Lab 1: Lab Fundamentals

Or: A 3 Hour face-to-face Intensive about Real equipment, Real networks

What You Will Do (WYWD):

1. Learn the setup of the Lab room (T113 or T108): lab cabling, access switches, control PCs
2. Confirm your knowledge of network cabling: recognition and use of each the 3 types.
3. Confirm your ability to identify equipment based on its physical characteristics.
4. Cable & boot up all the required equipment and resolve any startup issues.
5. Complete the configuration for basic connectivity for a router & switch to the remote server.
6. Capture and submit configs and other device details.
7. Demo your ability to use and understand the output of basic network monitoring tools: wireshark, ping, traceroute, DNS lookup.
8. Demo, in the three previous steps, your ability to **work in a shared environment**!!!

And in the Post-Lab:

9. Demo knowledge of using ping results to identify a host's OS type.
10. Confirm you have a up-to-date, working installation of PT (e.g. at least ver 8.01 or higher)
11. Confirm that you can access Algonquin's NetLab facility

Things that you will need to know or learn:

1. Essential device configuration – hostname, MOTD, Loopback/Vlan1, *basic security* , IP
2. The purpose and value of loopback interfaces.
3. Designing and implementing default and static routes for small or stub networks
4. The HUGE importance and value of validating full network connectivity.
5. How to capture configs and CLI output
6. Understand how ping and traceroute work, key differences, and what they can tell you.

What you need to submit and when:

1. For week 1, there is *no* pre-lab to be done on BrightSpace, **before** your lab period.
2. Complete the in-lab part of the exercise (see below), **before** the end of your lab period.
3. Complete "Lab 1 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] Demo of full, end-to-end network connectivity [Checkpoint **A]**
[1 mark] Config files saved to the TFTP server, with **correct** file names
[1 mark] Demo that your lab equipment is clear of any configs [Checkpoint **B**]
[1 mark] Zip file of configs, **all** correctly named, submitted on BrightSpace

The in-lab is worth **50%**, and the post-lab is worth **50%** of this lab, even though the number of points may differ between two parts. (The pre-lab is weighted at **0%** because there is none.)

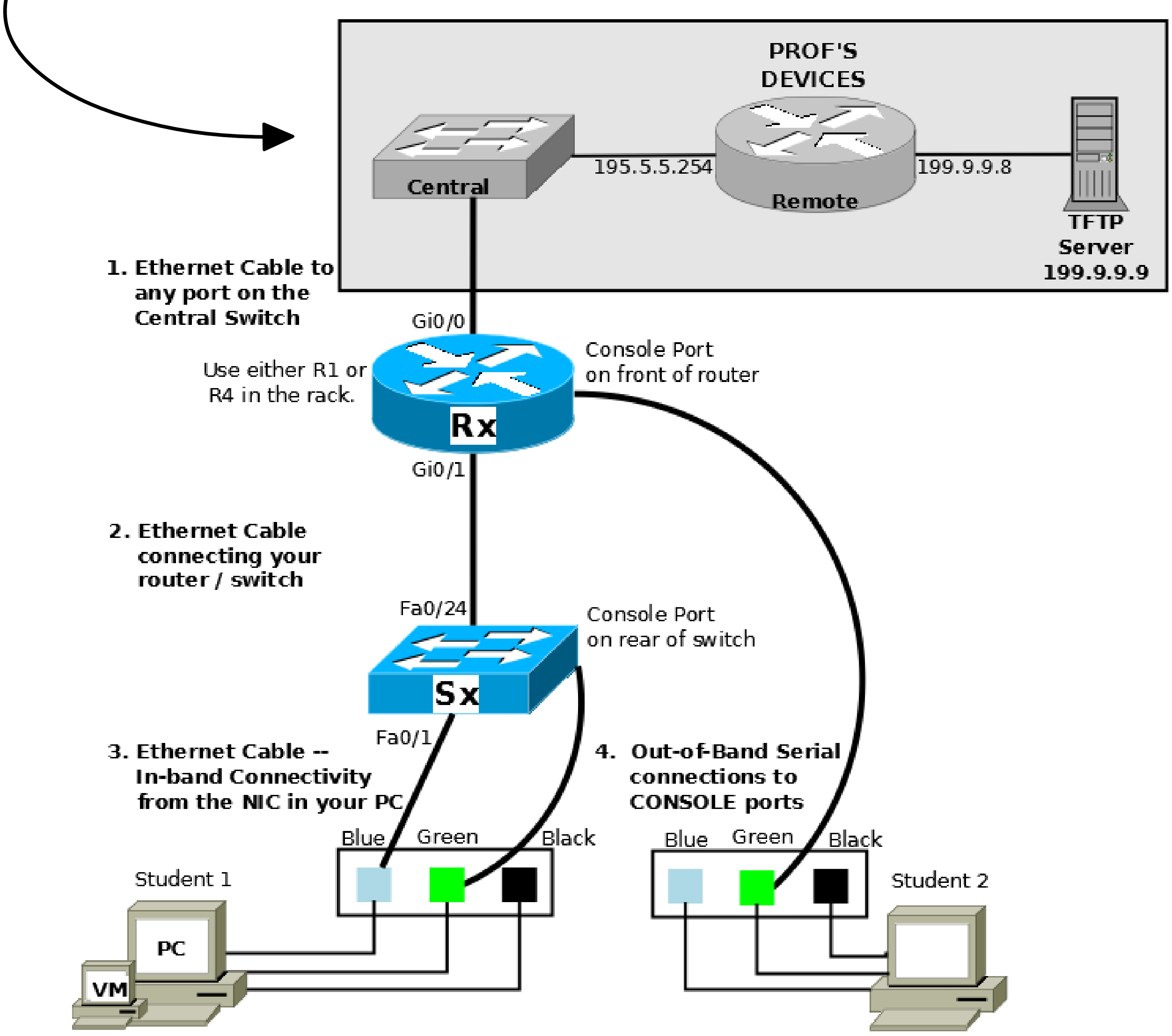
References and Resources:

- Information page on three types of network cables (see last page)
- All the materials used in your previous networking courses, including https://netacad.com
- Packet Tracer 8.0.1 (available from NetAcad)
- Algonquin's NetLab facility – http://netlab.algonquincollege.com

Lab 1 – Topology and Addressing Diagram

N.B. For the Central switch, the red cable connects to the:

College internet	= 🟥	**red jack**
Class network	= 🟨	**yellow jack** (This is what we will normally use.)


PROF'S DEVICES
Central
195.5.5.254
Remote
199.9.9.8
TFTP Server 199.9.9.9
1. Ethernet Cable to any port on the Central Switch
Gi0/0
Use either R1 or R4 in the rack.
Console Port on front of router
Rx
Gi0/1
2. Ethernet Cable connecting your router / switch
Fa0/24
Console Port on rear of switch
Sx
Fa0/1
3. Ethernet Cable -- In-band Connectivity from the NIC in your PC
4. Out-of-Band Serial connections to CONSOLE ports
Blue
Green
Black
Blue
Green
Black
Student 1
PC
VM
Student 2

Cabling from PC to Patch Panel is already installed:
- Blue: From the Realtek network adapter in the PC
- Green: From a USB/serial adapter used for a console connection to Cisco devices
- Black: From the OnBoard network adapter in the PC

Device	Interface	Address	Gateway
RA	Gi0/0	195.5.5. **U** /24	N/A
	Gi0/1	201. **U** .1.254 /24	N/A
SA	SVI Vlan 1	201. **U** .1.250 /24	
PC (student 1 only)	Realtek NIC	201. **U** .1.10 /24	
VM (student 1 only)		201. **U** .1.11 /24	
where **U** = your workstation number			

Task 1: Orientation to Lab Setup, Cables, Network Switches and Routers

This is a Professor-led group activity. You will be given an orientation to the room and equipment that you will be using for this semester (and next semester too). For convenience, the last page of this lab has summary information on cable types. Finally, there will be a brief discussion on what Cisco defines as "basic security settings" for their network devices. [Ref: WYWD 1-3,5]

Task 2: Cabling and Power-on

Working in pairs, wire up topology given on the previous page. Please note that each student plays a different role in connecting to the Cisco equipment. [Ref: WYWD 4]

Step 1. Cable the equipment, being sure to correctly connect to the Central Switch.
Step 2. On each PC, start a Putty session for the console: e.g.Serial, COM1, 9600 baud
Step 3. Power on your router and switch. Examine the output as the devices power up.
Question: How can you tell whether you're seeing a Cisco switch or a router booting (i.e. an obvious difference, lasting a fair time, and starting from very shortly after power-on)

Task 3: Addressing Scheme and Determination of Gateway

Choose one of the workstation numbers for your pair. Use that for your addressing scheme and amend the chart (previous page). What device / interface will your PC use for its default gateway? Similarly for the VM? Complete the chart with the default gateway address(es).

Task 4: Collecting Information for the Switch

In real-world scenarios, it's important to confirm you're configuring the correct piece of equipment! Gather some basic info about the Switch before starting the configuration.

Step 1. Enter privileged exec mode and **record** the model & IOS version: `show version`
Step 2. Confirm that the PC is correctly connected: `show interface status`
Fa0/1 should show as connected. **Record** the speed, and duplex for Fa0/1.
Step 3. Examine the MAC address table: `show mac address-table`
There should be an extry for your PC. **Record** the MAC stored for Fa0/1.
Step 4. Check for correlations on your PC: `C:\Users> ipconfig /all`
Record the mac-address for the Realtek card.

Task 5: Initial Connectivity between the PC and Switch [Ref: WYWD 5]

Step 1. [PC], configure the Realtek NIC with the address / mask /gateway from your address table, plus DNS server 199.9.9.9
Step 2. [Sw] Config hostname - **you must ALWAYS use this format whenever you are in lab: {Alg-NetID}-S{#}** where: **Alg-NetID** = your Algonquin Network ID; **#** = switch number
Step 3. Configure some basic device security:
– an exec password: **class** – console login password: **class**
– telnet to vty lines using local authentication with a user/pass of **cisco** / **class**
Step 4. Configure the management IP on Vlan 1 as well as the default gateway
Step 5. Now verify your work!! From the PC, ping the switch and then login via telnet.
Troubleshoot the config on your PC and Switch until it's working properly.

Task 6: VM Configuration [Ref: WYWD 5]

You will often use a VM as a 2nd workstation in your topologies. The VM is setup with its network adapter bridged through the 2nd NIC in your PC. This allows the PC and the VM to function as separate workstations.

Step 1. Cabling: The VM ethernet interface is cabled to the black port on the patch panel. Connect a cable from the black patch panel port to any unused port on your switch.
Step 2. In VMWare, start the Win7 VM.
Step 3. Configure the NIC with the address / mask / gateway info from the addressing table, plus a DNS server 199.9.9.9
Step 4. Now verify your work!! From the VM, ping the switch and then login via telnet. Troubleshoot the config on the VM and Switch until it's working properly.

Task 7: Router Configuration

For the Router, be careful to *distinguish* and correctly configure the interfaces! [Ref: WYWD 5]

Step 1. Config hostname - **you must ALWAYS use this format whenever you are in lab:**
{Alg-NetID}-R{#} where: **Alg-NetID** = your Algonquin Network ID; **#** = router number
Step 2. Configure the same basic device security as you did for the switch:
– an exec password: **class**– console login password: **class**
– telnet (and SSh) to vty lines using local authentication with a user/pass of **cisco** / **class**
Step 3. Configure addresses and then activate the two Gigabit interfaces.
Step 4. Verify the addresses showing just the interfaces that are configured:

```
# show ip int brief | ex una
```

Note that "ex una" is an abbreviation for "exclude unassigned".
Step 5. Configure a default route via Remote. Examine the topology diagram to get the next-hop IP address.
Step 6. Proceed to the next Task for testing, verification, and troubleshooting.

Task 8: Connectivity Verification

After ping tests, be sure to test application layer connectivity from Rx, Sx, the PC, and the VM. Do not omit the application layer testing; ping testing is not enough! There might be transmission media which can transmit small ping packets but not session or larger packets. There might be intervening firewalls / translation boxes / filtering devices which are misconfigured. Users on the network will always *need more than just ping*. At each step, stop and troubleshoot your config until you have successful connectivity. [Ref: WYWD 5]

Step 1. Ping tests: ping 199.9.9.9 from (1) Rx, (2) Sx, (3) PC, (4) VM
Step 2. DNS tests: ping www.8315.com from (1) PC, (2) VM
Step 3. HTTP tests: open a browser and connect to www.8315.com from the PC and VM
Step 4. With windows **already open** showing that all tests are successful, put your name on the whiteboard in the *Demo* list. Proceed with the next tasks if you need to wait for the lab Professor.

CHECK POINT A: Demo full, end-to-end connectivity

Task 9: More Testing and Backups of Configs

Backing up your Router and Switch configs via TFTP provides additional testing as well as creating a backup. It's possible that you haven't needed TFTP transfers when working in virtual environments. For that reason, complete command details are provided here. [Ref: WYWD 6]

Step 1. Backup the Rx config via TFTP:

```
# copy run tftp ↵
Address or name of remote host []? 199.9.9.9 ↵
Destination filename [ ]? ↵
```

Step 2. Use the same commands to upload the Sx config to the TFTP server.

Step 3. Verify that your files uploaded successfully. From a CMD window on your PC:
a. **ssh cisco@199.9.9.9** then login with password *cisco*
b. **ls -l /var/tftpboot**
c. exit

Step 4. A. Make local copies of the Router and Switch configs. For each one, make the filename: **{exact-same-as-the-hostname}.txt**.
B. Zip just the files (NOT in a subdirectory!); make the filename **{Alg-NetID}-L01.zip**
C. **Submit the zip file** on BrightSpace **within 2 hrs** of the end of your lab session.

Task 10: [Optional; time permitting]

Ping, traceroute, DNS lookups, and wireshark are generally considered the fundamental network monitoring tools. Some of their functionality is obvious, and other aspects are much more subtle. This task provides some practice in using them and gaining a deeper understanding that will be extremely useful in future courses and career(!) [Ref: WYWD 7]

Step 1. From each of the PC and VM, ping and traceroute to the TFTP server.
a. Compare the results between the PC and VM. Do they differ or are they identical? Why?
b. Are the TTL results identical between ping and traceroute? Why or why not?
This is *really important to note and understand*.

Step 2. From each of the PC and VM, do a DNS lookup for www.8315.com
Hint: in MS-Win use `nslookup` and in Linux or Mac use `host`

Step 3. On either the PC or VM, use wireshark to capture the activity from viewing the site www.8315.com In the capture, how can you determine the TTL of the web host?

BONUS CHECK POINT: Succinctly and correctly explain the results to all three steps to the Prof.

Task 11: Clearing the equipment [Ref: WYWD 8]

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

CHECK POINT B: Demo to the Prof that both the Router and Switch are cleared of all config.

Don't forget to complete the post-lab exercise on BrightSpace!

See you next week in lab. ☺

Cables

Learning Objectives

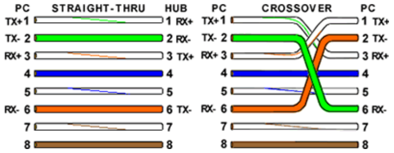
Upon completion of this lab, you will be able to:

□ Correctly identify cables for use in the network.

Cables and more Cables

At the Physical layer (Layer 1) of the OSI model, end devices must be connected by media (cables). The type of media required depends on the type of device being connected. In the lab, you'll find three different types of cables:

Straight-through Cables:
Straight through cable has connectors in each end that are terminated the same in accordance with either the T568A or T568B standards.



Use a straight-through cable for the following connections:

- Switch to router Ethernet port
- Computer to switch
- Computer to hub

Crossover cable:
Directly connects two network devices of the same type to each other over Ethernet.
In this lab, are cross-over cables a specific colour? Is this consistent for all cross-overs?

Use a crossover cable for the following connections:

- Switch to Switch
- Switch to hub
- Hub to hub
- Router to router Ethernet port

Console Cables:
Connects a computer to a Cisco device via the console port. Our rollover cables have DB9 connector at one end and a RJ45 connector in the other end.

Use a console cable for the following connections:

- Computer to a switch console port
- Computer to a router console port

In T108 and T113, the console cable is already attached to the computer
it is plugged in the GREEN connector. You would then cable from the patch panel into the console port of the switch/router with a straight through cable.