EECS Tutorial: Routing & Switching Lab

FAQ for accessing the Routing & Switching Lab in EE 328C and 328D

What is the default login username and password for Arista switches?

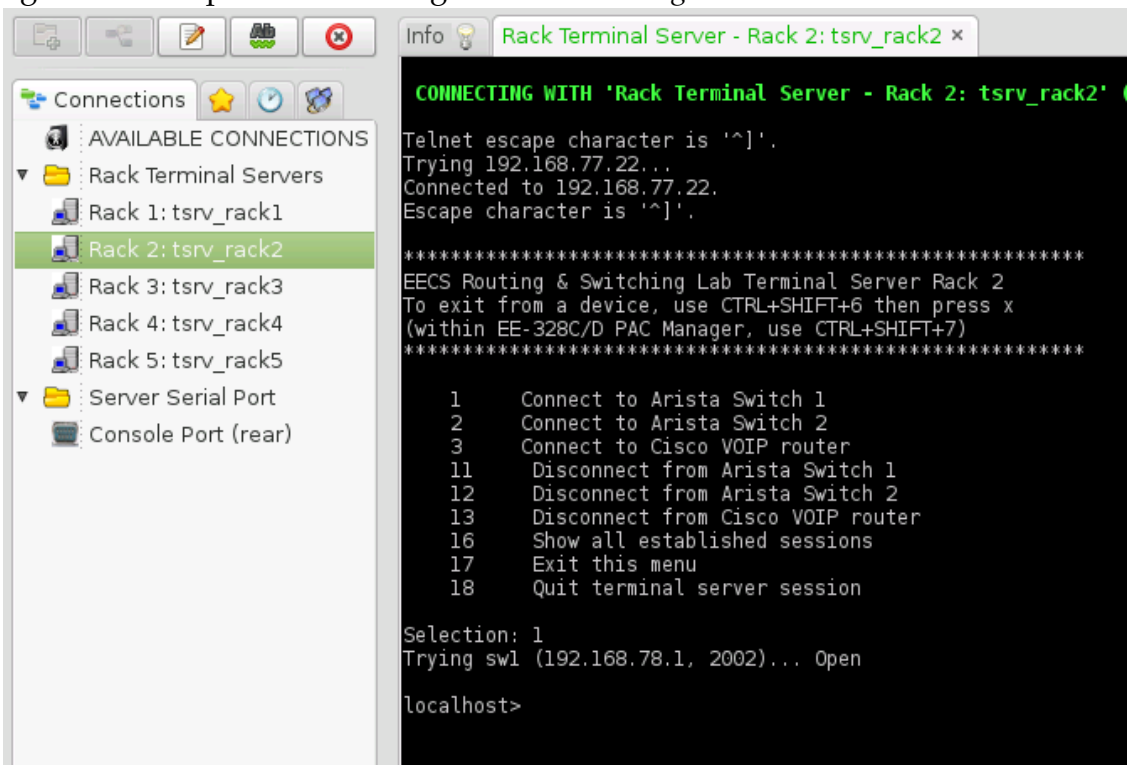
```
Username: student
Password: arista
```

How do I access rslab equipment from a mobile Linux terminal in EE 328C?

1. In EE 328C turn on a mobile Linux terminal. Computer will network boot from the rslab LTSP server and automatically log into a GUI desktop environment.
2. Open *PAC Manager* from the Desktop or the *applications* menu.
3. On left side, double-click the terminal server for the rack # assigned to you by GTA. A new session tab window will open and connect into the terminal server.
4. Once connected to the terminal server for your assigned rack, use the menu to connect/disconnect the Arista switches and Cisco router in the networking rack.
5. You can return to the terminal server menu by pressing `CTRL+SHIFT+7`.
6. To view all open connections in the session, return to the menu and press `16`.
7. To exit from the terminal server, return to the menu and press `18`.

NOTE: You can open more than one tabbed session within *PAC Manager* to access the same rack terminal server and connect to multiple network devices concurrently, but each switch or router can only be accessed by one terminal server session at a time.

Figure 1: Example of connecting with *PAC Manager* from a mobile Linux terminal



How do I access rslab equipment using a computer in EE 327 or EE 328 labs?

1. Run the SSH *PuTTY* client on a Windows computer in the lab.
2. In the *PuTTY* Configuration window, enter `rslab.cs.wichita.edu` into the **Host Name** field.
3. You may wish to make further *PuTTY* changes, such as adjusting items in *Window* Category, or adding your myWSU ID to *Connection–Data–Auto-login username*.
4. If you wish to save these settings for future use, within the *Session* Category, type a name for your session in the **Saved Sessions** field and click on **Save**.
5. When ready to connect to `rslab.cs.wichita.edu` click on **Open**, then enter your myWSU ID and password as prompted.
6. The first time you connect to `rslab.cs.wichita.edu` a **PuTTY Security Alert** window will likely pop up stating *"The server's host key is not cached in the registry."* Check the server's *key fingerprint* matches one of the rslab host key fingerprints listed at the bottom of this document, then click **Yes**.
7. You may see a "`Could not chdir...`" error message when you open a connection to the rslab proxy server. Disregard this message. rslab does not need access to your user home directory for access to the network rack in EE 328D.
8. Once logged into `rslab.cs.wichita.edu`, connect to an rslab networking rack by typing (where `#` is the rack number assigned to you by the lab GTA)
   `telnet rack#`
9. Once connected to the terminal server for your assigned rack, use the menu to connect/disconnect the Arista switches and Cisco router in the networking rack.
10. You can return to the terminal server menu by pressing `CTRL+SHIFT+6` and then `x`.
11. To view all open connections in the session, return to the menu and press `16`.
12. To exit from the terminal server and close the remote SSH connection to the rslab proxy server, return to the menu and press `18`.

NOTE 1: You can open multiple *PuTTY* windows from your Windows computer to access the same rack terminal server and connect to multiple network devices concurrently, but each switch or router can only be accessed by one terminal server session at a time. You can also use a terminal multiplexer such as *tmux* or *screen* within `rslab` to open multiple, simulaneous telnet sessions to an rslab terminal server.

NOTE 2: Due to WSU security policies, rslab network devices can only be remotely accessed from on campus in the labs or via the cslab Linux environment.

How do I access rslab equipment using the web-based cslab Linux environment?

1. Follow the eecs_tutorial_cslab_web_access document to log into cslab-gateway.cs.wichita.edu using a web-browser.
2. Once logged into cslab *guacamole*, open a **cslab_SSH_CLI_terminal** connection.
3. Connect to an rslab networking rack using *OpenSSH*, by typing (where `#` is the rack number assigned to you by the lab GTA)
   `ssh -t rslab telnet rack#`
4. Enter your myWSU password when prompted to do so.
5. The first time you connect to `rslab` you may see the warning:
   `The authenticity of host 'rslab' can't be established.`
   Check the server's *key fingerprint* matches one of the rslab host key fingerprints listed at the bottom of this document, then type `yes`.
6. You may see a "`Could not chdir...`" error message when you open a connection to the rslab proxy server. Disregard this message. rslab does not need access to your user home directory for access to the network rack in EE 328D.
7. Once connected to the terminal server for your assigned rack, use the menu to connect/disconnect the Arista switches and Cisco router in the networking rack.
8. You can return to the terminal server menu by pressing `CTRL+SHIFT+6` and then `x`.
9. To view all open connections in the session, return to the menu and press `16`.
10. To exit from the terminal server and close the remote SSH connection to the rslab proxy server, return to the menu and press `18`.

NOTE: You can open up to four **cslab_SSH_CLI_terminal** browser tabs or windows to access the same rack terminal server and connect to multiple network devices concurrently, but each switch or router can only be accessed by one terminal server session at a time. You can also use a terminal multiplexer such as *tmux* or *screen* within a **cslab_SSH_CLI_terminal** to open multiple, simulaneous telnet sessions to an rslab terminal server.

Figure 2: Example of SSH remote connection via a **cslab_SSH_CLI_terminal**

```
Linux cslab-node-0 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u6 (2018-10-08) x86_64
This system may be accessed by authorized users at WSU only.
Use of this system implies acceptance of authorized use policies.
Misuse may be subject to prosecution or disciplinary measures.

cluster_node host: cslab-node-0.cs.wichita.edu (10.10.10.6)
This system is managed by CFEngine v3.12.0
Support for EECS: Ben Roose (ben.roose@wichita.edu)

Last login: Thu Mar 21 17:51:06 2019 from 10.10.10.100
[redacted]@cslab-node-0:~$ ssh -t rslab telnet rack1
The authenticity of host 'rslab (172.18.208.160)' can't be established.
ECDSA key fingerprint is SHA256:X6dBKj4sqYYPWol6MXSQvGhpIQ6qBxh7mBQhnSw8n64.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'rslab,172.18.208.160' (ECDSA) to the list of known hosts.
[redacted]@rslab's password:
Could not chdir to home directory /opt/homes/stu04/[redacted]: No such file or directory
Trying 192.168.77.21...
Connected to rack1.
Escape character is '^]'.

************************************************************
EECS Routing & Switching Lab Terminal Server Rack 1
To exit from a device, use CTRL+SHIFT+6 then press x
(within EE-328C/D PAC Manager, use CTRL+SHIFT+7)
************************************************************

    1     Connect to Arista Switch 1
    2     Connect to Arista Switch 2
    3     Connect to Cisco VOIP router
    11     Disconnect from Arista Switch 1
    12     Disconnect from Arista Switch 2
    13     Disconnect from Cisco VOIP router
    16     Show all established sessions
    17     Exit this menu
    18     Quit terminal server session

Selection: 1
Trying sw1 (192.168.78.1, 2002)... Open


SW1 login: student
Password:
SW1>
```

What do I do if I cannot access the cslab Linux environment?

- If you cannot access the cslab environment, ensure you have changed your myWSU password within the last three months and can access the myWSU main website mywsu.wichita.edu. If you cannot access the myWSU website, then you will need to change your password before gaining access into the cslab environment.
- If you can access myWSU but cannot access the cslab environment, please contact the EECS systems administrator, ben.roose@wichita.edu.

Why do I sometimes see "% Connection refused by remote host"?

- Though you can open multiple connection sessions to the terminal server controlling each rack, you can only access each network switch or router device within the rack from a single terminal server session.
- This access restriction is caused by limitations of the serial communication protocol between the terminal server and each network device in the rack. The access restriction also acts as a security failsafe, since it reduces the possibility of more than one person or lab group attempting to make changes to a switch or router configuration concurrently.
- If you see the "`% Connection refused by remote host`" error, then either you already have opened a connection to this network device in another terminal server session or another person/lab group has an open connection to this network device. Check you do not already have an open connection in another terminal server session first, then speak with the lab GTA if you cannot resolve the connection refused error yourself.

How do I create a screenshot of my lab session?

EE 328C Linux Terminals

Within the EE 328C mobile Linux terminals there are three screenshot tools: pressing `Print Screen` key, using *Take Screenshot* located on the Desktop, or using *PAC Manager's* **Take Screenshot** menu option.

Remote Access Clients

Most Windows, Linux and Mac client systems have screenshot tools, which can be used to screenshot the remote access terminal window. Please see your system's documentation for further help.

How do I create a text log of my entire lab session?

EE 328C Linux Terminals

Within the EE 328C Linux terminals, *PAC Manager* can log all session data to a text file.

1. Right-click on the session title tab and select **Save session log...** from the menu.
2. Enter a name for the log file and click **Enter** button to save.

Remote Access Clients: Windows computer in lab

When accessing the rslab remotely with PuTTY on a Windows client, a session log can be specified at the start of the remote SSH session by configuring PuTTY's logging function:

1. In the *PuTTY Configuration* window, click on **Logging** category on the left.
2. Select **All session output** and click on **Browse** button.
3. Enter a name for the log file and click **Save** button to save.
4. *Optional:* Logging options can be saved as part of a host connection session in the *PuTTY* **Saved Sessions** list.
5. For further help on configuring logging in *PuTTY*, see:
   PuTTY User Manual: Section 4.2

Remote Access: cslab Linux Environment

When accessing the rslab remotely from a **cslab_SSH_CLI_terminal** connection, a session log can be specified at the start of the remote SSH session by typing (where # is the rack number assigned to you by lab GTA and log_filename is the path and filename for log)

```
ssh -t rslab telnet rack# | tee log_filename
```

For example:

```
ssh -t rslab telnet rack1 | tee cs764_assign1.log
```

For details on how to download the log file from the cslab Linux environment to your local computer, refer to the eecs_tutorial_cslab_web_access document.

Why is *PuTTY* or *OpenSSH* asking to confirm the authenticity of rslab host keys?

- SSH host keys are essential to securing an SSH connection into a remote server. If you see an incorrect host key, then it may mean a cyber-attacker has attempted to compromise the remote server using a "man-in-the-middle" attack.
- You can manually add SSH host keys to your *PuTTY* and *OpenSSH* known hosts. When adding new host keys you should always ensure the host key fingerprint is correct. `rslab` host key fingerprints must match one of the following SHA256 or MD5 hashes before you add or accept the host key:

```
ECDSA key fingerprint is
SHA256:X6dBKj4sqYYPWol6MXSQvGhpIQ6qBxh7mBQhnSw8n64
MD5:d8:ba:c6:1c:86:fa:7f:f6:92:4f:c1:02:30:ce:ab:99

ED25519 key fingerprint is
SHA256:zzozIV7cP1T9C77PLRaevzdzCu21k44lbjd8jaJKS8Q
MD5:6d:3d:8e:3a:db:f6:de:33:af:77:01:40:f3:71:1d:14

RSA key fingerprint is
SHA256:0CUyGZAYMdOd8vTOK3AtM2XTX3lMaGA2NP73rR7s6Ns
MD5:75:5a:16:53:1a:7c:c2:4b:99:66:2d:e3:1e:76:f9:c9

DSA key fingerprint is
SHA256:7zW122xr+aoBb5yiRI96nvdx8Ml07qLKHYwG2Wu6jIM
MD5:27:59:53:18:5a:67:71:f6:32:f1:e1:15:e9:e5:fe:b1
```