Computer Practical – Week 13

Objectives

The aim of this week's computer practical includes:

- Learn the basics of securing network devices
- Consolidate the knowledge and skills of configuring basic settings of network devices.
- Review show commands
- Explore a small to medium-sized business network

Tasks

Accordingly, you will need to complete the following tasks in this week's computer practical class:

1. Packet Tracer – Securing Network Devices
2. Packet Tracer – Using Show Commands
3. Packet Tracer - Explore a Network

Instructions of the activities are given on the next pages.

Assessment

This week's Computer Practical is assessed in class, and it is worth 2% of the total score of the course.

Notes:

- To be awarded marks for this computer practical, a student must:
  - attend week 13 Computer Practical class (being absent from the class will result in zero marks for week 13's computer practical), and
  - complete all the 3 tasks above and submit:
    1. the PKA file for Task 1
    2. the Word document with your answers to the questions of Tasks 2 and 3
- Use the link "Computer Practical-Week 13-Submission" link in Week 13 section of Learnonline course site to submit the files.
- If you cannot finish all the tasks in class, let your tutor know before leaving the class, and submit the files by Sunday 11:59 pm of Week 13. Late submission will result in zero marks for week 13's computer practical.

Packet Tracer – Securing Network Devices

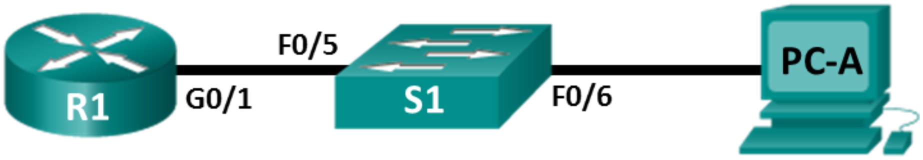
Before start:

1. Download from Learnonline course website (**Computer Practical-Week 13 folder**) the Packet Tracer activity file: **`wk13-computer-prac-PKA-a-Secure-Devices.pka`**

2. Open the Packet Tracer activity file downloaded

3. Follow the instruction **given below** to complete this Packet Tracer activity

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Basic Security Measures on the Router

Part 3: Configure Basic Security Measures on the Switch

Background / Scenario

It is recommended that all network devices be configured with at least a minimum set of best practice security commands. This includes end user devices, servers, and network devices, such as routers and switches.

In this lab, you will configure the network devices in the topology to accept SSH sessions for remote management. You will also use the IOS CLI to configure common, basic best practice security measures. You will then test the security measures to verify that they are properly implemented and working correctly.

Part 1: Configure Basic Device Settings

In Part 1, you will configure basic settings, such as the interface IP addresses, device access, and passwords on the devices.

Note: Refer to the Appendices of this document if you need to find out the necessary commands for initializing the devices or configuring their basic settings, but please firstly try to complete the steps without looking at the Appendices.

Step 1: Initialize and reload the router and switch.

Step 2: Configure the router

a. Assign the device name according to the Addressing Table.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password and enable login.

e. Assign **cisco** as the VTY password and enable login.

f. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

g. Configure and activate the router's G0/1 interface using the information given in the Addressing Table.

```
R1(config)# int g0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
```

h. Issue the **show running-config** command at the privileged EXEC prompt to verify the above configurations of the router.

Step 3: Configure the switch.

a. Assign the device name according to the Addressing Table.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password and enable login.

e. Assign **cisco** as the VTY password and enable login.

f. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

g. Configure the default SVI on the switch with the IP address information according to the Addressing Table.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.1.1
```

h. Issue the **show running-config** command at the privileged EXEC prompt to verify the above configurations of the switch.

Step 4: Assign static IP information to the PC interface

Configure the IP address, subnet mask, and default gateway settings on PC-A.

Step 5: Verify network connectivity.

a. From PC-A, ping its default gateway. If the ping fails, troubleshoot the connection.

b. From S1, ping its default gateway. If the ping fails, troubleshoot the connection.

Part 2: Configure Basic Security Measures on the Router

Step 1: Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

Step 2: Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length. **Note**: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

a. Change the privileged EXEC encrypted password to meet guidelines.

```
R1(config)# enable secret Enablep@55
```

Note that the password **cisco** set up in Part 1 will not be used any longer. Even though the password command still appears in the line sections of the running-config, this command was disabled as soon as the login local command was entered for those lines.)

b. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Note that the security passwords min-length command only affects passwords that are entered after this command is issued. Any pre-existing passwords remain in effect. If they are changed, they will need to be at least 10 characters long.

Step 3: Enable SSH connections.

In the past, Telnet was the most common network protocol used to remotely configure network devices. However, protocols such as Telnet do not authenticate or encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

For SSH to function, the network devices communicating must be configured to support it. In this step, you will configure the router to accept SSH connections over the VTY lines.

a. Assign the domain name as **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Create a local user database entry to use when connecting to the router via SSH. The password should meet strong password standards, and the user should have user EXEC access. (After the following command is issued, a user with username “admin” and password “Admin1p@55” is created, and the user’s privilege level is “1”, user EXEC mode access).

```
R1(config)# username admin privilege 1 secret Admin1p@55
```

c. Configure the transport input for the VTY lines so that they accept SSH connections, but do not allow Telnet connections.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. The VTY lines should use the local user database for authentication.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Generate a RSA crypto key using a modulus of 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
```

Note: If your router shows an error message after you have entered the above command line, then issue the command “**crypto key generate rsa”** only (i.e. without modulus 1024). Then the following message should display:

```
The name for the keys will be: R1.CCNA-lab.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
```

To answer the question “`How many bits in the modulus [512]:`”,type `1024`, then press Enter.

Step 4: Secure the console and VTY lines.

a. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after five minutes of inactivity.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. The following command impedes brute force login attempts. After the following command is issued, the router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
R1(config)# login block-for 30 attempts 2 within 120
```

What does the **2 within 120** mean in the above command?

____

What does the **block-for 30** mean in the above command?

____

Step 5: Verify that all unused ports are disabled.

Router ports are disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the **show ip interface brief** command. Any unused ports that are not in an administratively down state should be disabled using the **shutdown** command in interface configuration mode.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Step 6: Verify that your security measures have been implemented correctly.

a. On the PC, open the command line window and try to telnet to R1 by issuing the command:

```
telnet 192.168.1.1
```

Does R1 accept the Telnet connection? Explain.

____

b. On the PC, open the command line window and try to SSH to R1 by issuing the command (note: the parameter to use is “l” for line):

```
ssh -l admin 192.168.1.1
```

Does R1 accept the SSH connection? ____________________________

c. Close the SSH connection by typing “exit”

d. SSH to R1 again, and intentionally mistype the user and password information to see if login access is blocked after two attempts. What happened after you failed to login the second time?_________________

____

e. From your console session on the router, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 30 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

f. After the 30 seconds has expired, SSH to R1 again and login using the **admin** username and **Admin1p@55** for the password.

After you successfully logged in, what was displayed? _________________________

g. Enter privileged EXEC mode and use **Enablep@55** for the password.

If you mistype this password, are you disconnected from your SSH session after two failed attempts within 120 seconds? Explain.____

____

h. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Part 3: Configure Basic Security Measures on the Switch

Step 1: Encrypt the clear text passwords.

```
S1(config)# service password-encryption
```

Step 2: Strengthen Passwords on the switch.

Change the privileged EXEC encrypted password to meet strong password guidelines.

```
S1(config)# enable secret Enablep@55
```

Note: The security **password min-length** command is not available on the 2960 switch.

Step 3: Enable SSH Connections.

a. Assign the domain-name as **CCNA-lab.com**

```
S1(config)# ip domain-name CCNA-lab.com
```

b. Create a local user database entry for use when connecting to the switch via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 1) access by default.

```
S1(config)# username admin privilege 1 secret Admin1p@55
```

c. Configure the transport input for the VTY lines to allow SSH connections but not allow Telnet connections.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. The VTY lines should use the local user database for authentication.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Note: If your switch shows an error message after you have entered the above command line, then issue the command “**crypto key generate rsa”** only (i.e. without modulus 1024). Then the following message should display:

```
The name for the keys will be: R1.CCNA-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
```

To answer the question “`How many bits in the modulus [512]:`”,type `1024`, then press Enter.

Step 4: Secure the console and VTY lines.

a. Configure the switch to log out a line that has been idle for 10 minutes.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Note: if the above command for blocking login access does not work on your switch, skip this step.

Step 5: Verify all unused ports are disabled.

Switch ports are enabled, by default. Shut down all ports that are not in use on the switch.

a. You can verify the switch port status using the **show ip interface brief** command.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

b. Use the **interface range** command to shut down multiple interfaces at a time.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. Verify that all inactive interfaces have been administratively shut down.

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
```

```
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Step 6: Verify that your security measures have been implemented correctly.

a. Verify that Telnet has been disabled on the switch.

b. SSH to S1 again and log in using the **admin** username and **Admin1p@55** for the password.

   Did the banner appear after you successfully logged in? ___________

c. Enter privileged EXEC mode using **Enablep@55** as the password.

d. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Appendix A: Initializing and Reloading a Router and Switch

Part 1: Initialize the Router and Reload

Step 1: Access the router CLI and enter privileged EXEC mode.

Click on the router and then the CLI tab, and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

(**Note**: In real-life environment, will have to console into a router or switch to access its CLI to configure the device. For details of console connection, review the PT activity “Navigating the IOS”, which is part of Week 3 practical)

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 3: Reload the router.

Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

```
Router# reload
Proceed with reload? [confirm]

*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 4: Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Part 2: Initialize the Switch and Reload

Step 1: Access the router CLI and enter privileged EXEC mode.

Click on the switch and then the CLI tab and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
Directory of flash:/
```

```
    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Step 3: Delete the VLAN file.

a. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Appendix B: Configuring device basic settings

Notes:

- The following example configuration steps were done with a router. The commands for configuring the basic settings of a switch are the same.
- In real-life environment, there is no “CLI” tab available on a device for us to access the CLI of the device, instead, we will have to console into a router or switch to access its CLI to configure the device. For details of console connection, review the PT activity Navigating the IOS, which is part of Week 3 practical

a. Click on the device and the CLI tab, and enable privileged EXEC mode.

```
Router> enable
Router#
```

b. Enter configuration mode.

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

c. Assign a device name (e.g. R1) to the router.

```
Router(config)# hostname R1
```

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

```
R1(config)# no ip domain-lookup
```

e. Assign, e.g. **class** as the privileged EXEC encrypted password.

```
R1(config)# enable secret class
```

f. Assign, e.g **cisco** as the console password and enable login.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

g. Assign, e.g. **cisco** as the vty password and enable login.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

h. Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd #
Enter TEXT message.  End with the character '#'.
  Unauthorized access prohibited!
#
R1(config)#
```

j. Save the running configuration to the startup file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Packet Tracer – Using Show Command

Notes:

1. Download from Learnonline course website (**Computer Practical-Week 13** folder) the Packet Tracer activity file: `wk13-computer-prac-PKA-b-Show-Commands.pka`
2. Open the Packet Tracer activity file downloaded
3. Download from Learnonline course website **(Computer Practical-Week13** folder**)** the **Word file:** `week13-computer-prac-PKA-b-c-Instruction-Questions.docx`
4. Follow the instruction in the Word document to complete this Packet Tracer activity (Using Show Command).
5. Answer ALL questions in the word document by typing your answers in the space provided in the Word document.
6. Save the Word document with your answers. You will need this file for the next Packet Tracer activity.

Packet Tracer – Explore a Network

Notes:

1. Download from Learnonline course website (**Computer Practical-Week 13** folder) the Packet Tracer activity file: `wk13-computer-prac-PKA-c-Explore-Network.pka`
2. Open the Packet Tracer activity file downloaded
3. Open the **Word file:** `week13-computer-prac-PKA-b-c-Instruction-Questions.docx` (i.e. the file you have just used for the previous Packet Tracer activity)
4. Follow the instruction in the Word document to complete this Packet Tracer activity (Explore a Network).
5. Answer ALL questions in the word document by typing your answers in the space provided in the Word document.
6. Save the Word document with your answers and submit the word document as part of your Week 13 computer practical submission.