Institute of Telecommunications
Faculty of Electronics and Information Technology
Warsaw University of Technology, Nov 2021

IP LAB EXERCISES

LAB EXERCISE – EGP ROUTING – BGP

1. PURPOSE AND GOALS

BGP 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. 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.

A. 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! It is advised to study the additional Cisco routers documentation available on 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.

B. EXERCISE

Skip this point if you have already installed the Oracle VirtualBox software and downloaded the VM image.

The main exercise is executed using the VirtualBox virtual machine (VM). The VM image in .ova format is available for download from the Microsoft Teams group file repository. The virtual machine hosts the GNS3 application with the pre-configured lab network setup. The environment emulates Cisco routers, and so the router operation system is IOS.

To execute the lab, you need to download and install the following free software:

- Oracle VirtualBox and VirtualBox Extension Pack, both available for download at https://www.virtualbox.org/wiki/Downloads

The guide to running the virtual router lab can be found in Section 3. The tasks required to pass the exercise are described in detail in Section 4.

C. FINAL REPORT

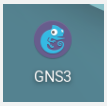
The last phase consists of lab report preparation. The report should contain the findings collected during the main practical part. This instruction will provide the questions and remarks as a guideline for the mandatory content of the report. Please make sure that you paste all required screenshots 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 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 console output from all routers' terminal windows. The archives without these files will be rejected.

3. USING THE VIRTUAL LAB ENVIRONMENT

1. Download the GNS3 project file prepared for this lab from the Microsoft Teams group file repository and copy it to the VM. Some of the ways to do this include:
    a. using the Shared Folders set in virtual machine settings (doesn't always work)
    b. copying the project file to pendrive and attaching the pendrive in guest system (the pendrive should appear as icon on the desktop)
    c. copying the project file to your private cloud storage (Google Drive, OneDrive, Dropbox …) and accessing it from within the VM
2. Run the virtual machine with GNS3 emulator. After seeing the desktop, start the GNS3 application by clicking on the GNS3 icon displayed on the desktop. Ignore the message about running the GNS3 application as root.



3. Import the GNS3 project using the "File / Import portable project" option. For each project, navigate to the folder where you have downloaded the project file and import it to GNS3.
4. After the project has loaded start the routers by clicking the "Start" button . Confirm that you want to start all routers and wait a few minutes until the routers boot (the network topology on the image below may be different from the actual project topology).

4. LAB EXERCISE

The topology of the network emulated in the virtual environment is shown in Figure 1. All emulated routers are Cisco 3745. The experience of configuring the routers running within the virtual environment is indistinguishable from configuration of actual devices via typical ssh console access.

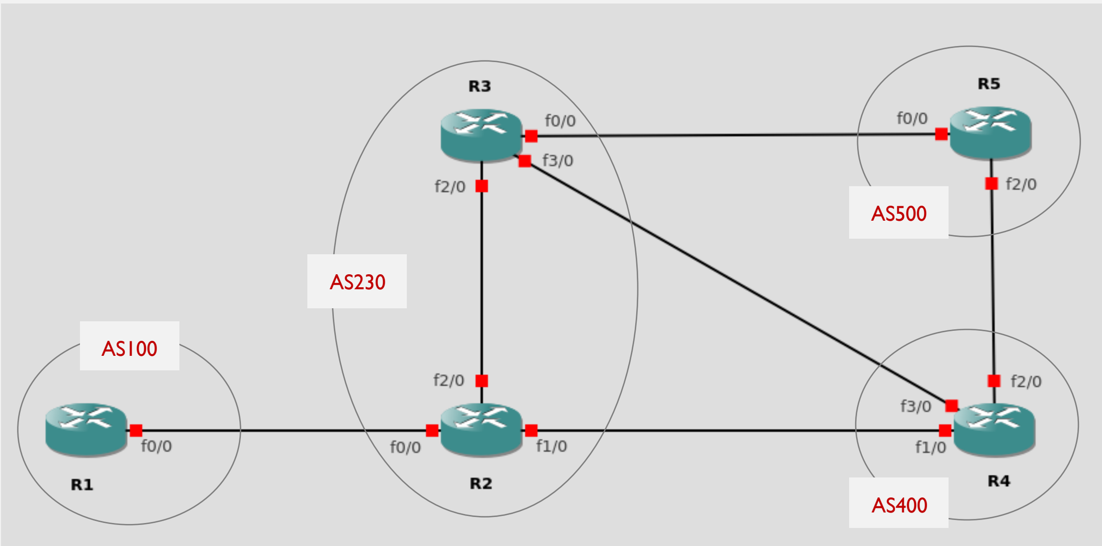


Figure 1. Router Lab configuration

The lab exercise itself is divided into three main parts:

- Preparation of IP address assignment for the network
- Configuration of OSPF protocol between R2 and R3
- Configuration of BGP peering and basic routing policies

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) perform the route-refresh by soft reset, using:
`clear ip bgp <neighbor address> soft`
this method is selective, keeps the TCP session up and just refreshes any routing changes.

A. 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.

The IP addresses are already assigned to all routers' interfaces, in accordance with the lab topology presented in Fig. 1, and the following scheme:

- Subnet address for a link between R*X* and R*Y* (where *X*<*Y*) is 10.0.*XY*.0/30; interface address for R*X* is 10.0.*XY*.1, for R*Y* is 10.0.*XY*.2
- AS numbers and loopback interface addresses are assigned according to the following table.

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
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

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

B. OSPF 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.

C. BASIC BGP CONFIGURATION

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 neighbours. Notice that there is no automatic discovery of the neighbour routers in the BGP protocol. Neighbours must be configured manually by the network administrator. You can configure the BGP neighbour 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 neighbour router. You can use the IP address of the neighbour router's interface. The second parameter is the AS number of the neighbour router (the AS system to which the neighbour 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 neighbour. 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 neighbour router while the <interface> parameter specifies the source interface for the BGP session with this neighbour. This command is typically used when you use loopback interfaces as the neighbour addresses or in case the BGP routers are multi-homed.

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.

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.

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 the network represented by the R3 loopback 1 interface to the BGP protocol using the network command described above. *Add the network represented by the R1 loopback 1 interface to the BGP protocol* in the same way. Check if these networks were successfully advertised by analyzing the routing tables of R1, R2 and R3 – recall the following commands:

show ip route (displays 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.

*Change configuration of router R2 to fix the problem identified above using an **appropriate configuration command**.*

Check the content of the routing table of R3 again, place the result to the report and explain the change. Confirm the reachability of R1 L1 from R3 using ***ping*** command with source address set to R3 L1 (check and explain why ping without source parameter does not work).

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.

TASK C5

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

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 why the route does not transit AS230. *Configure router R3 appropriately to advertise a reachable next hop towards R2.* Check the traceroute again and compare. Place the result of the trace in the report.

TASK C7

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 neighbouring 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 the R4 will leave AS 230 through the 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 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.

D. CLOSING REMARKS

Before closing 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: EINTE_2021Z_Kowalski.zip).

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

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. If you want to restart the routers just stop them and then start again using the GNS3 "Start"/"Stop" buttons. Note that all configurations not saved to the startup-config will be lost.