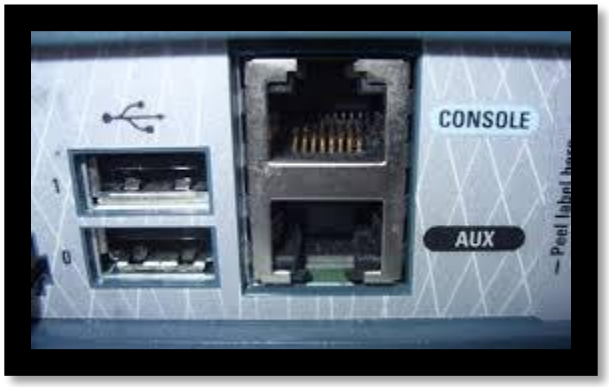

Networkforyou
Welcome
To
Network for you
Device Management
Networkforyou

Device Management:

- Traffic that network administrator uses to configure network devices is called device Managements.
- Management plane provides the ability to manage network infrastructure devices.
- Management plane traffic is usually consisting of protocol traffic like Telnet, SNMP or SSH.
- First step toward management is to set username and password.

Console Port:

- Console port is used to connect a computer directly to a router or switch.
- Every Cisco Router, Firewall or a Switch has a console port.
- Console port also known as the management port.
- It manages the router or switch since there is no display device for a router or switch.
- Console port must be used to initially to install routers.
- Console port can be used to log into a router directly without network connection.
- Console requires a terminal emulator application like putty to connect to router.
- Console port connects to router when a router cannot be accessed over the network.
- Console port is can be used to log into a router directly without network connection.



Virtual Terminal Line (VTY):

- VTY stand for Virtual Terminal Lines or Virtual Teletype.
- We are access network device virtually so we will use Virtual Terminal line.
- VTY is a Command Line Interface (CLI) created in a router
- VTY is just way to access Router or switch CLI Remotely.
- VTY are logical connections from the network to the switch or routers.

Telnet:

- Telnet is a network protocol that provides a command - line interface to communicate with a device remotely.
- In simple words we can say Telnet is use to access device remotely from different location.
- Telnet is an application layer protocol which is use to remotely access network devices.
- Telnet is work on Protocol TCP & Port # 23.
- First, we need to configure Telnet in network device then we can do Telnet from different place

Router Telnet configuration:

Config t
Enable password 12345
Line vty 0 4 ---------- if we want to allow 5 people to access device remotely then we will use vty 0 4 i.e. Qty 5

Password cisco
Login

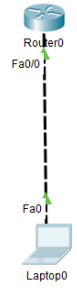
Or

Other Method

Config t
Username abc password abc

Enable password 12345
Line vty 0 4 ---------- if we want to allow 5 people to access device remotely then we will use vty 0 4 i.e. Qty 5

Password cisco
Login local



SSH: SSH (Secure Shell):

- SSH (Secure Shell) is a secure method for remote access as is include authentication and encryption. To do this, it uses an RSA public/private key pair.
- It works on Port number 22
- Very Secure Protocol
- SSH are two versions SSH Version 1 and SSH Version 2.
- Communication between server and client is encrypted in both SSH Version.
- SSH Version 2 is more Secure then SSH Version 1.
-

How to Configure SSH on CISCO IOS:

En
Config t
Hostname R1
Ip domain-name Networkforyou
Now we can generate the RSA Keypair:
Crypto key generate rsa
Then it will ask
The name for the keys will be: Branch2.Networkforyou
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]:

So we will choose let me choose 2048
Then we get

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

Then it will enable SSH

*Mar 1 5:21:55.540: %SSH-5-ENABLED: SSH 1.99 has been enabled

By default version 1 is enable . Now I am enabling to shh version 2

Then we will type ip ssh version 2

line vty 0 4

transport input ssh
login local
username admin password admin
enable password admin

How to access ssh:

Type
Ssh -l username IP
Password

Different between Telnet and SSH:

- Telnet and SSH protocols have the same purpose and both of them used to communicate to a remote device.
- Telnet is not secure because all the data would be sent in clear text including the passwords without authentication and encryption.
- where SSH is a Secure Protocol because it encrypts the data using authentication.

Console Access Troubleshooting:

- Check that the correct COM port been selected in terminal program like putty.
- Check and verify that the terminal program's settings are configured correctly.
- Check that any line password is used to authenticate to the console connection.
- Verify that local username and password is used to authenticate to the console.
- Check that AAA (authentication, authorization & accounting) used to authenticate.
- Check & verify that any method list been created for login authentication to console.
- Verify that the correct cable and drivers being used to connect to the console port.
- New devices use a mini-USB port, older devices use the serial-to-RJ45 console cable.
- Check and Verify that Mini-USD Port, is properly configured and Drivers is installed

SCP:

- SCP is network terms, which are stands for **Secure copy**.
- It is File Transfer Protocol.
- SCP provides secure and authenticated method for copying device image files.
- SCP provides secure and authenticated method for copying device configuration.
- Secure copy protocol relies on SSH, before enabling SCP, need to enable SSH.
- And also need to enable authentication and authorization on the Router and switch for SCP.

- SCP runs over TCP port number 22 by default which is port for SSH.
- SCP is also a connection oriented protocols secure like SFTP.
- It is used for sensitive and rapid file transfer and authentication and encryption is used.

To do this lab we need to download software from internet pscp.exe
Download this software. pscp.exe (https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html) and Save in C drive. First enable SSH then enable scp let do configuration: en config t hostname R1 int f0/0 ip add dhcp no sh ip domain-name abc crypto key generate rsa 2048 ip ssh version 2 line vty 0 4 transport input ssh login local username admin priv 15 password admin   ip scp server enable we will use small software to do this lab (pscp.exe) run this software write this in cmd cd \ pscp.exe -scp admin@ 192.168.38.155:running-config e:\r1.txt so it will copy configure in e drive

VTY Access Troubleshooting:

- Most devices are administered remotely via the vty lines, which support many protocols.
- Such as Telnet and Secure Shel (SSH) for remote access to Network devices such as router.
- Check and Verify that the IP address of the remote device Cisco router/switch is reachable.
- Check and Verify that the correct transport protocols are defined for the VTY Line SSH etc.
- Check and Verify that the line is configured to ask the user and Password for credentials.
- Check and Verify if only configured for password that the password is specified or not.
- Check and Verify that there is an Access control List defining which management stations.
- Also Check and Verify with show command that there are all vty lines available or busy.
- Check that there an ACL in the path between the client and the device blocking port 23.
- Check that there an ACL in the path between the client and the device blocking port 22.
- Check and Verify that the correct version and correct login command of SSH is specified.
- Also, check and verify that the correct key size been specified in network devices router.

SCP Troubleshooting:

- Ensure that SSH, authentication, and authorization have been configured correctly.
- Ensure , check and verify that an RSA key is available and can be used for encryption.
- Ensure, check and verify that AAA is configured correctly and is functioning in Router.
- Ensure that SCP is enabled on the Cisco device using the ip scp server enable command.
- Ensure, check and verify that the copy command is being used correctly in Cisco Router.
- Verify that the correct username and password are being used for copying in the Router.
- For additional help troubleshooting SCP issues, use the debug ip scp command in Router.
- Ensure that the correct IP address of SCP Server has been specified in the copy command.

SSH Troubleshooting:

- Most devices are administered remotely via the vty lines, which support many protocols.
- Such as Telnet and Secure Shel (SSH) for remote access to Network devices such as router.
- Check and Verify that the IP address of the remote device Cisco router/switch is reachable.
- Check and verify that the correct transport protocols are defined for the VTY Line SSH etc.
- Check and verify that the line is configured to ask the user and Password for credentials.
- Check and verify that there is an Access control List defining which management stations.
- Also Check and Verify with show command that there are all vty lines available or busy.
- Check that there an ACL in the path between the client and the device blocking port 22.
- Check and Verify that the correct version and correct login command of SSH is specified.

- Also, check and verify that the correct key size been specified in network devices Router.
- Domain name and hostname should be provided, and Crypto keys should be generated.

HTTP & HTTPS:

- HTTP is term, which stands for Hyper Text Transfer Protocol.
- HTTPS is term, which stands for Hypertext Transfer Protocol Secure.
- Cisco IOS has a HTTP server to managed web-based communication.
- HTTP Sends the data in clear text over the TCP port number 80.
- HTTP can be used for GUI access on Cisco devices routers & switches.
- Similar to HTTP, but HTTPs is encrypted over TCP port number 443.
- Cisco routers permit a user to connect to a router using HTTP.
- Cisco routers permit a user to connect to a router using HTTPS.

HTTP and HTTPS Troubleshooting:

- Cisco device must support HTTP client, check with the show ip http client all command.
- Router must connect to web server and ping the URL of the web server or its IP address.
- Ensure that correct URL or IP address of web server has been specified in copy command.
- Ensure that correct filename, username and password are specified in the copy command.
- Ensure, Check & verify that the correct port is specified in the copy command from router.
- Make sure specified the correct protocol in copy command in the Router HTTP or HTTPS.
- Check and Verify that the IP address of the remote device Cisco router/switch is reachable.
- Ensure, check and verify that the TFTP server is reachable from the Cisco device Routers.
- Check along path from source to destination for access lists that might be blocking HTTP.
- Check along path from source to destination for access lists that might be blocking HTTPS.
- Check and Verify that the device is configured to ask the user and Password credentials.
- Check and Verify that there is an Access control List defining which management stations.
- Check that there an ACL in the path between the client and the device blocking port 80.
- Check that there an ACL in the path between the client and the device blocking port 443.
- Check & verify that local username and password is used to authenticate to the HTTP.
- Check & verify that local username and password is used to authenticate to the HTTPS.
- Check & verify that HTTP and HTTPS services has been enable on Cisco devices or not.
- Check & Verify that there is an Access control List defining which management stations.