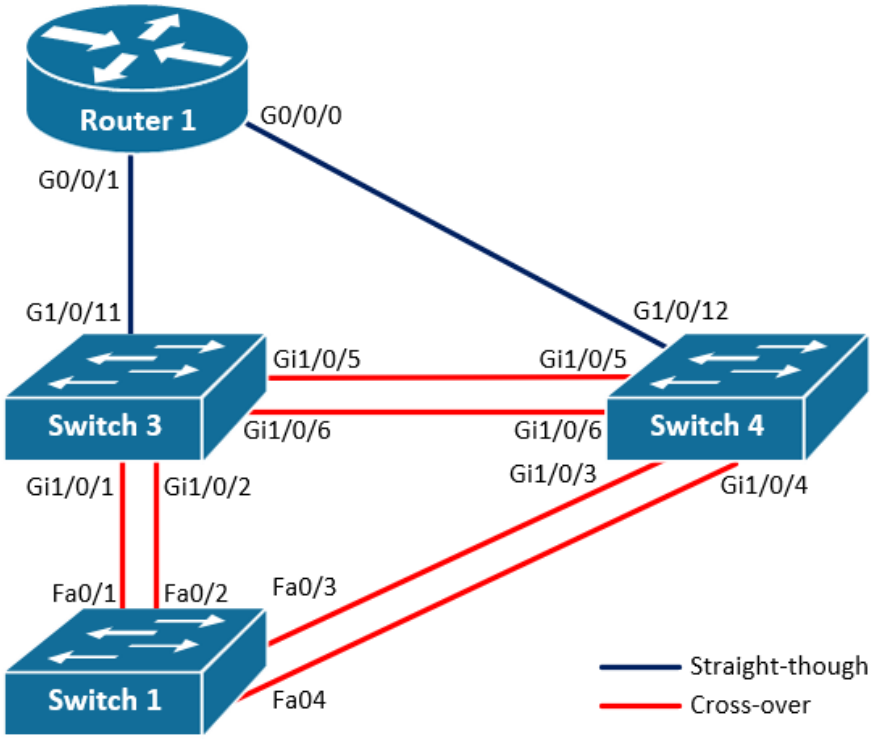
Lab SU-1a – Smart Rack Access and Wiring Scheme

TNE10006/TNE60006 Lab Infrastructure and Wiring Scheme



Objectives

1. **Understand TNE10006/TNE60006 Lab Infrastructure**
2. **Remote access networking lab devices**

Background / Scenario

Swinburne's Cisco Networking Labs are physically located in the ATC building, in rooms ATC328, ATC329 and ATC330. TNE10006/TNE60006 lab sessions run on ATC328 and ATC329. In each of these two rooms, there are five **Enclosures**, in each Enclosure there are five networking **Kits** and each kit is comprised of 8 cisco network devices:

Device Label	Type	Model
Switch 1 (S1)	Layer 2 Switch	Catalyst 2960
Switch 2 (S1)	Layer 2 Switch	Catalyst 2960
Switch 3 (S3)	Layer 3 Switch	Catalyst 3650
Switch 4 (S4)	Layer 3 Switch	Catalyst 3650
Router 1 (R1)	Router	ISR 4321
Router 2 (R2)	Router	ISR 4321
Router 3 (R3)	Router	ISR 4321
Router 4 (R4)	Router	ISR 4321

TNE10006/TNE60006 lab practices require the use of Switch 1, Switch 3, Switch 4 and Router 1.

In each enclosure, there is a **Smart Rack** server that physically connects to the console port of all network devices inside the enclosure. This Smart Rack server allows us to connect to the command line interface of the devices to manage them.

In this lab we will learn how to use the **Smart Rack** system to manage the Cisco devices in the lab, via console. We will also explore how network devices in the same kit interconnect under the generic wiring scheme.

Required Resources

- Personal Computer
- Internet Connection
- Swinburne VPN
- Terminal application

Part 1: The Smart Rack Web Interface

In Part 1, you will learn how to access the Smart Rack Web Interface and book a networking kit.

Step 1: Connect to Swinburne VPN

Note: if you using a computer connected to the Swinburne network, or your personal computer connected to the Swinburne WiFi network, you don't need to complete this step. However, you are advised to complete the VPN installation and configuration process on your personal computer for future use.

The Smart Rack system is only accessible from within the Swinburne network. This means that you must install and configure the Swinburne VPN on your personal computer to access the Cisco Lab equipment from outside campus.

The VPN software and associated support is provided by Swinburne's IT staff, teaching staff cannot provide direct support. To download and install the VPN software go to: https://vpn.swin.edu.au/mfa

Once you've installed the software, you can connect to Swinburne VPN using the following details:

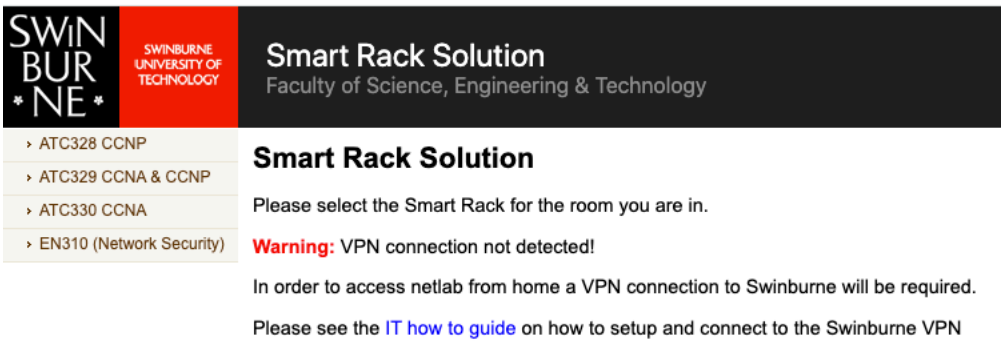
VPN Server Name: vpn.swin.edu.au/mfa
Username: your SIMS username (Student ID)
Password: your SIMS password.

If you are having issues installing the VPN and/or connecting to the VPN, you can contact IT for support at servicedesk@swin.edu.au or on tel:+61392145000

Step 2: Access Smart Rack Web Interface

If you are on-campus, or working remotely and connected to the VPN, you have access to the Smart Rack system. To access the Smart Rack Web Interface, go to: https://smartrack.swinburne.edu.au

Note: If you are working remotely and have not successfully connected to the VPN, you will still be able to access Smart Rack home page, however, a warning is displayed (see below) and you will not be able to go beyond this point.



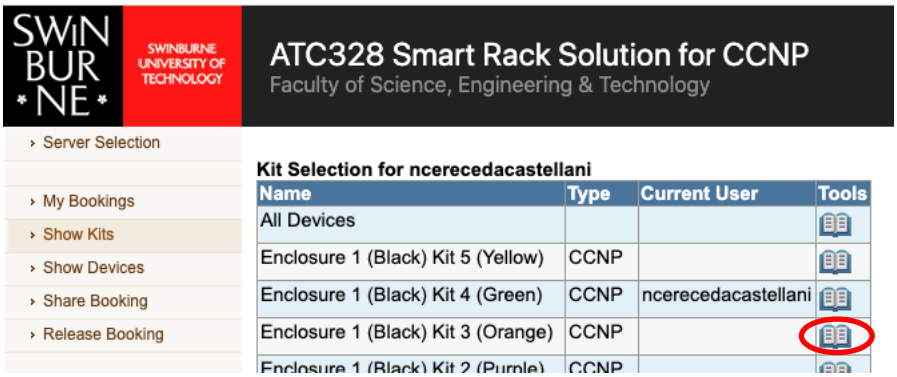
Step 3: Go to Your Allocated Lab Room

Once you are on the Smart Rack web interface, access your allocated lab room, **ATC328** or **ATC329**, by clicking on the room name in the left-hand side menu on the Smart Rack home page.

You can use **ATC330** for practicing outside your allocated lab time, however, be aware that the networking kits in this room have different model devices, with slightly different configuration commands.

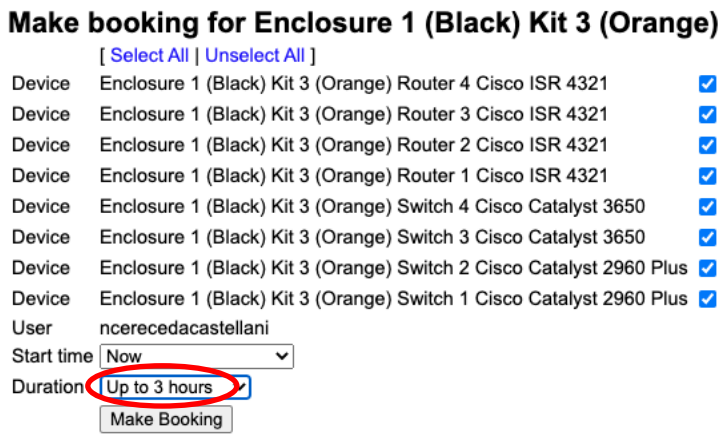
Step 4: Book an Available Networking Kit

Once you are in your allocated lab room, click on the **Show Kits** option in the left-hand side menu. This will display a list of all networking kits in the room. To book a kit, click on the book icon to the right.



Note: If you are **on-campus** you must book the kit specified on your desk label.

Make sure you set the booking period for the duration of the lab session (3 hours). If you fail to do this, a default booking duration of 1 hour will apply. When the booking expires, the devices will automatically power off and unsaved configuration settings will be lost.



Part 2: Connect to the Network Devices

In Part 2, you will learn how to access the console of the networking devices.

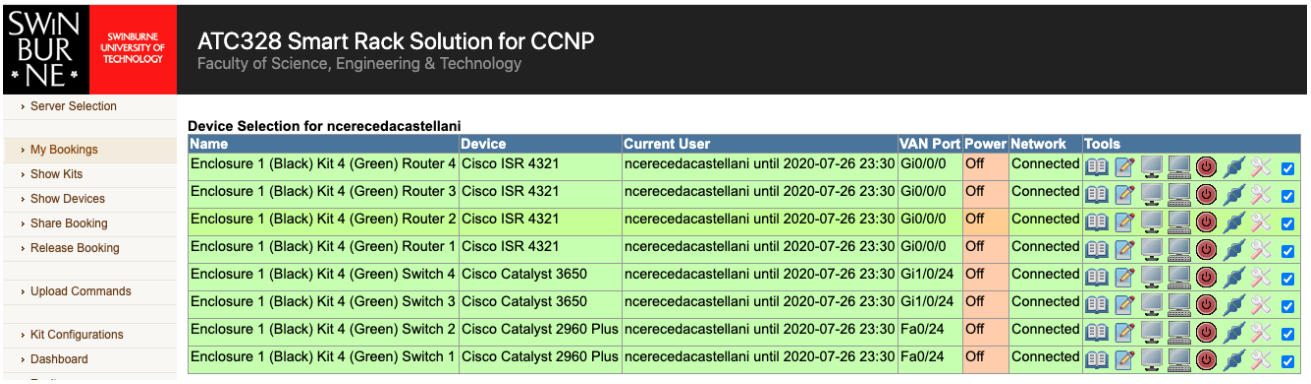
Step 1: Power On the Network Devices

Once you've booked a kit, the next step is to power on the devices you will be using during your lab session.

On this practice we are going to use the network devices shown in the **TNE10006/TNE60006 Lab Infrastructure and Wiring Scheme** diagram on page 1:

- Switch 1
- Switch 3
- Switch 4
- Router 1

To power on the devices, first click the **My Bookings** option in the left-hand side menu; this will display the list of devices in your booked kit. Click on the **power button** in the right-most column to power on a device. Do this for all the devices you will be using during your practice, making sure you leave all other devices off.



Name	Device	Current User	VAN Port	Power	Network	Tools
Enclosure 1 (Black) Kit 4 (Green) Router 4	Cisco ISR 4321	ncerecedacastellani until 2020-07-26 23:30	Gi0/0/0	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Router 3	Cisco ISR 4321	ncerecedacastellani until 2020-07-26 23:30	Gi0/0/0	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Router 2	Cisco ISR 4321	ncerecedacastellani until 2020-07-26 23:30	Gi0/0/0	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Router 1	Cisco ISR 4321	ncerecedacastellani until 2020-07-26 23:30	Gi0/0/0	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Switch 4	Cisco Catalyst 3650	ncerecedacastellani until 2020-07-26 23:30	Gi1/0/24	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Switch 3	Cisco Catalyst 3650	ncerecedacastellani until 2020-07-26 23:30	Gi1/0/24	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Switch 2	Cisco Catalyst 2960 Plus	ncerecedacastellani until 2020-07-26 23:30	Fa0/24	Off	Connected	
Enclosure 1 (Black) Kit 4 (Green) Switch 1	Cisco Catalyst 2960 Plus	ncerecedacastellani until 2020-07-26 23:30	Fa0/24	Off	Connected	

After a few seconds, the status under the Power column will change to **On.** Allow another 3 to 5 minutes for the devices to finish the booting process before you attempt to connect to the devices via console.

Note**:** the remaining Steps in Part 3 are only to be followed when accessing the lab environment from outside the Swinburne network. During your on-campus sessions you will connect to the console of the devices by clicking the **native console button** (the one immediately to the left of the power button).

Step 2: Open a Terminal Emulation Application

Note: you only need to complete this step if working on your personal computer. If working on a lab PC, a terminal emulation window will open automatically by clicking the **native console** button next to the device you wish to connect to (see Step 4).

To manage a network device via console, we first need to establish an **SSH connection** to the Smart Rack server in the enclosure where the device is physically situated. This server will then bridge the SSH connection to the console port of the device, allowing us to manage it via command line interface.

To establish this type of remote connections, we need to use **terminal emulation software**. Terminal emulators allow you to use your local computer's keyboard and display as input/output devices for the command line interface of an external system.

Windows 10 (and later), MAC and Linux operating systems include terminal applications you can use to establish an SSH connection to the Smart Rack server. Identify the terminal emulator application available on your system and open a new window.

If you are using an older Windows system, you will need to download and install a third-party terminal application. **Putty** is a free terminal application that you can download at: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

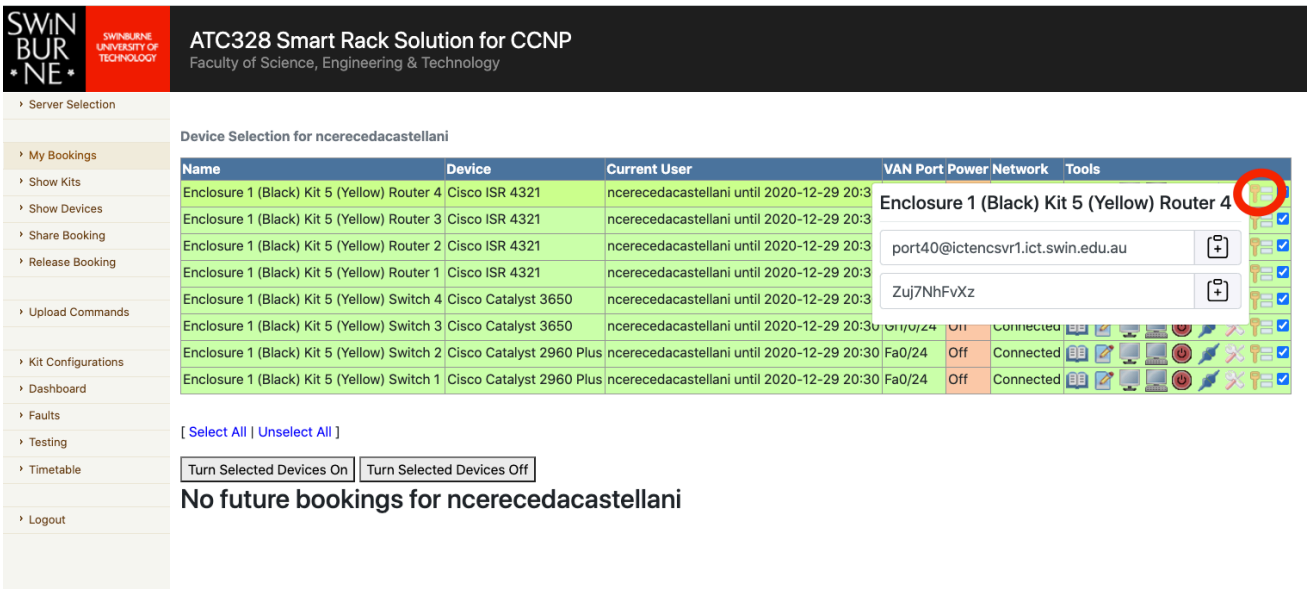
Step 3: Retrieve SSH connection details for Switch 1

Note: you only need to complete this step if working on your personal computer. If working on a lab PC, the connections details are passed on to the terminal emulator automatically when clicking the **native console** button next to the device you wish to connect to (see Step 4).

To connect to Switch 1 from your personal computer, you will need to establish an SSH connection to the specific Smart Rack server that is physically connected to Switch 1, using a specific username and password that will bridge your connection to Switch 1's console port. This means that you will need to retrieve the following details:

- **Hostname** of the server.
- **Username** associated with Switch 1's console.
- **Password** associated with Switch 1's console.

To retrieve these details from the Smart Rack Web Interface, go to **My Bookings** and click on the **key icon** next to the device you wish to access. See the example below:



Clicking the **key icon** will display two fields:

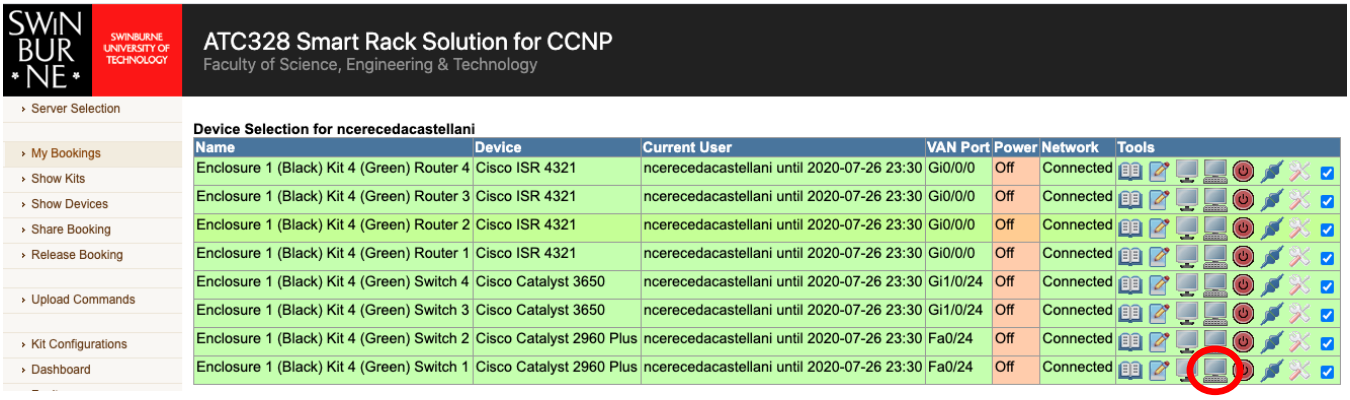
- The first field contains the username and hostname for the connection
  In the example above: port40@ictencsvr1.ict.swin.edu.au
  Username: port40
  Hostname: ictencsvr1.ict.swin.edu.au
- The second field contains the password for the connection.
  In the example above:
  Password: Zuj7NhFvXz

If you are having trouble retrieving the SSH connection details from the SmarRack Web Interface, ask your lab instructor for help. Alternatively, you can go to the **Manual Console** tab of the Remote Lab Access information page in Canvas, where you will find step-by-step instructions and a short video on how to retrieve SSH connection details from the Smart Rack Web Interface.

Step 4: Connect to Switch 1

Option 1: connecting from a lab PC:

If working on a **lab PC**, click on the **native console** icon in the right-most column next for the device you wish to connect to; in this case, Switch 1.



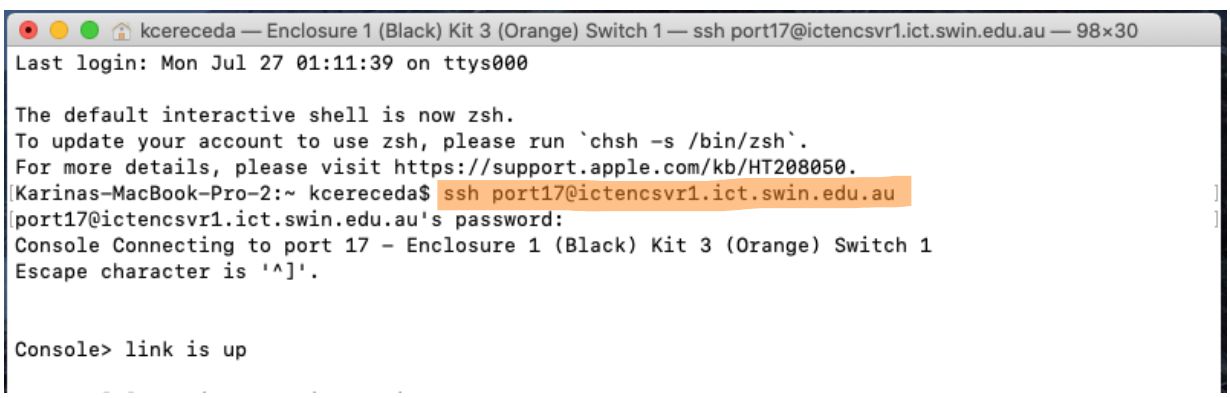
This will automatically open a Putty window with an SSH connection to Switch 1.

Option 2: connecting from your personal computer:

If working on **your personal computer** via remote access, open a terminal application window and initiate an SSH connection using Switch 1 connection details retrieved in Step 3.

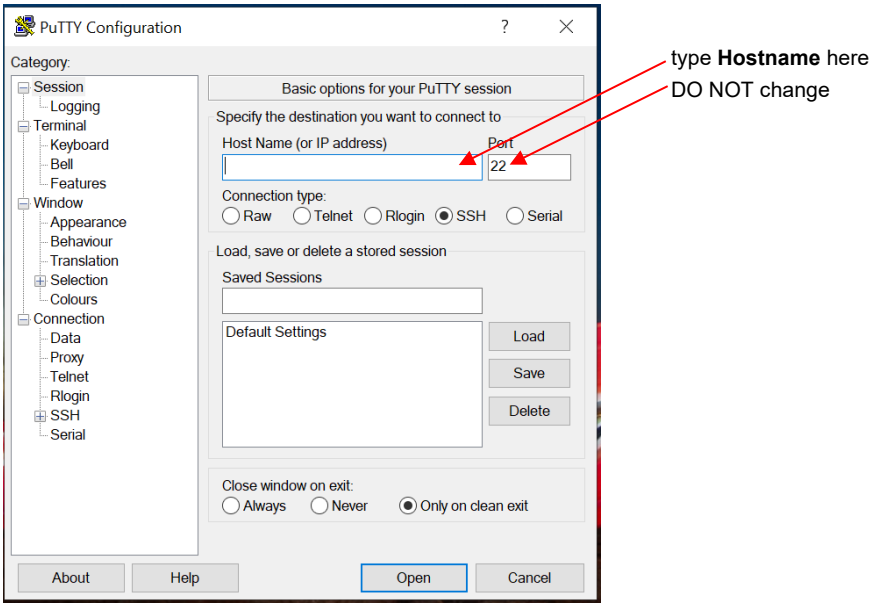
On Windows 10 or later, MAC or Linux operating systems, type the **ssh** command, with hostname and username details for Switch 1 (retrieved in step 3), in a terminal application window. Press Enter and type in the password when prompted. See the example below.

Example: **Username**: port17, **Hostname**: ictencsvr1.ict.swin.edu.au



Once the console link is up, hit Enter until you see the switch's command line prompt: Switch 1>

If you are using Putty, the initial window will look like this:



Type the **Hostname** for Switch 1 and make sure you DO NOT change the port number. This port number is not the related to the username for the connection (22 is the standard SSH application port).

Click **Open,** and a second window will open prompting you for the **Username** and **Password** to establish the connection. Use the username and password details retrieved in Step 3.

Once the console link is up, hit Enter until you see the switch's command line prompt: **Switch 1>**

Note: when prompted "Would you like to enter the initial configuration dialog?" answer "no" and then press Enter to confirm.

Step 5: Connect to Switch 3, Switch 4, and Router 1

Repeat Steps 3 and 4 to connect to Switch 3, Switch 4, and Router 1.

Note: you will need to open a new terminal emulator window for each device.

Part 3: Explore the Wiring Scheme

In part 4, you will explore how devices interconnect to each other under the generic Wiring Scheme

Step 1: Display the Interface Status on Switch 1

After you've successfully connected to the network devices via console, you have access to use Cisco command line interface commands to display status information, display and change configuration settings, reload the devices, etc.

One of the first commands you will learn is the **show ip interface brief** command. This command displays the physical and logical status of the network interfaces on the devices. We will discuss this command in more details in a later lab session, however, we will use it in this exercise to validate the interconnections shown in the **TNE10006/TNE60006 Lab Infrastructure and Wiring Scheme**

Switch 1 is connected to Switch 3 via FastEthernet0/1 and FastEthernet0/2, to Switch 4 via FastEthernet0/3 and FastEthernet0/4. Therefore, since both Switch 3 and Switch 4 are powered on, ports Fa0/1 to Fa0/4 on Switch 1 should be in the **up** status, indicating that they are connected to an active interface on another device.

Use the **show ip interface brief** command to validate ports **Fa0/1 to Fa0/4 status is up** in both the Status and the Protocol columns.

```
Switch# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
FastEthernet0/4        unassigned      YES unset  up                    up
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
```

Note: this is a partial output, you will find that Switch 1 has 24 FastEthernet interfaces and 2 GigabitEthernet interfaces.

Step 2: Display the Interface Status on Switch 3 and Switch 4

Use the **show ip interface brief** command on Switch 3 and Switch 4

Which ports are in the **up** status on Switch 3? _____

Which ports are in the **up** status on Switch 4? _____

Are there any ports that you think should be **up** but aren't? _____

Step 3: Display the Interface Status on Router 1

As opposed to switch interfaces, router interfaces are **disabled** by default. When a network interface is disabled, it will show as **administratively down** in the Status column of the show ip interface brief output.

```
Router> show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   unassigned      YES unset  administratively down down
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
GigabitEthernet0       unassigned      YES unset  administratively down down
```

This explains why Switch 3 and Switch 4 interfaces connecting to Router 1 are down: the network interfaces they connect to on Router 1 are not active.

Step 4: Power Off Switch 1

Go to the Smart Rack Web Interface and click on the power button power off Switch 1.

Will Switch 3 interfaces status change? And if so, for which interface(s)?

_____

Will Switch 4 interfaces status change? And if so, for which interface(s)?

_____

Use the show ip interface brief command on Switch 3 and Switch 4 to validate your answers.