source interface for the BGP session with this neighbor. This command is typically used when you use loopback interfaces as the neighbor addresses or in case the BGP routers are multi-homed.

I. Task C1

Your first task is to configure the iBGP session between routers R2 and R3 using the above commands. Use the loopback 0 addresses for defining the BGP neighbors (do not explicitly specify the source IP address for the BGP session yet). Check the BGP session state using the **`show ip bgp neighbors`** command.

Next, specify the source IP addresses for the BGP session between routers R2 and R3. Use the L0 (loopback 0) addresses as the source addresses for the BGP session. Check the BGP session state again, confirm that it is established and place the proof (the relevant part of the **`show ip bgp neighbors`** command) in the report.

II. Task C2

Configure eBGP session between routers R1 and R2. Use the IP addresses of the direct link between routers R1 and R2, **not** the loopback addresses). Note that it can take some time for the session to be established.

Check the status of the BGP adjacency on R1 and R2 using the following commands:

```
show ip bgp summary
show ip bgp neighbors
```

Place the output of the first command to the report as a proof that the session is established.

III. Task C3

To assign networks to the BGP process (or, in other words, advertise prefixes via the BGP), use the following BGP sub-mode command:

```
network <network prefix> mask <mask>
```

The **`network`** command takes two arguments: the network address and the mask of the network that should be added to the BGP process. The subnets added with the network command will be propagated by the BGP protocol throughout the network.

Remark: When executing lab tasks please think and decide carefully which networks must be added to BGP protocol. Do not add networks that are irrelevant for performing the given lab tasks (such as subnets related to router interfaces, if this is not required).

Add network represented by the R1 loopback 1 interface to the BGP protocol using the network command described above. *Ado the same with loopback 1 interface on R3.* Check if the networks you have entered to the BGP protocol are present in the routing tables of routers in AS100 and AS230 using the following commands:

`show ip route` (the content of the routing table: the best paths from all routing protocols + static routes and directly connected networks)

`show ip bgp` (prefixes from the bgp database)

Place the result of the above commands in the report and explain why the address advertised from R1 (loopback 1) is not visible in the routing table of R3.

Configure router R2 to solve this issue ***using an appropriate command*** *(consult e.g. the lecture slides related to basic BGP path attributes).*

Check the content of the routing table of R3 again, place the result in the report and explain the change. Now check if the advertised network (loopback 1 of R1) is accessible from R3 using **`ping`** command with source address set to R1 loopback 1. Check and explain why the ping does not work without the source address even if the target network is now present in the routing table of R3 (think of how the ping service works in both directions).

IV. Task C4

*Configure all remaining eBGP sessions between Autonomous Systems in the lab setup (using addresses of interfaces connecting the relevant peers – **not** loopback interfaces).*

Check if all sessions are established properly. Provide the proof in the report.

V. Task C5

Advertise all remaining L1, L2 (where applicable) and L3 (where applicable) loopback addresses via the BGP. Check if they have propagated into the routing tables of all routers and provide the proof in the report.

VI. Task C6

*On router R1, check the connectivity to the advertised R5 loopback 1 interface using the **`ping`** command.* Hint: execute the **`ping`** command specifying the R1 loopback 1 interface as the source IP address:

```
ping <ip address> source <interface>
```

Next, execute the **`traceroute`** command to the R5 loopback 1 interface, setting R1 loopback 1 interface as the source IP address (hint: use *ctrl-shift-6* to cancel the traceroute if needed):

```
traceroute <ip address> source <interface>
```

Place the result of the trace in the report. Explain what path the traffic takes between R1 and R5 and why (check the routing tables of the routers on the path, paying attention to the next hop router addresses).

Configure router R3 to override the next hop in the BGP advertisements with its own address (this is analogous to what should have been done in task C3). Check the traceroute again and compare. Place the result of the trace in the report and explain the difference.

3D. ADVANCED BGP CONFIGURATION

If you have decided to devote a separate session to execute this part of the lab exercise, please configure the following (using the experience from executing the tasks from section C):

- network interface addresses
- OSPF and iBGP inside AS 230
- next-hop-self on R2-R3 iBGP session
- all eBGP sessions between ASs
- L1, L2 (where applicable) and L3 (where applicable) advertisements via BGP on all routers.

I. Task D1 (LOCAL PREFERENCE)

Local preference attribute is used to control how the traffic leaves a given AS system. It allows a network administrator to control the *outbound* traffic flow. The local preference attribute has only local meaning (it is not propagated to the neighboring AS systems). It has also no influence on the inbound traffic (which is controlled by the other AS). Local preference is sent to all internal BGP routers in your autonomous system but not to the external peers. The default Local Preference value is 100.

Your aim is to configure AS 230 in such a way that all traffic sent from R1 to R4 will leave AS 230 via interface e0/3 of router R3.

Execute the traceroute command from router R1 to R4 loopback 1 interface, setting R1 loopback 1 interface as a source. Copy and paste the output of the traceroute command to the report.

Next, configure the local preference to force the outbound traffic from AS230 to AS400 to be routed through the interface e0/3 of router R3. This option is usually used to prefer higher capacity links to route traffic out of the given AS.

To set the local preference you should create a route-map. A route map is an ordered sequence of individual statements, each has a permit or deny result. Evaluation of a route-map consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is aborted once the first statement match is found and an action associated with the statement match is performed. The route-map mechanism enables (among other uses) defining routing policies considered before the router examines the forwarding table. Route-map clauses are numbered. Typically, clauses have sequence numbers 10, 20, and 30. Cisco recommends to number clauses in intervals of 10, to reserve numbering space in case you need to insert clauses in the future.

For the current task you can define your route-map use the following commands:

```
route-map <name> permit <number>
```

Then set the local preference value (inside the route map configuration menu):

```
set local-preference <value>
```

The route map sets the local preference of received routes to the <value> parameter — the higher is the value, the more preferred is the route. Then <name> parameter is the name of the route map of your choice.

Next, the route map should be applied to the relevant BGP session using BGP sub-mode command: enter **router bgp ...** and then:

```
neighbor <neighbor address> route-map <name> in
```

The last part of the command indicates that the route-map is applied to the routing information received from a given neighbor. Clear the relevant BGP sessions after application of the route map(s) to observe changes.

Think on which routers you must specify and apply the route-maps (and over which BGP session or sessions) to obtain the required result (you can use the fact that the default value of Local Preference attribute is 100). Place the relevant configuration snippets in the report.

To prove that the Local Preference is working, repeat the **traceroute** command from router R1 to the loopback 1 of R4 (note that it can take some time to propagate changes in the inter-AS routing). Copy and paste the output of the traceroute command to the report.

II. TASK D2 (address aggregation)

Configure router R5 such that it advertises an aggregate /21 prefix covering both L1 and L2 subnets. Check the routing tables and the content of BGP database on all routers. *Copy and paste the content of BGP database on R3 to the report.* Execute *traceroute* to R5 L1 from R1 using R1 L1 as the source address. *Copy the result of this command to the report.*

III. TASK D3 (Path Prepending) - OPTIONAL

Modify the aggregate address advertisement on R5 using path prepending such that the inbound traffic to AS500 (packets destined to R5 L1 and L2) will come from AS400. Copy the relevant R5 configuration snippet to the report. Check the BGP database entries on all routers. Copy the content of the BGP database from R3, paste to the report and explain in the context of actions executed on R5. Execute *traceroute* from R1 to R5 L1 using R1 L1 as a source. Copy and paste the result of this traceroute to the report and explain.

3E. 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: SIP_2020L_Kowalski.zip).

Please note that the clarity of the report will also contribute to your final score.

4 DOCUMENTATION

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

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