Computer Networks *(Redes de Computadores - RCOMP)* – 2025/2026

***Networking Laboratory (B308) - activities 2***

(to be undertaken in week 6, week 7 or week 8 of the course, in the second part of the laboratory class)

Accessing and managing a device through the console serial port. Initial configuration and basic security of a device. Enabling SSH access to a Cisco device. Resetting a Cisco 2811 router to factory defaults.

# 1. Guidelines on using the DEI Networking Laboratory

The DEI Networking Laboratory has three open racks, with working desks on both sides. **There are a total of six working desks next to the racks, therefore the class should be divided into up to six teams.**

Each rack holds in the upper positions four similar sets of two devices as shown in Figure 1. Each of the four sets has a Cisco Catalyst 2950 switch (with dark green panel), and below it, a Cisco 2811 router.

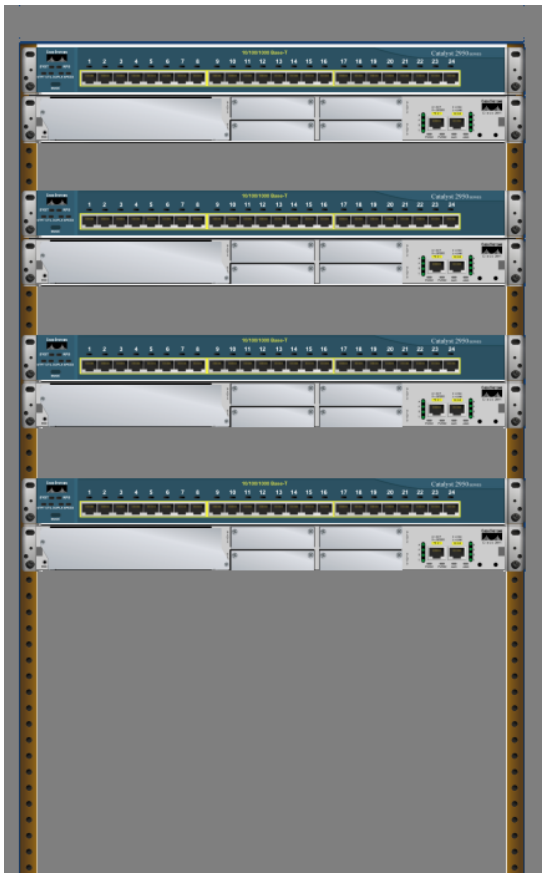

*Figure 1 - Upper part of the racks*

- There is a U unit spacing between each set.
- The power switch of the 2811 routers is at the rear panel on the left side.
- These switches don't have a power switch; you must plug or unplug the power cable at the rear panel on the right side.

**For the activities in this script:**

- Only the two upper sets of devices in each rack are to be used.
- Each team is placed at a desk next to a rack.
- The team at the right side of the rack is going to use the set at the top of the rack.
- The team at the left side of the rack is going to use the second set counting from the top.

# 2. Accessing and managing a device through the console serial port

The console of a device is the primary input/output system for human interaction, frequently it is the only mean of interaction during the device boot. Once the boot completes successfully, other alternative means of access may be available (e.g., SSH access through the network), however, if the boot fails or there is a configuration issue, those alternatives will probably be unavailable, and the console is the only option.

Some higher-level devices like servers may have their own video controller and keyboard controller, but more specialized devices like routers and switches most often have a console access through a serial terminal connection. Nowadays most hardware terminals are in museums, but we can use a standard PC with a terminal emulator (e.g., PuTTY).

Figure 2 shows the RJ45 console port of a Cisco 2811 router, at the rear panel.


*Figure 2 - The console port of a Cisco 2811 router*

The Cisco console ports and console cables are usually painted in light blue. Despite being an RJ45 connector port, it is not an Ethernet port, it is an RS232 serial port. The original specification for RS232 adopted a 25 pins D connector (DB-25), latter widely replaced by a 9 pins D connector (DB-9). A specific cable (Figure 3) is required to connect to a personal computer.


*Figure 3 - RJ45 to DB-9 roll-over console cable*

(https://blog.router-switch.com/2017/07/how-to-connect-laptop-to-router-console-port-with-ethernet-rj-45-console-cable/)

*Table 1 - Roll-over cable pinouts*

| Signal | Console Port | RJ-45 Pin | DB-9 Pin | Signal |
|---|---|---|---|---|
| RTS | 1 | 8 | 7 | CTS |
| DTR | 2 | 7 | 4 | DSR |
| TxD | 3 | 6 | 3 | RxD |
| GND | 4 | 5 | 5 | GND |
| GND | 5 | 4 | 5 | GND |
| RxD | 6 | 3 | 2 | TxD |
| DSR | 7 | 2 | 6 | DTR |
| CTS | 8 | 1 | 8 | RTS |

(Cisco ASA 5585-X Adaptive Security Appliance Hardware Installation Guide)

This console cable is also known as **roll-over cable** because, as shown in the table above, it mirrors the RJ-45 pin connections (Table 1).

And what if the laptop does not have an RS-232 serial port? Well, then there is no other option than to use an RS-232 to USB adapter, and most likely an appropriate software driver will have to be installed on the laptop.

In the market there are console RJ-45 to USB cables, though they are not plain cable wirings, they include an active RS-232 to USB adapter chip, usually embedded in the USB connector.

## 2.1. Practical activity – accessing the console of a Cisco 2811 router

- Use the appropriate serial cable to connect a PC to a Cisco 2811 router.
- In the PC, run the terminal emulator software (e.g., Putty), configure it to use the appropriate serial port (e.g., COM1), and set the speed to 9600 bps (this is the serial line speed for the console with the default configuration register 0x2102).
- If not already on, power on the Cisco 2811 router.
- Check if you can interact with the console. If prompted, skip the "initial configuration dialog"
- Check if you can enter the privileged mode (**enable** command) mode.

If you are prompted for a username and password when accessing the console of just for a password when accessing the privileged mode, this means the router has been previously configured and secured by someone. **Nevertheless, by having physical access to the device and the console, it is always possible to reset the configuration or recover from a lost password scenario.**

If you find your Cisco 2811 router is protected by passwords, before continuing, follow the proceedings described ahead in Chapter 4 about how to reset your Cisco 2811 router configuration.

### 2.2. Practical activities – initial settings of a Cisco 2811 router – name and DNS domain

We will start by giving a name to the router and setting the local DNS domain name, notice that later we are going to generate an RSA private and public key for SSH access, and those keys are stored with a name matching the router name and local DNS domain name.

At the router console, enter configuration mode, set the router name to rcomp-rt and the DNS domain name to dei.isep.ipp.pt.

```
router>enable
router#conf t
router(config)#hostname rcomp-rt
rcomp-rt(config)#ip domain-name dei.isep.ipp.pt
```

### 2.3. Practical activities – initial settings of a Cisco 2811 router – access control

As you have witnessed, by default, there's no access control to the console neither to the privileged mode. One important initial configuration is enforcing secrets for such accesses.

Enter the configuration mode and establish a secret (password) for privileged mode access:

```
rcomp-rt>enable
rcomp-rt#conf t
rcomp-rt(config)#enable secret NEW-PASSWORD-E
```

Now on, when entering the privileged mode, you will be prompted for the secret. Test it.

Access to the console is still open, however, the access to the privileged mode is not.

To establish access control on the console itself, we must first create a local user, and then, configure the console to require local user authentication (login local).

```
rcomp-rt#conf t
rcomp-rt(config)#username admin secret NEW-PASSWORD-A
rcomp-rt(config)#line console 0
rcomp-rt(config-line)#login local
```

Mind the two passwords (secrets) used here could be the same, but that's not the recommended practice, by having different passwords two levels of access control are enforced, meaning that to reach the privileged mode, two secrets must be known.

Check that now you are prompted for a username and password for accessing the console, type the **exit** command until you ultimately leave the unprivileged mode.

# 3. Accessing and managing a device through SSH

Interacting with the console requires local physical access, this means the administrator is not able to remotely manage the device and managing several devices at the same time would become a serial lines nightmare.

Once the network configuration of the device has been settled, the network itself may be used to create a channel (TCP connection) that simulates a serial line, this is called a virtual terminal (VT). To safely use this kind of access, the SSH (Secure Shell) protocol must be used, the older TELNET protocol is obsolete and totally unsafe (traffic is unencrypted).

## 3.1. Practical activity – create a testing network layout

We will start by creating a network layout with a client PC connected to an Ethernet switch, in turn connected to the **Fa0/0** port of the router (Figure 4).

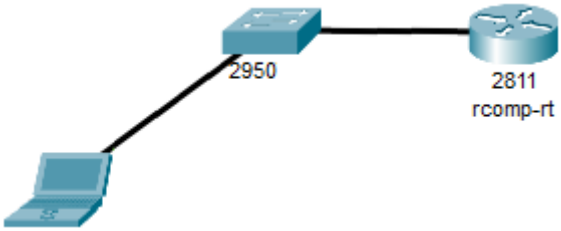


*Figure 4 - Laptop - Switch - Router*

You will need two copper patch cords. As far as your laptop has an Ethernet interface, you should use your own laptop for this activity. We will use the **10.0.0.1/24** IPv4 address for the Fa0/0 router interface, and presume the PC is being configured by DHCP, so we will create a DHCP pool in our router to automatically provide the IPv4 configuration to the client PC.

Back to the router's console, let us configure the IPv4 address and activate the Fa0/0 interface:

```
rcomp-rt(config)#interface Fa0/0
rcomp-rt(config-if)#ip address 10.0.0.1 255.255.255.0
rcomp-rt(config-if)#no shutdown
```

The link lights should be now on at the router's Fa0/0 interface and at the switch port on the other end of the cable.

Now let us create a DHCP pool, because this is an isolated network, no default gateway or DNS servers will be established for this pool:

```
rcomp-rt(config)#ip dhcp pool MYLAN
rcomp-rt(dhcp-config)#network 10.0.0.0 255.255.255.0
```

Use a copper patch cord to connect the PC's Ethernet network interface to a switch port, check that the corresponding link light is on.

Assess the IPv4 connectivity between the PC and the router by using the ping command at the PC's command prompt:

```
ping 10.0.0.1
```

If successful, proceed, otherwise try to solve the issue. Check if the PC is getting the IPv4 configuration through DHCP.

### 3.2. Practical activity – enable SSH access at the router

Now that we have IPv4 connectivity between the laptop and the router, let's go back to the console of the router to configure the SSH access. We will start by generating an RSA private/public keys pair, the default key size is 512 bits and nowadays that is unsafe, **enter a key size of 2048 bits**.

The default SSH version is 1, and that is not safe either, so we will change to version 2.

```
rcomp-rt(config)#crypto key generate rsa
rcomp-rt(config)#ip ssh version 2
```

Notice that the "crypto key generate rsa" command line would fail if the router's name or the local DNS domain name were not set.

We have already created a local user ("admin"), so the missing step to be able to remotely access the router through SSH is configuring the virtual terminals at the router to allow SSH access and local users authentication:

```
rcomp-rt(config)#line vty 0 4
rcomp-rt(config-line)#transport input ssh
rcomp-rt(config-line)#login local
```

This sequence of commands configures 5 virtual terminals (0 to 4) to allow SSH only access, the user login authentication is local.

The configurations enforced so far are stored in volatile memory, if the device is reset or powered off all will be lost. We can save the current running configuration (**running-config** in volatile memory) to the **startup-config** file, stored in non-volatile memory (NVRAM) by running the following copy command:

```
rcomp-rt#copy running-config startup-config
```

Notice that normally the **startup-config** file in NVRAM is automatically loaded into memory when the device boots.

**We can check the SSH access to the router command line, at the laptop:** start a terminal emulator (e.g., PuTTY), but instead of selecting a serial line connection, select the SSH protocol and specify the router's IPv4 address (**10.0.0.1**).

Use the admin user credentials to access the router's command line.

# 4. Resetting a Cisco 2811 router configuration

The access to a device's console and the physical access to a device **grants total power over a device, this is something we can never forget**, that is why servers, routers, switches, and other devices must be inaccessible to the public, and carefully closed in dedicated rooms with physical access control.

For every kind of device, manufacturers have created a recovery proceeding for emergencies, some are somewhat peculiar, but most often they encompass power cycling the device and intervention at the console during the boot.

Common emergency scenarios are a forgotten password, or some misconfiguration that prevents the normal administrative access to the device.

In Cisco device, you have access to the privileged mode, to reset the configuration you can simply erase the startup-config file stored in NVRAM with the following command: **`erase startup-config`**

## 4.1 The ROM Monitor (ROMMON)

The ROM Monitor is the bootloader software that initializes Cisco devices like routers and switches; after initializing the hardware it will ultimately load the Cisco IOS operating system and pass the control to it. The ROM Monitor is itself a tiny operating system with its own command line and specific commands.

For a Cisco 2811 router, there are at least two ways of accessing the ROM Monitor command prompt:

- By sending the break signal through the console serial line within the first minute after the device's boot.
- By making the Cisco IOS image unavailable to the ROM Monitor during the boot. In the case of a 2811 router that is easy to do because the Cisco IOS image is stored at the compact flash card, if we remove it, on the next boot we are going to be left at the ROM Monitor command prompt.

Once at the ROM Monitor prompt it is possible to change some low-level device configurations, and for instance change the boot process, making it ignore the configuration file (startup-config), this means using the factory-default configuration.

One way to access the ROM Monitor is by **sending the BREAK signal through the console serial connection**, within the first minute of the router's boot.

It looks quite easy, often not so simple is knowing how to send the BREAK signal, most modern laptops don't even have a BREAK key, often for a PC with a standard keyboard CTRL+BREAK may work with some terminal emulators (e.g., Putty). **On the other hand, most terminal emulators have an explicit menu option to send a break signal.**

## 4.2. The Cisco configuration register

Cisco routers and switches have a 16-bits internal register (non-volatile) called configuration register. The value of the configuration register changes the way the device operates, namely during the boot.

We can see the current value of the configuration register by looking at the last line of the output of the **show version** command at the privileged level of the Cisco IOS:

```
Device#   PID                   SN
------------------------------------------------
*0        CISCO2811/K9          FTX10178MNW-


Configuration register is 0x2102
```

The **0x2102** is the default value and it implies that the Cisco IOS operating system, once started, will automatically load, and apply the **startup-config** file stored in the NVRAM. By changing the value to

**0x2142**, that behaviour changes and the Cisco IOS operating will no longer load the **startup-config** file on boot.

We can change the value of the configuration register both at the ROM Monitor prompt and at the Cisco IOS operating system prompt:

- At the ROM Monitor prompt, by using the **confreg** command.
- At the Cisco IOS operating system prompt, by using the **config-register** command.

### 4.3. Practical activity – resetting the Cisco 2811 router configuration to factory defaults

We need access to the console, even if we are not able to login (forgotten password), and we need physical access to the router so we can use the power switch.

The first step is accessing the ROM Monitor command prompt:

- At your terminal emulator connected to the router's console, try to figure out how could you send the break signal, there might be a menu option for that.
- Switch off the router (power button), wait some seconds and power it up again.
- At the terminal, send a break signal. To be effective this must be done in less than a minute after powering up.

You should now be at the ROM Monitor prompt:

```
rommon 1>
```

(The number at the prompt increments with every newline)

Change the value of the configuration register to **0x2142**, and then reboot the device through the **reset** ROM Monitor command.

```
rommon 1>confreg 0x2142
rommon 2>reset
```

Because the **startup-config** file is not loaded, the device now has the factory-default configuration, this means there's no console access control and no enable secret.

The next steps depend on our goals:

- If we want to preserve the previous configuration and just make some changes to it (most often change the secrets), then we would: enter privileged mode and load the startup-config (**copy startup-config running-config**), then enter configuration mode and enforce the required changes (e.g., change the secrets).
- Otherwise, we will attain a fresh device with no configurations whatsoever, in this class it's what we want.

In either case there are two additional final steps required: save the current configuration to the startup-config file, and change the configuration register in order for it to be loaded in following boots:

```
router#copy running-config startup-config
router#conf t
router(config)#config-register 0x2102
```