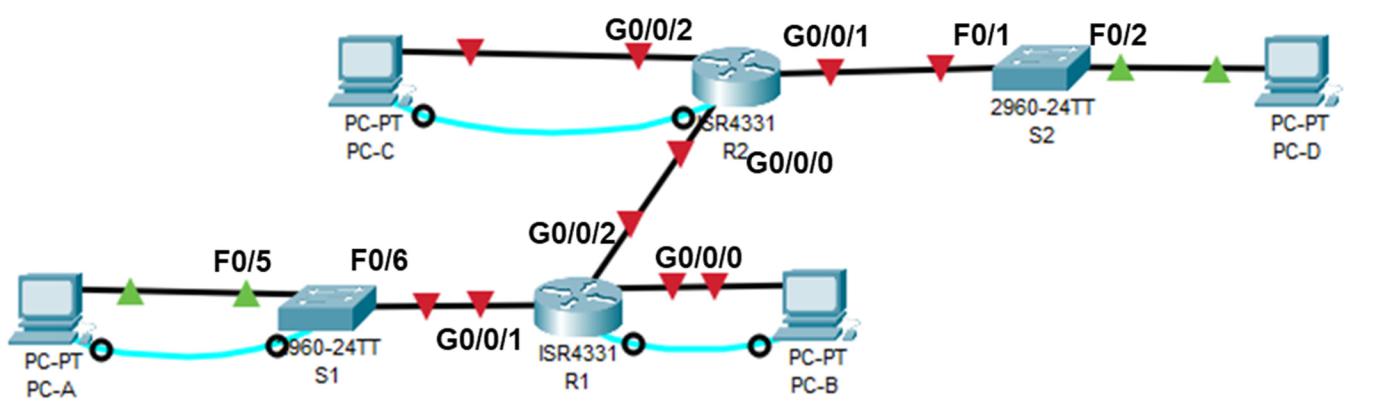
|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**CCNA ITN Lab 3** **Instruction** **Deadline: 8.1.2021**

**Updated Version**

**Name: Shabnaz Khanam**

**IPv4 Network and Static Routes Secure SSH Connection and Device Security TCP, UDP, DNS**

****

|  |  |  |
| --- | --- | --- |
| **NP Course** | **NP Chapter 4‐7** | |
| **PrepExam:** | **ITN Module Group Exams 14‐17** | |
| **Tasks:** | **Task 1** | **‐ IPv4 Network and Static Routes** |
|  | **Task 2** | **‐ Accessing Network Devices with SSH** |
|  | **Task 3** | **‐ Securing Network Devices** |

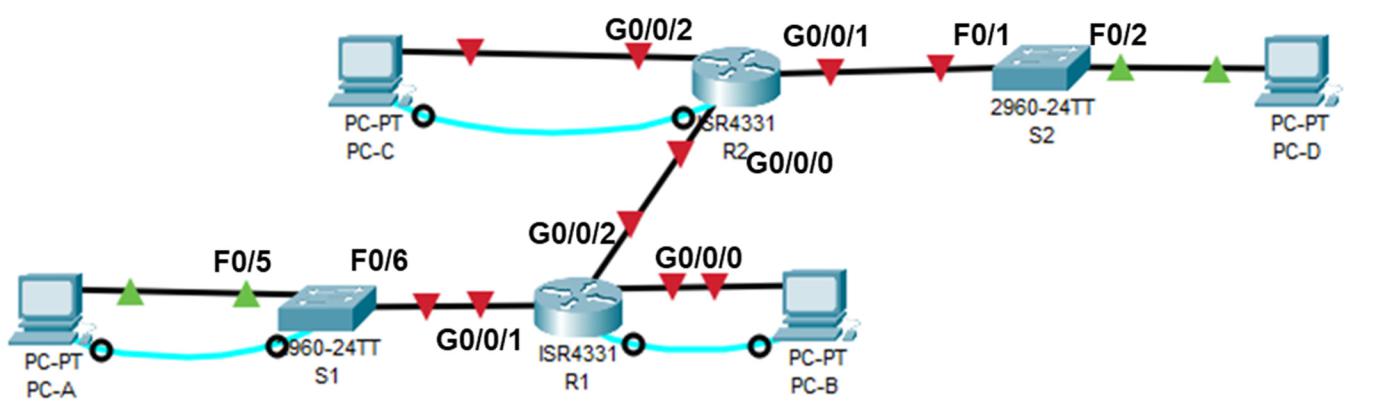
**Task4 ‐ Observe the TCP 3‐Way Handshake, UDP, and DNS**

Page 1 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Task 1 – IPv4 Network and Static Routes**

**Packet Tracer Topology**

****

**Addresing Table**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Device** |  |  | **Interface** |  |  | **IP Address** |  |  | **Subnet Mask** |  |  | **Default Gateway** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | R1 | |  | G0/0/0 | | 10.0.2.1 | |  | 255.255.255.0 | |  |  | N/A | |
|  |  |  |  |  | |  | |  |  | |  |  |  | |
|  |  |  |  | G0/0/1 | | 10.0.1.1 | |  | 255.255.255.0 | |  |  | N/A | |
|  |  |  |  |  | |  | |  |  | |  |  |  | |
|  |  |  |  | G0/0/2 | | 172.16.0.1 | |  | 255.255.255.252 | |  |  | N/A | |
|  |  | |  |  | |  | |  |  | |  |  | |  |
|  | S1 | |  | VLAN 1 | | 10.0.1.2 | |  | 255.255.255.0 | |  | 10.0.1.1 | |  |
|  |  | |  |  | |  | |  |  | |  |  |  | |
|  | R2 | |  | G0/0/0 | | 172.16.0.2 | |  | 255.255.255.252 | |  |  | N/A | |
|  |  |  |  |  | |  | |  |  | |  |  |  | |
|  |  |  |  | G0/0/1 | | 192.168.20.1 | |  | 255.255.255.0 | |  |  | N/A | |
|  |  |  |  |  | |  | |  |  | |  |  |  | |
|  |  |  |  | G0/0/2 | | 192.168.10.1 | |  | 255.255.255.0 | |  |  | N/A | |
|  |  | |  |  | |  | |  |  | |  |  | |  |
|  | PC‐A | |  | NIC | | 10.0.1.10 | |  | 255.255.255.0 | |  | 10.0.1.1 | |  |
|  |  | |  |  | |  | |  |  | |  |  | |  |
|  | PC‐B | |  | NIC | | 10.0.2.20 | |  | 255.255.255.0 | |  | 10.0.2.1 | |  |
|  |  | |  |  | |  | |  |  | |  |  | |  |
|  | PC‐C | |  | NIC | | 192.168.10.30 | |  | 255.255.255.0 | |  | 192.168.10.1 | |  |
|  |  | |  |  | |  | |  |  | |  |  | |  |
|  | PC‐D | |  | NIC | | 192.168.20.40 | |  | 255.255.255.0 | |  | 192.168.20.1 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Part 1:** **Set Up Network Topology and Initialize Devices**

**Step 1: Build topology in Packet Tracer.**

**COVID‐19 Version:** Build topology in **Packet Tracer**. Use and re‐label the following devices:

1. Build the network with ISR4331 routers, 2960 switches, and PCs in Packet Tracer. Rename the de‐ vices.
2. Implement a 3rd Gigabit Ethernet interface GLC‐T SFP in slot G0/0/2 in each ISR 4331 router.
3. Cable the network according to the topology with straight‐through TP cables .
4. Connect rollover console cables  from R1, R2, and S1 the shown PCs.

Page 2 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Part 2: Router R1 Settings**

**Step 1:** **Perform basic Router configurations**

Access router R1 through the Serial Console Port and Desktop Terminal of PC‐B

* Assign a device name **R1** to the router
* Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names

**Step 2:** **Secure access lines and basic device security**

* Assign **class** as the privileged EXEC secret
* Create a **banner** that warns anyone accessing the device that unauthorized access is prohibited
* Assign **cisco** as the console password and enable login
* Assign **cisco** the Telnet (VTY) password for 5 lines and enable login
* **Encrypt** the clear text passwords in the configuration file

**Step 3:** **Configure and activate router interfaces**

* Configure and activate interface g0/0/0 with IP address, mask and description
* Configure and activate interface g0/0/1 with IP address, mask and description
* Configure and activate interface g0/0/2 with IP address, mask and description

**Step 4:** **Test LAN A and LAN B Connectivity**

* Assign static IP address, network mask and default gateway to PC‐A and PC‐B.
* From PC‐A ping switch S1. Successful (y/n)no
* Test PC‐A to PC‐B connectivity by ping. Successful (y/n). yes

Remove errors and reconfigure network in case of no connectivity.

**Part 3: Router R2 Settings**

**Step 1:** **Perform basic Router configurations**

Access router R2 through the Serial Console Port and Desktop Terminal of PC‐C

* Assign a device name **R2** to the router
* Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names

**Step 2:** **Secure access lines and basic device security**

* Assign **class** as the privileged EXEC secret
* Create a **banner** that warns anyone accessing the device that unauthorized access is prohibited
* Assign **cisco** as the console password and enable login
* Assign **cisco** the Telnet (VTY) password for 5 lines and enable login
* **Encrypt** the clear text passwords in the configuration file

Page 3 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Step 3:** **Configure and activate router interfaces**

* Configure and activate interface g0/0/0 with IP address, mask and description
* Configure and activate interface g0/0/1 with IP address, mask and description
* Configure and activate interface g0/0/2 with IP address, mask and description

**Step 4:** **Test LAN C and LAN D Connectivity**

* Assign static IP address, network mask and default gateway to PC‐C and PC‐D.
* From PC‐D ping router R2 interface g0/0/2. Successful (y/n)yes
* From router R2 ping router R1 interface g0/0/2. Successful (y/n) yes
* Remove errors and reconfigure network in case of no connectivity.

**Step 5:** **Check Routes in Router R1**

* From PC‐A test connectivity to PC‐D by ping. Successful (y/n) no
* Display routing table of router R1. Record the networks which are reachable by router R1.

0.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.1.0/24 is directly connected, GigabitEthernet0/0/1

L 10.0.1.1/32 is directly connected, GigabitEthernet0/0/1

C 10.0.2.0/24 is directly connected, GigabitEthernet0/0/0

L 10.0.2.1/32 is directly connected, GigabitEthernet0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.0.0/30 is directly connected, GigabitEthernet0/0/2

L 172.16.0.1/32 is directly connected, GigabitEthernet0/0/2

* Explain, why PC‐D is not reachable from PC‐A:

R2 is unable to forward message

**Part 4: Configure Static Routes**

**Step 1: Configure a recursive static route on R2.**

With a **recursive static route**, the next‐hop IP address is specified. Because only the next‐hop IP is

specified, the router must perform multiple lookups in the routing table before forwarding packets. The IP ad‐ dress is the next hop router address:

1. Which networks must be configured as static routes on R2? 10.0.1.0

Which next hop address must be used on R2? 172.16.0.1

1. Configure the PC‐A LAN as **recursive static route** on R2.

**Step 2: Directly connected static route on R2.**

With a directly connected static route, the *exit‐interface* parameter is specified, which allows the router to resolve a forwarding decision in one lookup. A directly connected static route is typically used with a point‐to‐point serial interface.

1. Configure the PC‐B LAN as **directly connected static route** on R2.

**Step 3: Static default route on R1**

A default route identifies the gateway to which the router sends all IP packets for which it does not have a learned or static route. A default static route is a static route with 0.0.0.0 as the destination IP address and subnet mask. This is commonly referred to as a “quad zero” route. In a default route, either the next‐hop IP address (recursive static route) or exit interface (directly connected static route) can be specified.

1. Configure the R1 router with a default route using the exit interface of g0/0/2.

**Step 4: Verify connectivity of the LANs.**

1. Display IP routing table of router R2. Is there a path to PC‐A LAN?yes
2. From PC‐A, is it possible to ping R2 interface g0/0/0?yes
3. From PC‐A, is it possible to ping PC‐C?yes
4. From PC‐D, is it possible to ping PC‐A?yes

Remove errors and reconfigure network in case of no connectivity.

1. Display the routing table of router R1.

Which networks are routed in router R1?

Text

Description automatically generated

How is this new static default route marked in the routing table?

S\* 0.0.0.0/0 g0/0/2

Page 4 of 14

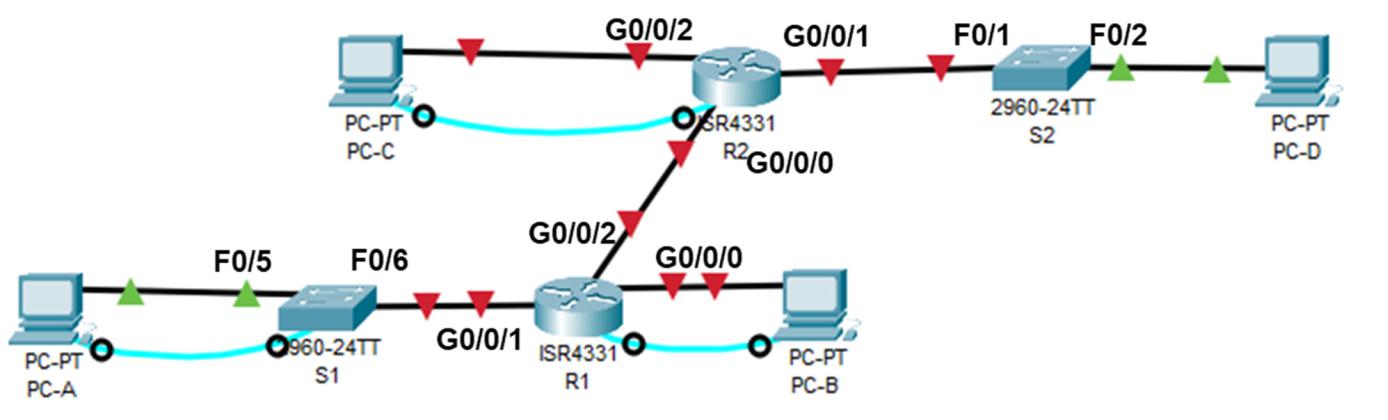
|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

Page 5 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Task 2 – Accessing Network Devices with SSH**

**Packet Tracer Topology**

****

Continue with topology and addressing of Task 1.

**Objectives**

Protocols such as Telnet do not authenticate or encrypt the information. This allows a network sniffer to intercept passwords and configuration information. Secure Shell (SSH) is a network protocol that estab‐ lishes a secure terminal emulation connection. SSH encrypts all information and provides authentication of the remote computer.

**Part 1:** **Configure Router R2 for SSH Access**

**Step 1:** **Configure device authentication with crypto key.**

The device name and domain are used as part in the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command. We use **RSA** encryption with a key length of **1024 Bytes**.

1. Configure the domain for the device.

R2(config)# **ip domain-name ccna-lab.com**

1. Configure crypto key

R2(config)# **crypto key generate rsa**

The name for the keys will be: **R2.ccna‐lab.com** Choose the size of the key of 1024 bits.

How many bits in the modulus [512]: **1024**

**Step 2:** **Configure a local username stored in the local database.**

The local database is used to store usernames and passwords with additional privilege levels.

**Note**: A **privilege level of 15** gives the user **administrator** rights.

R2(config)# **username admin privilege 15 secret adminpass**

Page 6 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Step 3:** **Enable SSH on the VTY lines.**

1. Enable only SSH on the **inbound** VTY lines using the **transport input** command.

R2(config)# **line vty 0 4** R2(config-line)# **transport input ssh**

1. Change the login method to use the **local database** for user verification and save the running configuration to the startup configuration file.

R2(config-line)# **login local** R2(config-line)# **end**

R2# **copy running-config startup-config**

**Note**: From now, access via VTY without having a local user is prohibited!!

**Part 2:** **Use SSH Client to start an SSH session to the Router**

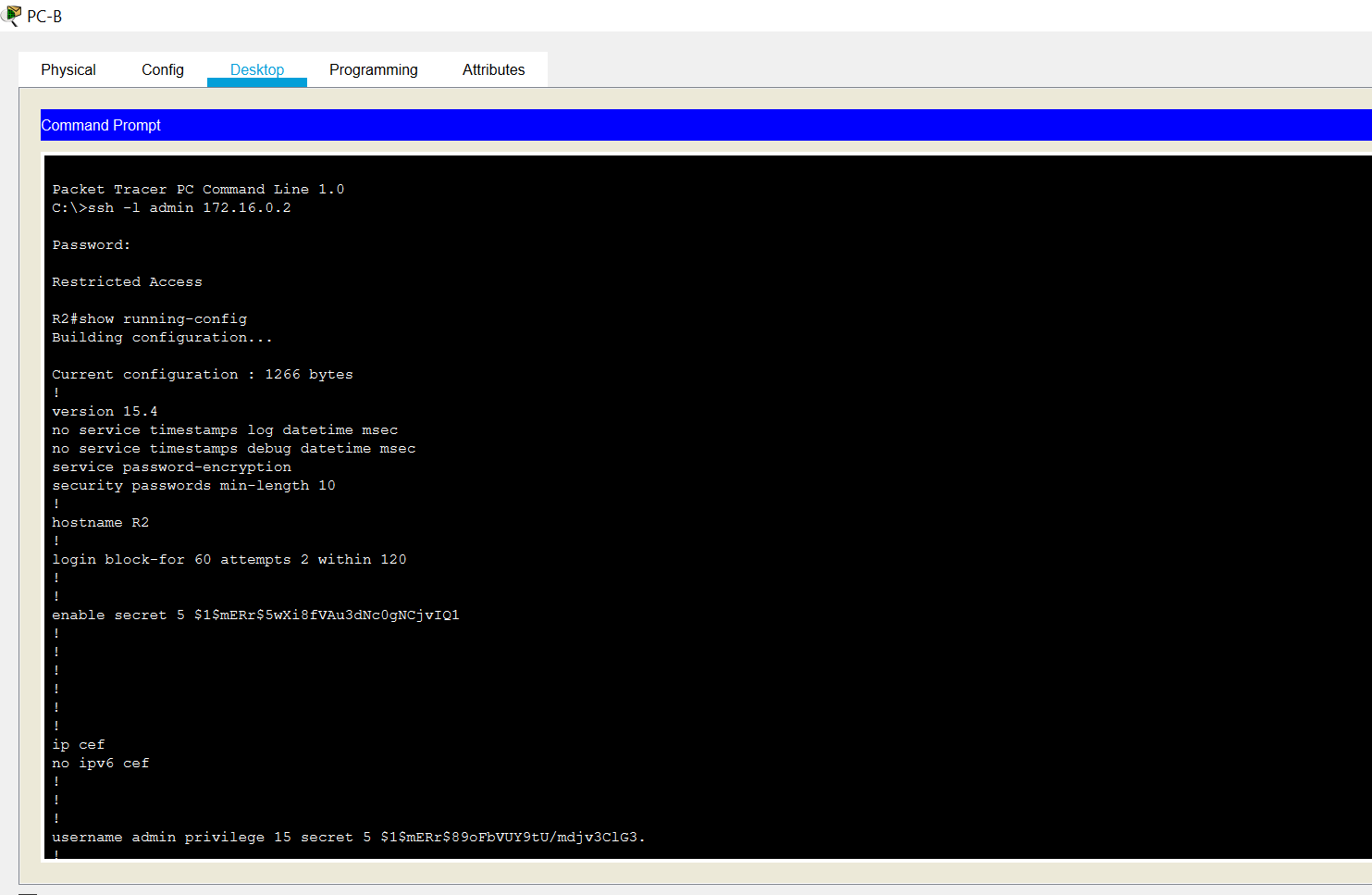
**Step 1:** **SSH Client**

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.

1. What is the default TCP port used for SSH sessions?22
2. From PC‐B, start the Telnet/SSH Client from Desktop and establish an SSH connection to router R2.

**Step 2:** **Administration Tasks**

1. Login as administrator on R2. At login the data from local database will be used.
2. Record the administrator password from running‐configuration.

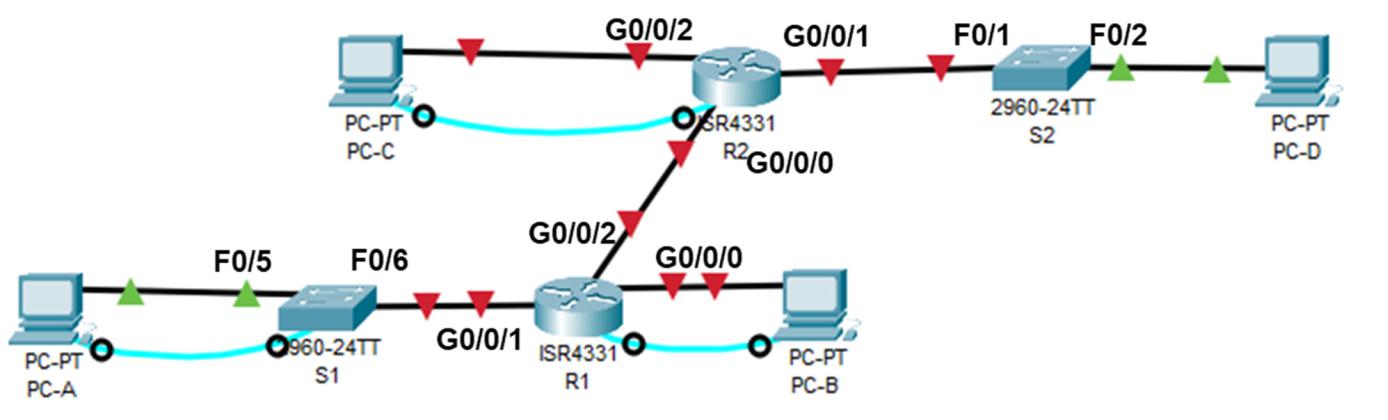


1. Enter **exit** to exit the SSH session and close the SSH Client.

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Task 3 ‐ Securing Network Devices**

**Packet Tracer Topology**

****

Continue with topology and addressing of Task 1.

**Part 1: Basic Switch Security Measures**

**Step 1: Configure Switch S1 via Console Cable**

Access switch S1 through the Serial Console Port and Desktop Terminal of PC‐A

* Provide hostname **S1**
* Prevent DNS domain lookup

**Step 2:** **Secure access lines and basic device security**

* Assign **class** as the privileged EXEC secret
* Create a **banner** for motto‐of‐the‐day
* Implement terminal login (Console) and password is **cisco**.
* Implement 5 Telnet lines (vty) and password is **cisco**.
* **Encrypt** all passwords

**Step 3:** **Switch Virtual Interface**

* Configure and switch‐on VLAN 1 interface
* Configure the switch default gateway.

**Step 4:** **Shut off unused switch ports.**

Switch ports must be secured as well. Switch ports are enabled by default. Shut down all ports that are not in use on the switch. Use the **interface range** command to shut down multiple interfaces at a time. Use it for those ports, which are not in use!

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

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

S1# show ip interface brief

Record the status of interface g0/1:

Page 8 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |
| **Part 2:** | **SSH at Switches** |  |

**Step 1:** **SSH connectivity on Switch S1**

On switches the same security mechanisms as on routers may be applied.

1. Configure the domain for the device.

S1(config)# **ip domain-name ccna-lab.com**

1. Configure crypto key

S1(config)# **crypto key generate rsa** ...

How many bits in the modulus [512]: **1024**

1. Enable SSH on the **inbound** VTY lines and login method to use the **local database** for user verification.

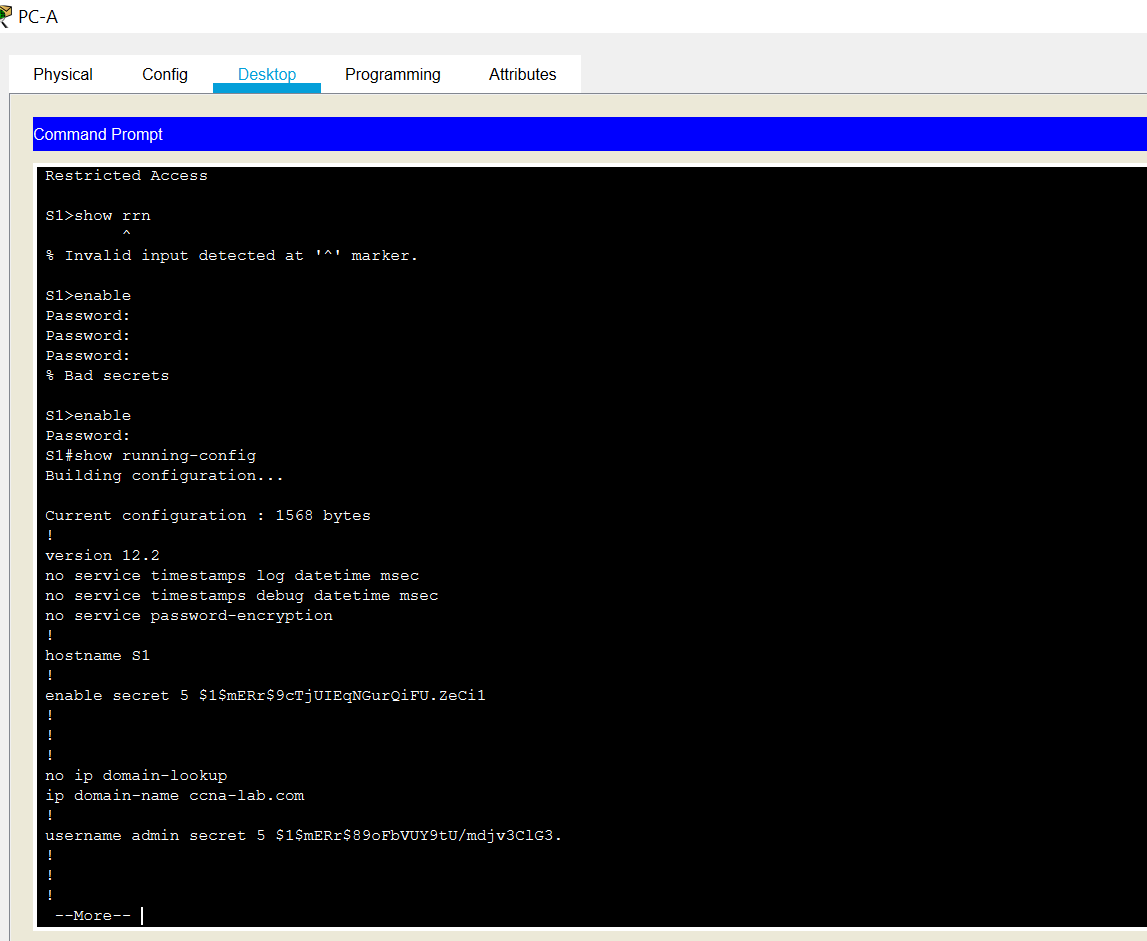
S1(config)# **username admin privilege 15 secret adminpass** S1(config)# **line vty 0 4**

S1(config-line)# **transport input ssh** S1(config-line)# **login local** S1(config-line)# **end**

**Step 2: Test SSH connectivity to Switch S1.**

1. Open a Telnet connection from PC‐A to switch S1. Does S1 accept the Telnet connection?yes
2. Open an SSH connection from PC‐A to switch S1. Does S1 accept the SSH connection?yes
3. Issue the **show run** command.

What indicates the configuration of SSH in the running‐configuration?



**Part 3:** **Strengthen Login and Password Security**

**Step 1: Strengthen passwords on Router R2.**

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include mixing letters, numbers, and special characters in the password and setting a minimum length.

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

R2(config)# **enable secret Enablep@55**

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

R2(config)# **security passwords min-length 10**

Page 9 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Step 2: Secure the console and VTY lines by timeout and lock**

1. 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 au‐ tomatically logs the user out after the specified time.

The following commands cause the line to log out after five minutes of inactivity.

R2(config)# **line console 0** R2(config-line)# **exec-timeout 5 0** R2(config-line)# **line vty 0 4** R2(config-line)# **exec-timeout 5 0**

1. The following command impedes brute force login attempts. The router blocks login attempts for 60 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the pur‐ pose of this lab.

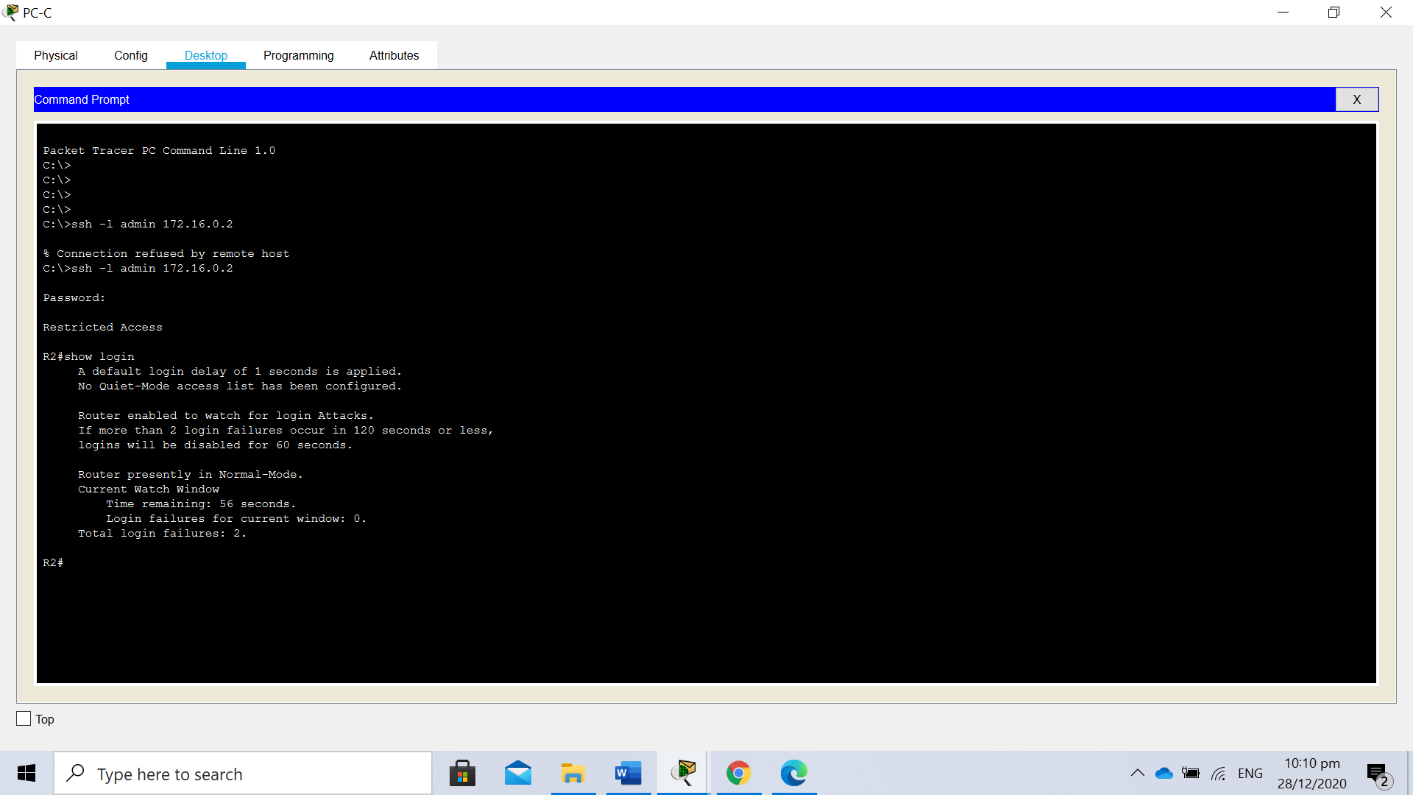
R2(config)# **login block-for 60 attempts 2 within 120**

1. From PC‐D create an SSH connection to router R2 and intentionally mistype the user and password information to see if login access is blocked after two attempts.

From your PC‐C console session on the router, issue the **show login** command.

1. After the 60 seconds has expired, SSH to R2 again and login using the **admin** username and **adminpass** for the password.

From your PC‐C console session, after you successfully logged in, what was displayed in the log?

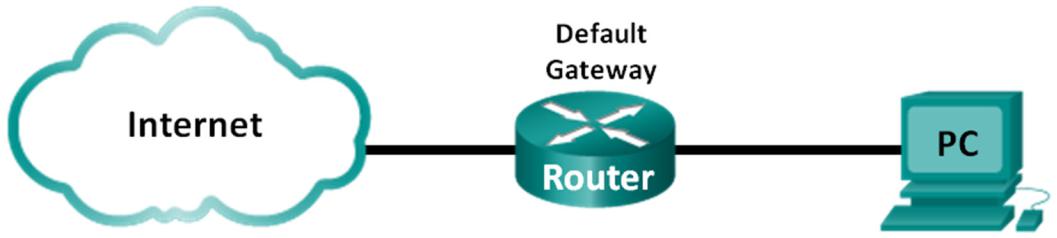


Page 10 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Task 4 ‐ Observe the TCP 3‐Way Handshake, UDP, and DNS**

**Topology**

****

Use your private PC with Internet Connectivity.

**Part 1:** **TCP 3‐Way Handshake Analysis**

**Step 1:** **Retrieve the PC interface addresses.**

Connect your PC to the switch on your workbench. For this lab, you need to retrieve your PC’s IP ad‐ dress and its network interface card (NIC) physical address, also called the MAC address.

IP address 192.168.0.3

MAC address C0-B5-D7-47-91-AB

Default gateway IP address 192.168.0.1

DNS server IP address 81.173.194.69 , 81.173.194.74

**Step 2:** **Start Wireshark and select the appropriate interface.**

**Step 3:** **Perform a website data capture.**

1. ‐ Start a data capture. Open a browser and go to www.dn.th‐koeln.de.
   * **Close (!)** the browser window to end the HTTP session, and return to Wireshark.
   * Stop the data capture.
2. By nslookup record the IP address of [www.dn.th‐koeln.de](http://www.dn.th‐koeln.de): 139.6.19.7 (2001:638:402:1300:7)
3. Check the Wireshark capture window.

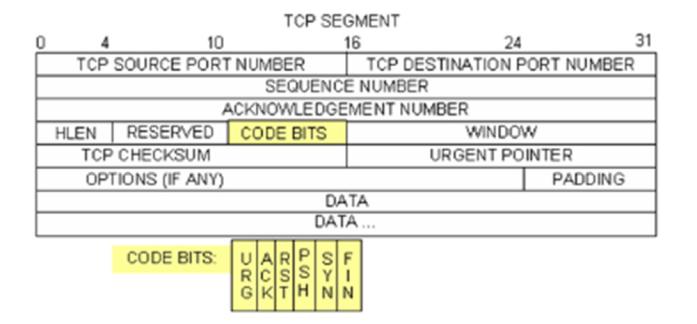
Check the **Source**, **Destination**, and **Protocol** columns.

Find the appropriate packet for the start of the first TCP session to the Webserver in this capture.

1. **Filter your capture to this 1st TCP Session to the www.dn.th‐koeln.de Webserver.**

Which Socket (IP address and Port) has been used by the webserver in the first TCP session you cap‐ tured? 2001:638:402:1300:7 port:443 (Non-authoritative)

Which Socket has been used by your Web client in the first TCP session?



2a0a:a543:d28c:0:fc9b:b9c3:3e1:d281 port:49981

**Step 4:** **Analyze TCP Segments**

The image shows a TCP datagram diagram.

Page 11 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

1. Which three TCP messages start the setup of a TCP session? **Note**: These messages are without any application data.SYN-SYN-ACK

The web client initiates the TCP session. Select the 1st TCP message of a TCP session. Which flag is set in this first TCP segment?0x002 (SYN)

Record is the initial sequence number of the web client:0

1. Which TCP flags are set in the first response from the server?0x012(SYN,ACK)

Record the sequence number and the acknowledgement number in this TCP message.

Seq No:0 Ack No:1

1. Which TCP flag is set in the TCP segment, to finish the TCP 3‐way‐handshake?FIN,ACK

Record the sequence number and the acknowledgement number in this TCP message.

Seq No:21956 Ack No:1277

**Important Note:** in all TCP segments excluding the first segment, the ACK flag is set.

1. From the TCP 3‐way‐handshake packets record the initial TCP parameters **maximum windows size** **(WIN)** and **maximum segment size (MSS)** of the web client and the web server.1024

**Note**: By the window scale (WS) factor, the window size (WIN) is multiplied, check details of the

Wirshark presentation of WS. (Answer yourself the Q: Is the DN‐Webserver multiplier 7 or 128?)128

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Web client** | **Web server** |
|  |  |  |

MSS 1440 1380

WIN 64800 64800

WS 8(multiply by 256) 7(multiply by 128)

WIN\*WS 64800\*256= 16588800 64800\*128 = 8294400

**Step 5:** **Display IP flows by Wireshark.**

1. In complex scenarios it is helpful to use additional analysis by Wireshark. For our HTTP session to www.heise.de show the TCP flow graph by selecting **Statistics – Flow Graph – TCP flow,** and display only TCP segments of the selected flow.

Graphical user interface, table

Description automatically generated

By which TCP messages is TCP closed?FIN,ACK

**Note**: In TCP closing process, the ack. number is incremented without any data transmission.

1. The web client acknowledges the received TCP segment data (number of application bytes) by TCP packets with the ACK flag and the actual acknowledgement number.

Initial HTTP **client** ack. number after TCP session setup (SYN, SYN/ACK, **ACK**):1,0/1,0

ackinitial:1

Final HTTP **client** ack. number, following the last closing FIN message(s): ackfinal: 483011

Calculate the number of Bytes M (TCP data = encapsulated HTTP data here), which has been received by the web **client** on application level.

M = ackfinal – 1 – ackinitial =

483011-1-1=483009

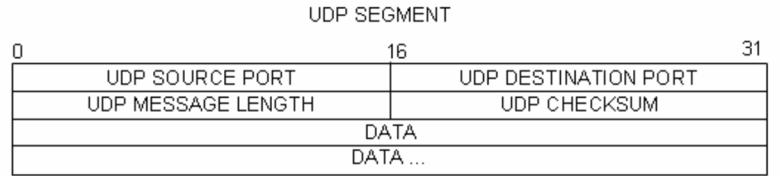
Page 12 of 14

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

**Part 2: Examine Captured DNS and UDP Packets**

**Step 1:** **Continue and Examine UDP segment using DNS query.**

From the same Wireshark capture, examine UDP by using a DNS query, as DNS is encapsulated in UDP. A UDP header only has four fields: source port, destination port, length, and checksum. Each field in UDP header is only 16 bits as depicted below.



**Note**: If you do not see any results after the DNS filter was applied, close the web browser and in the com‐mand prompt window, type **ipconfig /flushdns**.

Restart the Wireshark capture and repeat the instructions in Part 2b –2e. If this does not resolve the issue, in the command prompt window, you can type **nslookup www.google.com** as an alternative to the web browser.

1. Which client socket is used for the DNS query (IP address, transport protocol, port number)?

2a0a-a543-d28c-0-fc9b-b9c3-3e1-d281 port: 63944 length:47 checksum:0x3f39

1. Which server socket is used for the DNS query (IP address, transport protocol, port number)?

2001:4dd0:100:1020:53:2:0:1 port:53 length:150 checksum :f5488

1. Is your DNS server connected in the same subnet as your PC client?yes
2. To the MAC address of which device is the DNS query sent?c0:c5:22:f3:f5:4f
3. In case you want to prevent your network of packet fragmentation, and the MTU size is 1500 Bytes, calculate the maximum UDP segment can be transferred.63944-8= 63936

**Step 2:** **Examine DNS responses.**

1. In your own DNS capture, evaluate the DNS query response and fill out the following table for the DNS query response message.

**Note:** Students without access to the NP chapter on application protocols may check en.wikipedia.org tolearn extent about DNS from CCNA ITN chapter.

|  |  |  |  |
| --- | --- | --- | --- |
| **DNS Flags / Answers** |  | **Value** | **Suggested Meaning** |
|  |  |  |  |

**Authoritative Server** Flag 0 Source is not authority for domain

**Recursion desired** Flag 1 Recursion desired

**Recursion available** Flag 1 Server can do recursive

Answer Name [www.google.com](http://www.google.com) this the name of desired server

|  |  |  |
| --- | --- | --- |
| NP | Networks and Protocols (NP) | Prof. Dr. A. Grebe |
| CCNA ITN | Introduction to Networks (ITN) |  |

Answer **Type A Host Address**

Answer **Class IN 0x001**

Answer **Time to live 26**

Answer **Address 216.58.212.164 Query reply**

**Checkout**

When you successfully finished this Lab, record your solution.

1. Create a ***PDF file*** **ITN‐Lab3‐Result.pdf**, which includes these instructions completed by your answers. Write your answers in **red color**. You may use the comment capabilities of the free Adobe reader.
2. Save your final Packet Tracer file **ITN‐Lab3‐PT.pkt**
3. Record the running configuration of router R1 and router R2 (**show run**) in a ***text file*** **ITN‐Lab3‐Con‐** **figs.txt**
4. Upload these 3 files **ITN‐Lab3‐Result.pdf** , **ITN‐Lab3‐PT.pkt** , and **ITN‐Lab3‐Configs.txt** in Ilias.

Page 14 of 14