Lab 2: OSPFv2

Or: *Dynamic protocols exist because doing everything manually sucks*

What You Will Do (WYWD):

1. Confirm your understanding of Lab T113 by cabling a given network topology.
2. Complete basic configuration, including loopbacks and vty access for telnet + SSH
3. Configure simple single-area OSPF (using the interface configuration method).
4. Confirm successful OSPF neighbouring.
5. Confirm full end-to-end network reachability.
6. Successfully book and use a NetLab session to repeat this lab's OSPF configuration.

Things that you will need to know or learn:

1. Essential device configuration – including basic security, SSH, vty access
2. The 2 key commands for implementing OSPF, using the interface configuration method
3. How to transfer configs between different environments: physical lab, remote access, PT
4. Anything else from Lab 1 that you couldn't do quickly or at all.

What you need to submit and when:

1. Complete the pre-lab quiz on BrightSpace, **before** the start of your lab period.
2. Complete the in-lab part of the exercise (see below), **before** the end of your lab period.
3. Complete “Lab 2 Post-lab” exercise and quiz on BrightSpace, **before** your next lab.

Required Equipment:

- A laptop and/or a USB memory stick to save results for post-lab questions
- **Hard-cover lab notebook**, for reference during **SBA** at the end of the course.

In-Lab Marks:

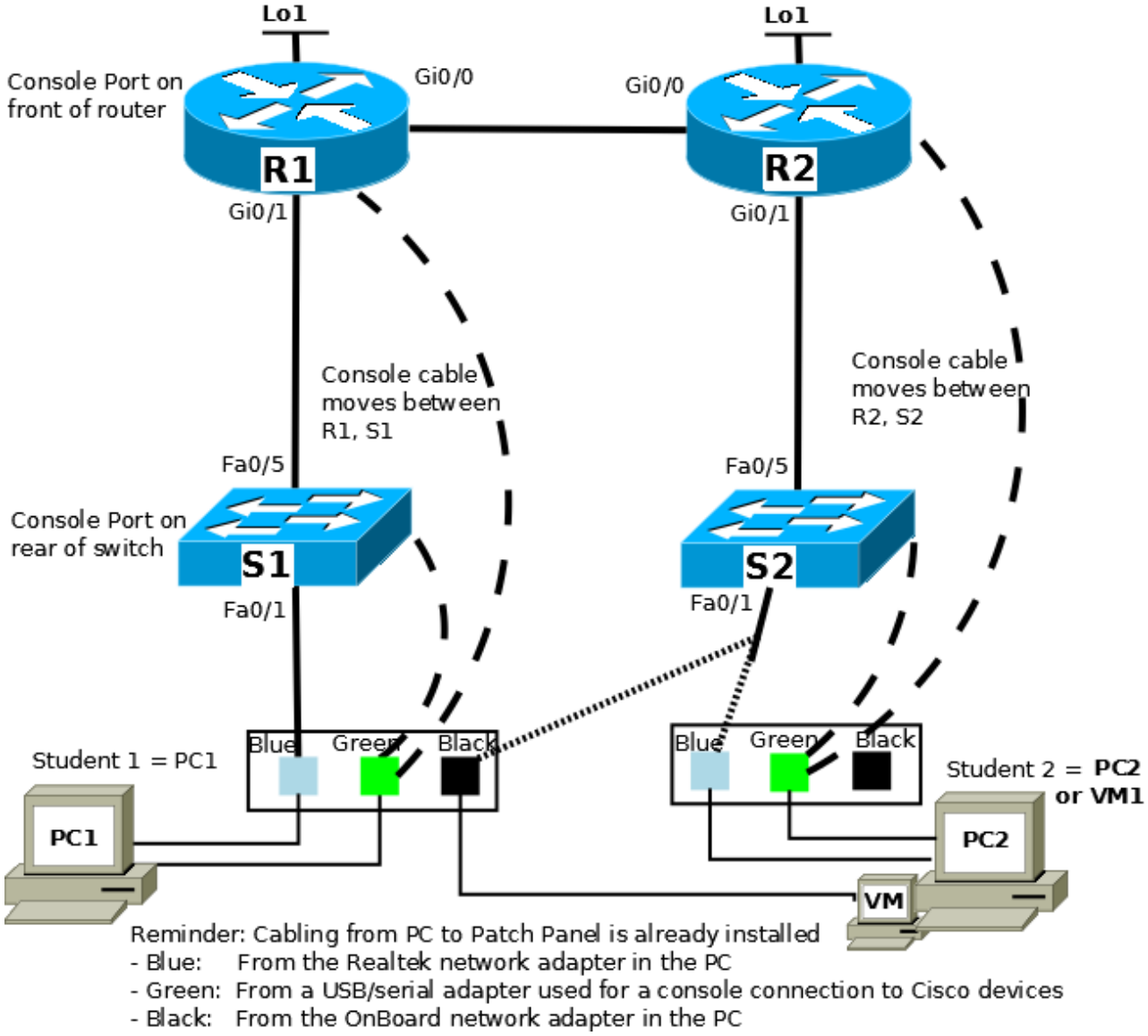
[1 mark] Separate, full connectivity within each of the left, right sides
[1 mark] OSPF neighbouring, with suitable "show" commands to provide proof
[1 mark] Full end-to-end connectivity throughout your entire network.
~~[1 mark; Bonus] Demo full OSPF neighbouring in a NetLab session~~

The pre-lab is worth **33%**, the in-lab is worth **33%**, and the post-lab is worth **34%** of this lab, even though the number of points may differ between two parts.

References and Resources:

- All the materials used in your previous networking courses, including https://netacad.com
- Packet Tracer ver 8 (available from NetAcad)
- Algonquin's NetLab facility – http://netlab.algonquincollege.com

Lab 2 – Topology Diagram and Addressing Table



Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway
R1	G0/0	10.1.2.1	255.255.255.0	–
	G0/1	10.1.1.254	255.255.255.0	–
	Loopback1	1.1.1.1	255.255.255.0	–
S1	VLAN 1	10.1.1.253	255.255.255.0	?
PC1	Realtek	10.1.1.10	255.255.255.0	?
R2	G0/0	10.1.2.2	255.255.255.0	–
	G0/1	10.2.2.254	255.255.255.0	–
	Loopback1	2.2.2.2	255.255.255.0	–
S2	VLAN 1	10.2.2.253	255.255.255.0	?
PC2 **or** VM1	Realtek or Onboard	10.2.2.10	255.255.255.0	?

Task 1: Cable the Network

Cable the devices as shown in the diagram above, to create the required network topology.
Note: If R1-R2 and S1-S2 are being used by another student, please use R3-R4 and S3-S4 instead!

Task 2: Configure basic settings for PCs

Working in pairs, determine whether to use two physical PCs, or only 1 PC with both the real NIC (Realtek) and VM NIC (Onboard). Note that if you choose the 1 PC option, you'll have to shuffle the console cable around for configuring all four Cisco devices; with 2 PCs, there's a lot less shuffling to be done!

Step 1. According to your choice, configure the necessary IP settings: address, mask, and gateway. Note that in this lab we will not be using DNS services.

Task 3: Configure the two Switches

The switches need to be configured along four categories of basic requirements, as listed below.

Step 1. **Fundamentals**: (a) hostname; (b) disable DNS lookup to prevent (long, slow) lookups from incorrect commands; (c) MOTD clearly restricting access to authorized users
Step 2. **Security**: (a) Exec ~~password~~ secret of **cisco**; and (b) console password of **cisco**; (c) ensure plaintext passwords are all encrypted automatically
Step 3. **IP addressing**: (a) VLAN 1 interface; and (b) default gateway according to the addressing table. You need to determine a suitable gateway address!
Step 4. **VTY access** via both SSH and telnet (to eliminate shuffling the console cable in later tasks). (a) SSH requires **5 additional commands** beyond what's already configured, and (b) telnet access requires only that one of those 5 commands is slightly modified.
Step 5. Verify ping connectivity on each side (left, right) between the PC and switch. Troubleshoot as necessary. Verify telnet and SSH connectivity and once successful, ditch the console cable and just use Putty from now on!

Task 4: Configure the two Routers with basics

The routers also need to be configured along the same four categories of basic requirements.

Step 1. **Fundamentals**: (a) hostname; (b) disable DNS lookup to prevent (long, slow) lookups from incorrect commands; (c) MOTD clearly restricting access to authorized users
Step 2. **Security**: (a) Exec ~~password~~ secret of **cisco**; and (b) console password of **cisco**; (c) ensure plaintext passwords are all encrypted automatically
Step 3. **IP addressing**: (a) loopback interface Lo1; (b) Gi0/0; and (c) Gi0/1
Step 4. **VTY access** via both SSH and telnet (to eliminate shuffling the console cable in later tasks). (a) SSH requires **5 additional commands** beyond what's already configured, and (b) telnet access requires a small modification of one of those.
Step 5. Verify ping connectivity on each side (left, right) between the switch and router, then the PC and router. Troubleshoot as necessary. Verify telnet and SSH connectivity; optionally ditch the console cable once successful and just use Putty from now on!
Step 6. When using telnet or SSH, ensure you see log messages: **terminal monitor**
Step 7. Now, most importantly for the next tasks, verify that R1 can ping R2.

CHECK POINT #1: Have Putty windows open showing telnet/SSH from the PC to router.

Task 5: Configure simple, single-area OSPF

These next tasks **will NOT WORK** if the above tasks are not 100% complete!! Do not proceed unless you have full connectivity throughout each of the right and left sides.

There's really only 1 single command, or at most 2, to *configure* single-area OSPF on a router. More interesting though is using show commands to compare before / after and see the results! READ the instructions carefully for each side (right, left) so that you see the differences!

Step 1. On each router, show what (dyamic) protocols are running: (**do**) **show ip protocol** **Record** what, or how much, is output by the command at this stage.
Step 2. On R1 (left side) **only**: enter the OSPF process config context: **router ospf 10** and then exit the context.
Repeat step 1 for *both* routers (show protocols) and **record** the results.
Step 3. On each router, enter the interface configuration context for G0/0 and configure it as participating in OSPF: **ip ospf 10 area 0** and *quickly* repeat step 1; **record** the results.
Step 4. After at least 30 secs has passed, note any console messages that appeared.
Step 5. Repeat step 1 and **record** the results.
Step 6. Examine all the output and generate some conclusions: two similar, but not identical configuration sequences were completed. Was the end result the same? What is the absolute, bare-bones, minimum number of different commands that are needed for OSPF?

Task 6: Confirm OSPF operation

Verifying OSPF (e.g. for troubleshooting purposes) can be done by showing three aspects: the participating interfaces, valid neighbours, and OSPF routes appearing in the routing table.

Step 1. On each router, verify the status of G0/0 in OSPF: **show ip ospf interface g0/0**
Step 2. On each router, prove that you have an OSPF neighbour: **show ip ospf neighbor**
Step 3. On each router, prove that OSPF is sharing topology info: **show ip ospf database**

... Is it necessary to repeat that you should **record** your results??

CHECK POINT #2: Have putty windows open, showing the interface, neighbours, and database

Task 7: Extend and verify full end-end connecitivity

Hmm. We configured loopbacks early on. Are they participating in OSPF? What's necessary to make them reachable from everywhere? Do it! Hint: we've only used 1-2 OSPF config cmds! Now what about G0/1 interfaces in each router? Test to find out if they need to be included too.

CHECK POINT #3: Have CMD windows showing pings to the loopback on the opposite side.

Task 8: Repeat on NetLab

Get a head start on the post-lab: if you have time remaining, you can get a bonus mark by repeating all this on Netlab. How about copying & pasting some of the configs to save time??

~~**BONUS CHECK POINT**: Demo OSPF working between R1 and R2, including loopbacks.~~

Task 9: Clearing the equipment

Hopefully you know how to clear Cisco equipment, but just in case:
Router: **`erase startup-config`** Switch: **`erase startup-config`** then **`del vlan.dat`**