htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

htl donaustadt

Configure Basic Router Settings

Laboratory protocol Configure Basic Router Settings

Subject: NWT|ANGE
Class: 3AHITN
Name: Stefan Fürst, Marcel Raichle
Group Name/Number: Dumm und Dümmer/7
Supervisor: ANGE
Exercise dates:
Submission date:

Contents

1 Task definition

2 Summary

3 Complete network topology of the exercise
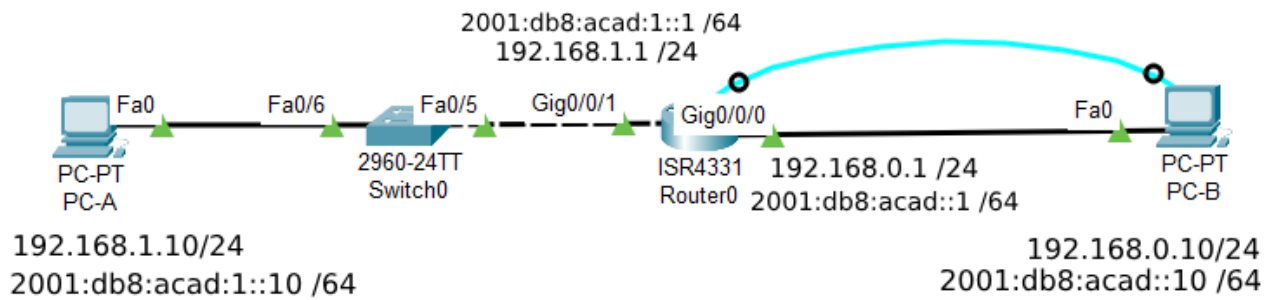
Figure 1: Complete network topology of this exercise

htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

htl donaustadt

4 Exercise Execution

4.1 Set Up the Topology and Initialize Devices

This exercise was done in Cisco Packet Tracer and the devices were placed and wired using the automatic cabling type, as all the devices are Auto-MDIX compliant anyway.
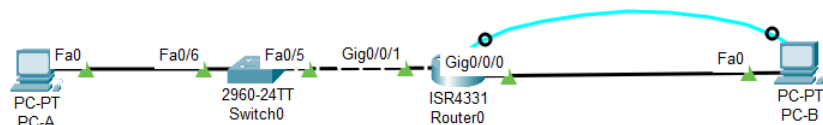

Figure 2: Network topology required for this exercise

After that, everything was turned on and the router and switch were both iniliazised and reloaded.

4.2 Configure Devices and Verify Connectivity

4.2.1 Configure the PC interfaces

The IP addresses for both PCs have been set in the IP Configuration application.

Figure 3: IP configuration for PC-A and PC-B

htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

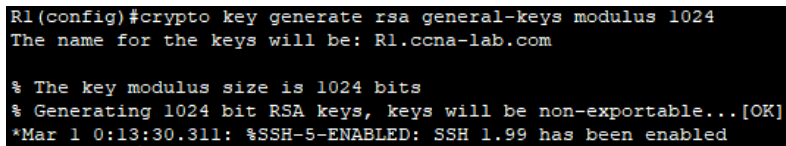htl donaustadt

4.3 Configure the router

To access the router's configuration mode, connect to the router through the console port and execute the *en* and *conf t* commands.

The following basic settings are configured using the commands listed below:

```
#setting the hostname
hostname R1
#setting the domain name of the router
ip domain name ccna-lab.com
#disable DNS lookup on mistyped commands
no ip domain lookup
#encrypt plain text passwords
service password-encryption
#setting the minimum password length to 12 characters
security passwords min-length 12
```

To set up SSH for configuring the router over the network, first, a user must be created with the *username SSHadmin secret 55Hadm!n2020* command, which creates a user named SSHadmin and sets an encrypted password.

Once the user has been created, an RSA key pair needs to be generated using the *crypto key generate rsa general-keys modulus 1024*[1] command.
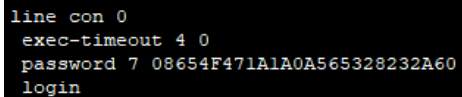


```
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:13:30.311: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Figure 4: Key pair generation

```
#setting a password to enter EXEC mode
enable secret $cisco!PRIV*
line console 0
#setting password for console access
password $cisco!!CON*
#termination of the session after four minutes of inactivity
exec-timeout 4 0
#enabeling login
login
```



```
line con 0
 exec-timeout 4 0
 password 7 08654F471A1A0A565328232A60
 login
```

Figure 5: Viewing the configuration of VTY line 0

```
#entering the configuration for lines for vty lines 0 to 4
line vty 0 4
#setting a password to access the lines
password $cisco!!VTY*
#termination of the session after four minutes of inactivity
exec-timeout 4 0
#only allowing ssh connections
transport input ssh
```

---

[1]As this is done in Packet Tracer and the hardware in the lab is outdated, the keys are limited to 1024 bit length instead of the 4096 bit length that should be used in a production environment.

```
#enabeling login using the local database
login local
```



```
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
```

Figure 6: Viewing the configuration of VTY lines 0 4

```
#createing a banner to warn that unauthorized access is prohibited
banner motd $ unauthorized access is prohibited $
```



```
Password:
 unauthorized access is prohibited

R1>
```

Figure 7: Viewing the MOTD banner

```
#enable ipv6 routing
ipv6 unicast-routing
#setting the ip addresses according to the addressing table
interface g0/0/0
ip address 192.168.0.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad::1/64
no shutdown
exit
interface g0/0/1
ip address 192.168.1.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:1::1/64
no shutdown
exit
interface loopback0
ip address 10.0.0.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:2::1/64
no shutdown
exit
```

Figure 8: Displaying the IP addresses set

```
#setting a timeout of 2 minutes after 3 failed login attempts in 60 seconds
login block-for 120 attempts 3 within 60
exit
#setting the clock
clock set 9:22:40 08 Nov 2024
```


Figure 9: Display of current time

```
#copying the current running-config to the startup-config
copy run start
```

If the router is reloaded before running this command, the running configuration will be lost, as the RAM is erased during a reload.

4.4   Verify network connectivity

5 List of figures

List of Figures