Institute of Telecommunications
Faculty of Electronics and Information Technology
Warsaw University of Technology, November 2019

EINTE LAB EXERCISES

LAB EXERCISE – EGP ROUTING - BGP

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.

A. PREPARATIONS

The preparations are crucial to the successful execution of the main exercise. Without proper study there is no possibility to fulfill 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.

B. EXERCISE

The main exercise is executed using the VirtualBox virtual machine available for download from the course web page.

The virtual machine (VM) runs the router emulation environment configured such that the individual router consoles are accessible via telnet service on specific TCP ports. The 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.

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
- MobaXTerm terminal for Windows, available at https://mobaxterm.mobatek.net/download-home-edition.html

The guide to running the virtual router lab can be found in Section 3. Note that if you already have the VM downloaded and installed (e.g. from previous lab exercise), you can skip the entire 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. 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.

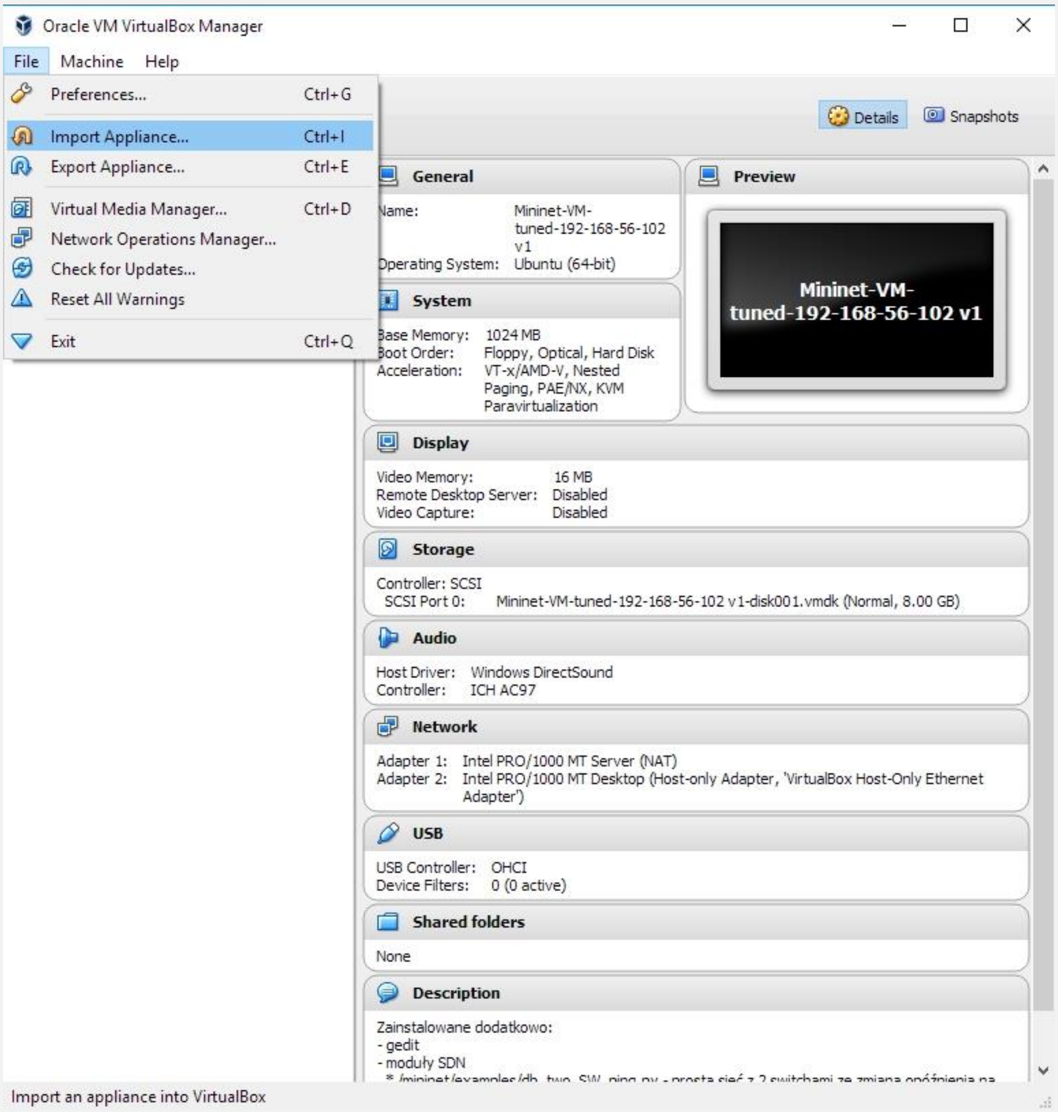
All phases of the exercise and your findings collected during the main practical part should be documented in the report. This instruction may also contain questions and remarks (usually marked with distinct colour) that shall be answered or considered in the report. Finally, you should attach the configuration files (running configs) from all routers with the final configurations that you have prepared during the 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.

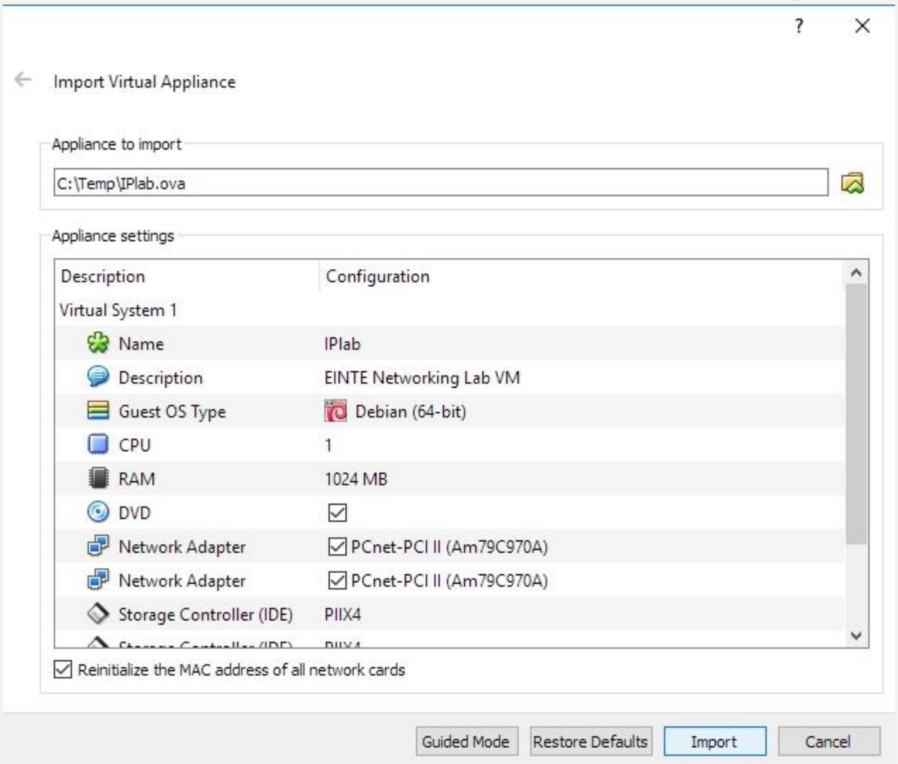
3. USING THE VIRTUAL LAB ENVIRONMENT

After downloading and installing the software indicated in Section 2B on your local PC, the following steps are necessary to run and use the virtual router lab environment.

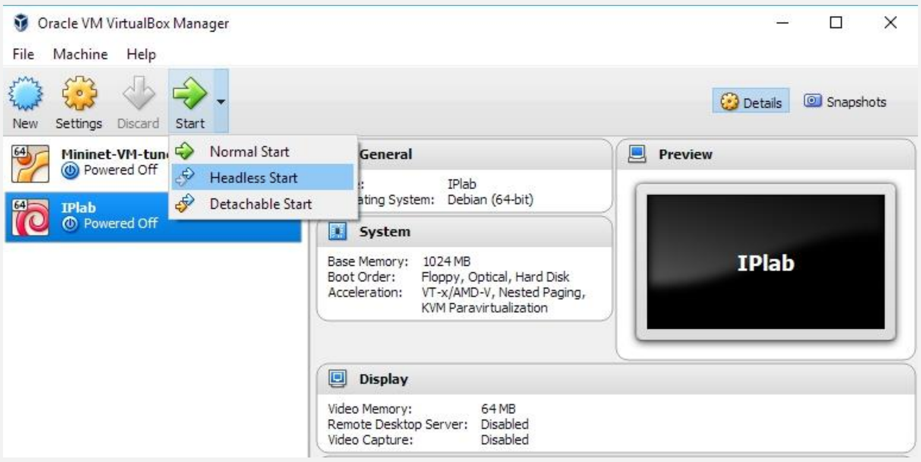
1. Run the VirtualBox and select File/Import Appliance from the main menu



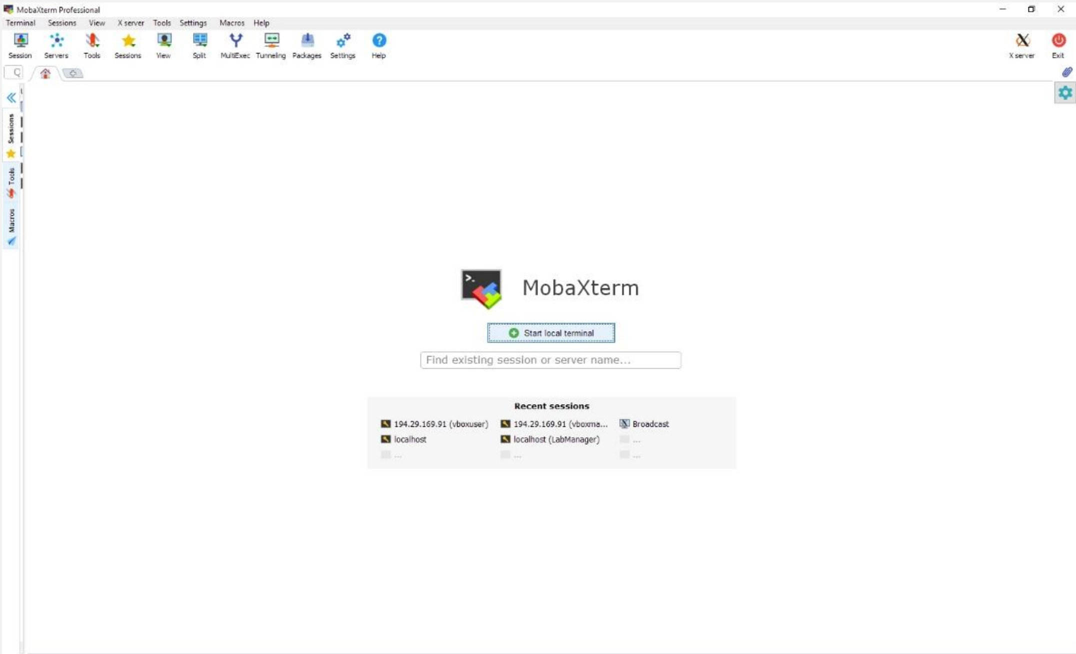
2. Select the downloaded EINTE IP Lab virtual machine (in example below the name is IPlab.ova), check the "Reinitialize the MAC address of all network cards" checkbox and click the "Import" button.



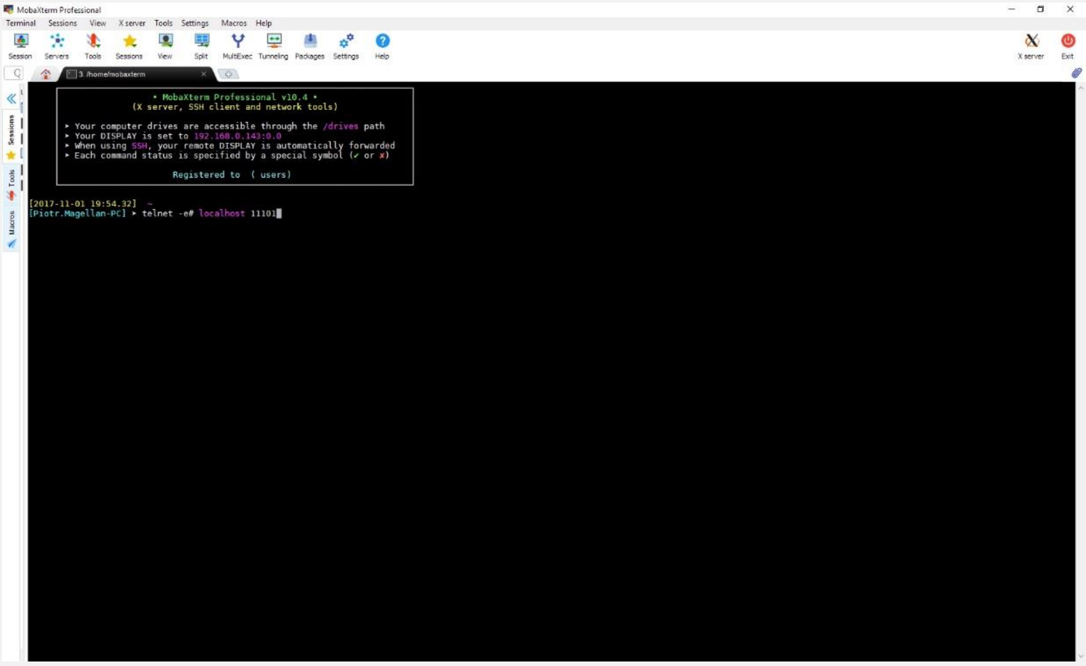
3. After the IPlab VM (Virtual Machine) is imported, select it on the panel, click the right side of the "Start" button and select "Headless Start" from the drop-down menu. The VM is based on Debian linux without any graphical interface, and needs about one minute to fully boot (optionally, you can observe the boot process by selecting the "Show" button, available after the VM is started – this will open the separate window with the VM). <u>Note: there's no need to log in to the VM – you just need to start it.</u>



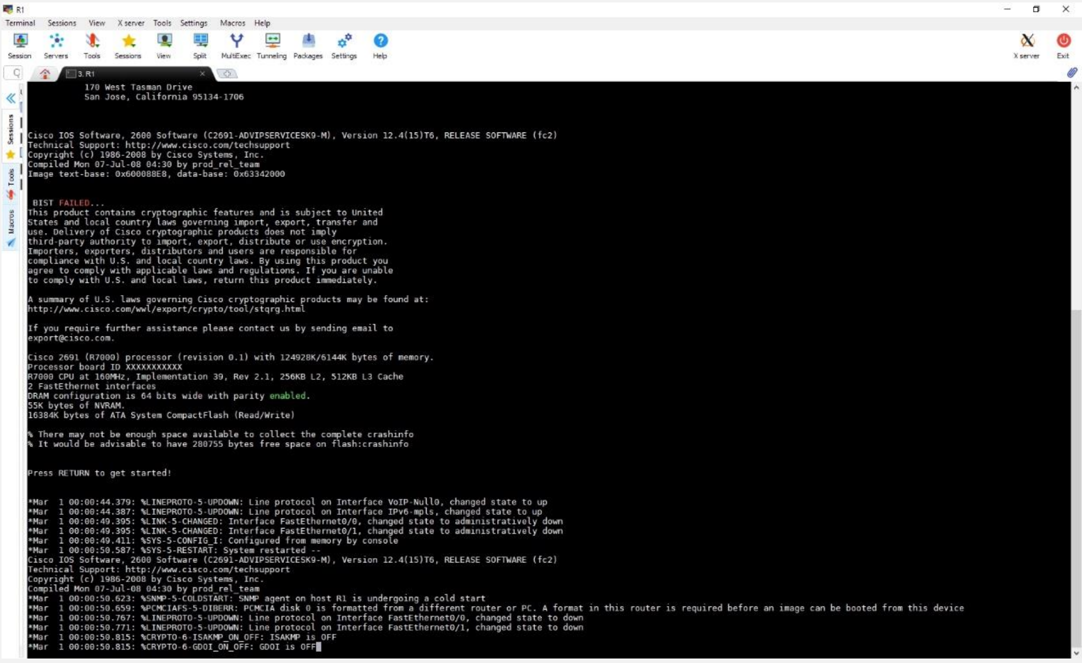
4. Start the MobaXTerm software and click the "Start local terminal" button – this will open the terminal first tab .



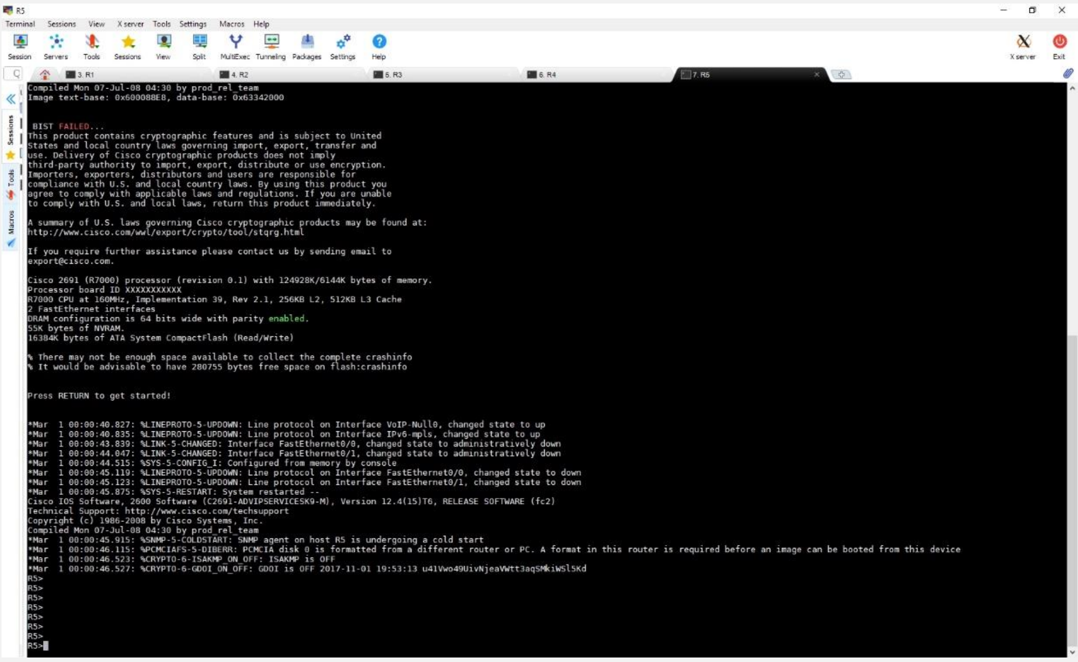
5. In terminal window, run the following command: `telnet -e# localhost 11101`



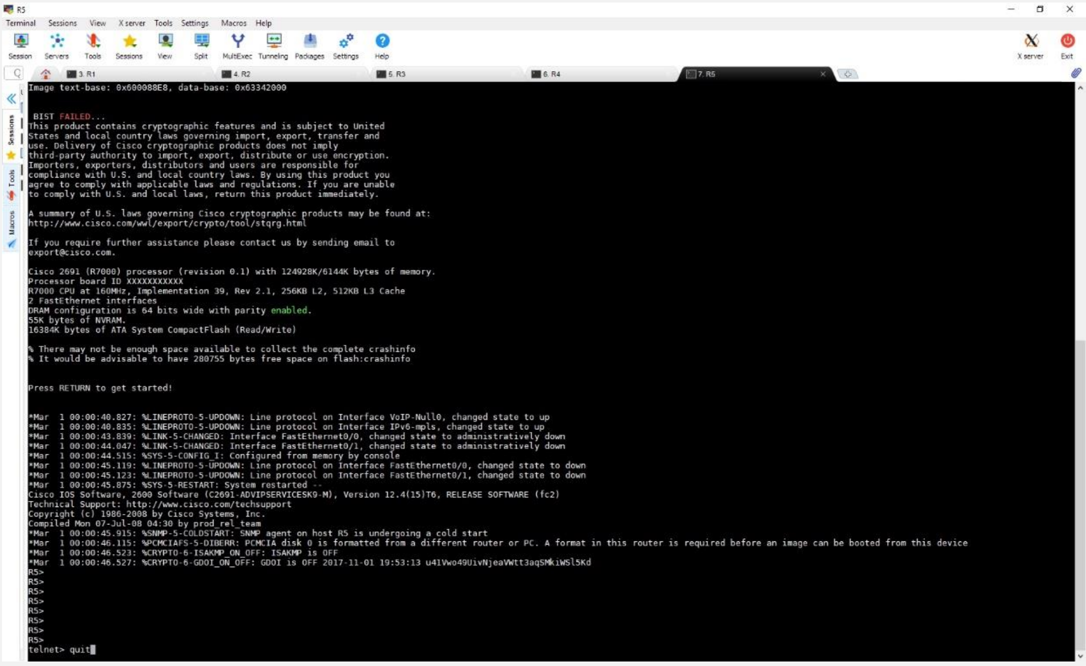
This should provide access to the console of router R1 – you should see the boot process of the router:



6. Open the second tab by clicking on the "+" sign on the right of the first tab. This will open the second terminal tab. After typing the following command: `telnet -e# localhost 11102` you should see the console of router R2.
   Repeat this step, opening three more tabs for routers: R3, R4 and R5, changing only the port number in `telnet` command to 11103, 11104 and 11105, respectively.



7. After the routers end the booting process (typically 1-2 min), the Cisco IOS command line interface will be available on each tab to configure the routers according to the requirements of the exercise.



If you want to close any of the terminal sessions, the best way is to press # (the "escape" sign defined for the telnet session in invoking command) and type "quit" after the "telnet" prompt appears.

Important remarks:

- To save all the text appearing on the terminal tab, select the "Terminal/Save terminal text" from the main menu. You can save the terminal text even after the terminal session is torn down, provided that the session tab is still opened. <u>Note that you must do such save for each tab (router console) separately at the end of the exercise, as it is required to attach the saved files to the report archive.</u>
- After finishing the exercise, close the terminal sessions and power off the virtual machine selecting the "Machine/Close/ACPI Shutdown" from the VirtualBox menu.
- You can save the state of the VM using "Machine/Pause". Even after closing the VirtualBox, the VM state can be restored afterwards. However, the opened terminal sessions will be closed.
- <u>If you close (power off) the VM, at the next power-on all virtual routers will be fully reset to base configurations</u> (no routing protocol enabled, no IP addresses assigned to interfaces etc.).

4. LAB EXERCISE

The topology of the network emulated in the virtual environment is shown in Figure 1. All emulated routers are Cisco 2691. The experience of configuring the routers running within the virtual environment is indistinguishable from configuration of actual devices via typical ssh console access.

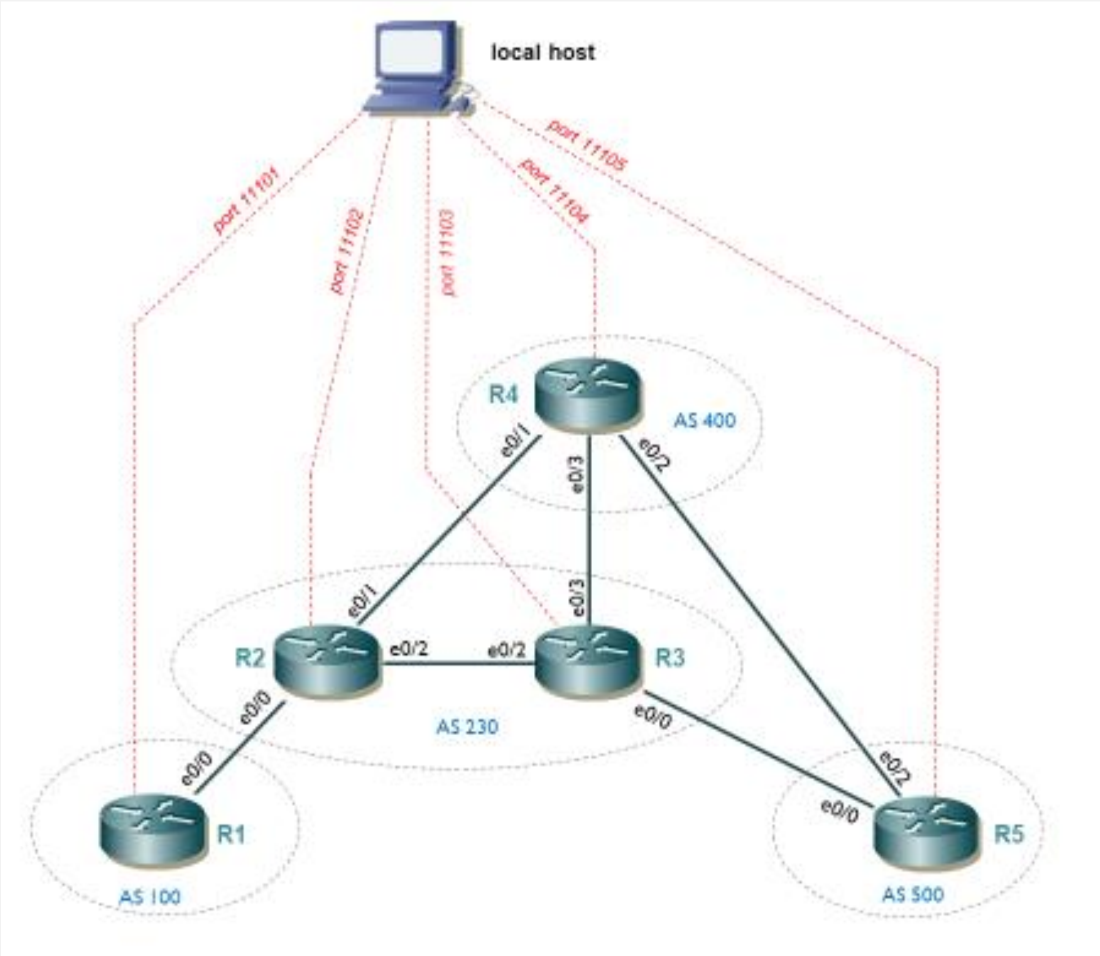


Figure 1. Router Lab configuration

The lab exercise itself is divided into 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) 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.

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). Write all the details of network addressing in your report.

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
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>

Hint: You should plan the addressing scheme during preparation phase. You should end this step with IP addresses configured on all routers' interfaces.

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.

B. 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 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 (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 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 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 network represented by the R1 loopback 1 interface to the BGP protocol using the network command described above. Check if the network you have entered to the BGP protocol is present in the R2 and R3 routing tables 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 override the next hop in the iBGP advertisements with its own address. Use the following command:

neighbor <ip address> next-hop-self

Check the content of the routing table of R3 again, place the result to the report and explain the change. Now check if the advertised network (loopback 1 of R1) is accessible from R3 using ***ping*** command. Explain why the ping does not work even if the address is now present in the routing table of R3 (think of how the ping service works in both directions). What should be done to make this command work? Implement the solution and place the result of the successful ping in the report.

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.

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 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. Check the traceroute again and compare. Place the result of the trace in the report and explain the difference.

D. ADVANCED BGP CONFIGURATION

If you continue the lab exercise from section C in a single go, please follow the tasks described below. 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.

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 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 the traffic sent from R1 to the R4 will leave AS 230 via interface f0/0 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 AS2 to AS4 to be routed through the interface f0/0 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.

TASK D2 (MED – MULTI-EXIT DISCRIMINATOR)

Unlike the local preference attribute that controls how the traffic leaves the AS, the MED attribute controls how the traffic enters the AS. MED (also called metric) is exchanged between autonomous systems and allows to inform the other AS which path it should use to enter given AS (lower MED value is preferred; the default in Cisco IOS is 0). Note however that the BGP attributes are checked in specific order that defines which attributes are preferred over the other.

First, disable Local Preference configuration in AS230 (it may require refreshing the relevant BGP sessions). Then, configure AS400 in that way that the traffic sent to subnets L2 and L3 will enter the AS400 via f0/0 of R4 (for L2) and f0/1 of R4 (for L3). The ***traceroute*** command with the **`source`** option can be used to emulate sending traffic to subnets L2 and L3 respectively. Execute this command from router R1 and check the effect of setting the MED attribute.

To configure the MED attribute, you must define two access lists (prefix filters) on router R4 (one for each loopback interface mentioned above) using the following command:

access-list <number> permit <address> <wildcard mask>

The <number> parameter is the number of an access list (numeric). The <address> parameter is the IP address used to define the access list matching criteria (in your case, it is the IP address of the loopback interface L2 or L3). The <wildcard mask> is like the regular IP mask. It specifies which part of the IP address is used for comparison (0 the bit is used, 1 otherwise).

The exemplary access list is defined as follows (the first three bytes of the L0 interface will be used for as example) – note that you will use interface L2 and L3 for defining access lists:

access-list 10 permit 192.168.41.0 0.0.0.255

To set the MED attribute of the BGP session you must create a route-map (similarly as in case of local preference):

route-map <name> permit <number>

assign the access list to the route map:

match ip address <number of access list>

and use the ***set metric*** command to define the MED value:

set metric <value>

The final step in configuring MED is to assign route maps to the BGP session:

neighbor <neighbor address> route-map <name> out

You must create and assign two route maps (possibly with more than one clause): one to the BGP session between R4 and R2, and one to the BGP session between R4 and R3. Each route map must be related to the appropriate access list (as stated above).

Explain in the report how you have configured R4 to obtain the requested result. Provide the relevant snippets of the configuration. In addition, execute the ***traceroute*** command between routers R1 (source loopback 1) and R4 (destination L1, L2 and L3) to prove that the configuration is working as intended. Copy and paste the output of the traceroute command to the report. Explain the result that you observe from the traceroute to loopback 1 of R4.

E. 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 (see remarks at the end of Section 3).

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

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, or reboot the Virtual Machine hosting the IP Lab environment to reset all routers to initial state.

5. APPENDIX – INTRODUCTION TO CISCO IOS

The routers used in the lab exercise run Cisco IOS. There is an abundance of in-depth information related to the IOS in the Internet, so here only a very brief introduction is given.

IOS is the Cisco routers' operating system. You control IOS, and thereby the router, using IOS command line interface, in short – the CLI.

A. COMMAND COMPLETION AND HELP

In most cases it is not necessary to write the IOS commands in full. As soon as there are enough characters so that the CLI can differentiate between commands available in the specific context, you can stop entering characters.

If you are not sure which commands are available you can always enter a **?** sign for help. This is also true if you want to check subcommands.

You can also use the TAB key for command completion.

B. MODES

IOS has several command levels or modes. Depending on mode you can use different commands. When you connect to a router you enter the EXEC mode. The command you will use most in this mode is the show command. In EXEC mode the command prompt ends with a >

R1>

To be able to control the router you must change the mode to PRIVILEGED. You can do this by entering the enable command in EXEC mode. In the PRIVILEGED mode the command prompt ends with a #:

R1#

You can return to EXEC mode from PRIVILEGED mode with the command exit.

Another mode is the CONFIG mode (see subsection D).

C. CONFIGURATION

The router has two configuration storages. The first one is the ***startup-config***. This configuration is stored in non-volatile memory and is read into ***running-config*** memory when the router starts up or reboots.

The ***running-config*** memory contains is the configuration that is used when the router is up and running. When you are in CONFIG mode and enter configuration commands you change the ***running-config*** immediately, thereby changing the behavior of the router. You can copy the ***running-config*** to ***startup-config*** memory by using

copy running-config startup-config

Doing so at the beginning of the exercise will create the ***startup-config*** and allow reverting to the initial state by typing:

configure replace nvram:startup-config

The following should also work:

copy startup-config running-config

Note! *Do not use the **reload** command to revert to the default configuration as you will lose access to the router console afterwards.*

D. THE „CONFIGURE" COMMAND

To enter CONFIG mode, you issue the ***config*** command. This command takes parameters, and in our case, you want to enter configuration commands from the terminal. So, the command should be ***configure terminal*** or in short just ***conf t.***

Once in CONFIG mode remember that each configuration command you enter is activated immediately. It is easy to cut off the branch you are sitting on, then. In our lab, though, you are accessing the router via the console port which is very hard to shut down.

Each function in the router can be set or unset. To set a function you just use the specific configuration command. To unset a function, you write **no** in front of the same command. All functions have a default status, for most of them this state is unset. The default state is not printed in the configuration listing. So those few commands that have the state set as the default state, you will not see in the configuration print out. They will only be listed if you have unset them, that is they will show in the listing with a no in front of them and will be unseen again if you activate that function.

CONFIG mode has several sub modes, for instance the interface configuration sub mode. You enter this mode by typing the interface configuration command:

(config)# interface ethernet 0/0

or in short just

(config)# in e0/0

In configure interface sub mode you can assign the interface an IP address. Use the command ***ip address <ip address> <mask>***. In this sub mode you can also open and close individual interfaces. To close an interface, use the ***shutdown*** command. And in consequence of what was said above, you open an interface with the command ***no shutdown***. You can also create and delete virtual interfaces, so called loopback interfaces, in the configure interface sub mode. To create a new loopback interface just type the configure command ***interface loopback <interface-number>.*** You can exit from CONFIG mode or any sub mode to PRIVILEGED mode by typing ***ctrl'Z***. To exit from a sub mode or from the CONFIG mode use the ***exit*** command.

E. THE „DEBUG" COMMAND

Another nifty command is the **debug** command. In general, it is dangerous to use, since by issuing this command you might end up in a situation where all packets going through the router are displayed on the console terminal. This may have severe impact on the router throughput. <u>Do not use this command in the lab until it is explicitly stated in the lab manual or it is absolutely necessary for troubleshooting.</u> You can debug nearly anything you want, from each single IP-packet to routing announcements sent between the routers. To see the output from the debugging you must direct it to the terminal console that you are connected to. Use the ***terminal monitor*** command. To turn on debugging you issue command ***debug <parameter …>*** . To turn it off it is often best to use ***no debug all***.

F. THE "SHOW" COMMAND

The ***show*** command is the one that you will use the most. All parameters of the router can be inspected with this command. Here are some typical uses of this command that you will need.

show running-config	With this command you inspect the running-configuration. It must be given in PRIVILEDGED mode.
show interface	With this command you inspect the status of an interface. You can enter an interface name if you don't want to list them all.
show IP interface brief	With this command you get a list of all the router's interfaces with IP addresses.
show IP protocol	This command gives you information on parameters and status of routing processes running on the router.
show IP route	You show the router's current forwarding table with this command. If you want to see a routing table for the one of perhaps several routing protocols, use the command ***show ip route <routing protocol>***.
show CDP neighbor	Cisco Discovery Protocol is Cisco's proprietary protocol used to exchange information between Cisco equipment. It allows retrieving information on which neighbors are connected to a device, and some basic information about them. This command is a good way to check your connections. If you add the parameter ***detailed*** as a suffix to this command, you will get a lot of information.

G. THE "PING" AND "TRACEROUTE" COMMANDS

Both ***ping*** and ***traceroute*** are available tools in IOS. In their normal form they take the remote host as parameter. Example:

> ***ping 192.168.101.10***
> ***traceroute 192.168.7.17***

Since a router has several interfaces, i.e. more than one, there is a minor issue here: Which of the several addresses of a router should be used as a source address?

All functions that make use of IP packets, including ***ping*** and ***traceroute***, use the interface closest to the remote host, and therefore the IP address of this interface is used as source address. In our lab we will meet situations where this is not what we want. We might want to check connection with a router loopback interface as source.

In PRIVILEDGED mode you can use the extended version of ***ping*** and ***traceroute***. Just enter the ***ping*** or ***traceroute*** command without any parameters, and you will have several ways to control these commands, like number of packets sent, packet size, and more. Answer ***yes*** to Extended commands question and you will have the possibility to declare source interface or source IP address. In the latter case the IP address must be one of the router's own IP addresses.

H. ADDITIONAL HINTS

- Router interfaces are inactive by default. After proper configuration they must be activated using ***no shutdown*** command.
- Command lines starting from **show** (and ***debug***) work properly only in the PRIVILEGED mode (indicated by the **#** sign next to the router name). However, you can issue these command from CONFIG mode using the ***do*** suffix (e.g. ***do show ip bgp***)
- After configuring a router and routing protocol it is advised to check the validity of configuration by reviewing the config file (***show running-config***) and router's routing table (***show ip route***).