Introduction to Cisco router configuration

AFNOG 2001 Workshop
07 to 11 May 2001
Accra - GHANA

By:
Adiel AKPLOGAN
CAFE Informatique S. A. - TOGO
E-mail: adiel@akplogan.net - Web: http://www.akplogan.net
Introduction

- Router are intelligent equipments used for packet forwarding and network interconnection.

- Description
  - Front panel
  - Back panel

- Need to process information and data

- For that purpose they run a real operating system

- IOS: Internetworking Operating System
Router components

- Like a computer they are composed of:
  - Microprocessor to run the IOS
  - RAM to store data, run programs and buffer data.
  - NVRAM to store instruction for performing the self test of the device. It also contain a subset of of the l'IOS.
  - Flash memory: like an NVRAM that can be erase and rewrite electronically (used like PC use disk storage). The copy of IOS the router run is store on it.
  - Network Interfaces: Primary for the router.
CISCO IOS

- **Accessing the router:**
  - By the Console port
  - Or from network

- **Login to the router:**
  - With a password stored in the config file.
    
  Password:
  - Through access server (TACACS+, RADIUS)
    - TACACS (Terminal Access Controller Access Control System)
    - RADIUS (Remote Access Dial-In User Service)

- **two mode**
  - user exec mode
    
    routeur-t2>
  - privilege exec mode (enable/disable)
    
    Routeur-t2#
CISCO IOS

- the command are automatically interpreted by the user interface.

  Routeur-t2>show version
  - You can abbreviate the commands
  Routeur-t2>sh ver
  - help available at any level
  E.g.: routeur>?  
  - Access command history trough direction key on your keyboard (up and down) –*show history* to see what is in the buffer
  - Filter the output of command
  ex: routeur>sh ver |include
  exclude
  begin key
CISCO IOS

- Editing feature on Cisco IOS
  - Cursor Movement:
    - Ctrl+A → cursor to the beginning of the line
    - Ctrl+E → cursor to the end of the line
    - Ctrl+B → cursor to the beginning of the previous word
    - Ctrl+K → delete all characters from the cursor to the end of the command line
    - Ctrl+U or X → delete from the cursor to the beginning
    - You can recall deletions and past them on the line of the cursor
      - Ctrl+Y paste the most recent deletion at the cursor
      - Esc+Y recall the next buffer entry and paste at the cursor

- You can turn off terminal editing
  # terminal no editing
Router configuration

- Three possible methods to configure a router:
  - Terminal (entering the commands directly)
  - From memory (copy config. from RAM to NVRAM)
  - From network (copy configuration from an tftp server)

  - For this track we will address mostly terminal configuration by accessing the routers through the console port
Router configuration

- user exec mode ">
- privilege exec mode "#"
- configuration "(conf)#"
  - interface "(conf-if)#"
  - line "(conf-li)#"
  - router "(config-router)#"
Terminal configuration mode

- Enter configuration mode
  from your FreeBSD machine connect to the router using the serial interface and configuration cable provide (to be connect to the console port)

    /etc/remote (to see the device configure to be used with "tip")

you will see at the end, a line begin with cuaa0c… (you can change it to cisco)

bash$ tip cuaa0c (or cisco)

router>
routere>enable
rouuteur#
Configuration (cont'd)

- **Read the router configuration**
  
  ```
  routeur#show running-config
  ```

- **Summary of interfaces**
  
  ```
  routeur#show interface
  routeur#show interface brief
  ```

- **The first thing we should do is to set the name of our router.**
  
  ```
  routeur# configure terminal
  routeur(config)# hostname router-X
  ```
  
  (where X stand for you table letter)

  ```
  router-X(config)#
  ```
  
  - **You may optionally want to add a banner**

  ```
  router-X(config)#banner motd #AFNOG success#
  ```
Interface configuration

- Set the enable password:
  
  ```
  router-X(config)# enable password t2@afnoq
  ```

  - If you see in your config file, you will see that the enable password is displayed in clear text -- that is not safe, you have to encrypt it.

  ```
  router-X(config)# service password-encryption
  router-X(config)# enable secret "your pswd" (MD5 encryption)
  ```

- To configure interface you should go to interface config menu
  
  ```
  router-X(config) interface ethernet0 (or 0/x)
  router-X(config-if)#
  ```

- Save your config
  
  ```
  router-X #copy running-config startup-config
  ```
Manage configuration file

- You can manipulate file in router. The most common manipulation is the copy.
  
  router-X#copy run star
  router-X#copy running-config tftp
  
  *Copy the active config file to a tftp server on the network*

  router-X#copy tftp running-config
  
  *Copy the backup config file from tftp server to the active configuration file.*

- You can specify on your configuration file where you want the router to boot from
  
  router-X# boot system flash afnog.ios
  
  - You can have many boot method set on your config file
Configuration wizard

- It is possible to configure Cisco router through an interactive configuration mode.
  - Automatically start on router without config store on the NVRAM
  - From the command line interface
    
    `router-X#setup`
IOS Upgrade

- The IOS reside in the router as a file stored in flash memory. It is run directly from there (small routers), or from a copy put in the RAM at boot time.
  - For small router:
    - Use of **flash load helper utility**: The flash load helper will reboot the router using the ROM-based IOS and copy the new IOS to flash.
Basic security configuration

- Some commands used to secure your router configuration:

  **GENERAL**
  - enable secret
  - service password-encryption
  - no service tcp-small-server
  - no service udp-small-server
  - no service finger
  - no cdp running
  - no cdp enable
  - logging
  - no ip source-route
  - access-list

  **no ip proxy-arp**
  - route 0.0.0.0 0.0.0.0 null 0 255

  **INTERFACES**
  - no ip-direct-broadcast
  - iaccess-group *list* in

  **LINES**
  - access-class list in
  - transport input
  - login
Securing your router login/access

- You can secure your router access by using authentication server access login.
  - TACACS+ (proprietary)
  - RADIUS (tiers – Lucent, Merit…)
    - They are all available free on the network

- Secure access by packet filtering
Authentication server setup

- **Installation**
  - Download the binary source code
    - TACACS+ : ftp-eng.cisco.com/pub/tacacs
    - RADIUS : [www.freeradius.org](http://www.freeradius.org)
  - Compile, Install and configure

- **Enable authentication on the router**
  - TACACS+
    ```
    aaa new-model
    aaa authentication login default group tacac+ enable
    aaa authentication enable default group tacac+ enable
    aaa accounting exec start-stop group tacac+
    ```
    ```
    ip tacacs source-interface
    tacacs-server host 215.20.110.1 port xx
    tacacs-server key trstech#01
    ```
Authentication server setup

- **Activate authentication on the router**
  - RADIUS

```
aaa new-model
aaa authentication login default group radius enable
aaa authentication enable default group radius enable
aaa accounting exec start-stop group radius

ip radius source-interface xxxx
radius-server host 215.20.110.1 auth-port 1812 acct-port 1813
radius-server key t2@afnog
```
Using up access lists

- **The ACL**
  - Access Control Lists
    - IP (1 - 99)
    - IP extend (100 – 199)
Securing with access lists

- Egress and Ingress filtering
  - IP
    access-list 4 permit 208.224.122.73
    access-list 4 permit 216.226.223.158
  - IP EXTEND
    access-list 110 deny ip host 0.0.0.0 any
    access-list 110 deny ip 10.0.0.0 0.255.255.255 any
    access-list 110 deny ip 172.16.0.0 0.15.255.255 any
    access-list 110 deny ip 192.168.0.0 0.0.0.255 any
    access-list 110 deny ip 205.224.122.0 0.0.0.255 any
    access-list 110 deny ip 127.0.0.0 0.0.0.255 any
    access-list 110 deny tcp any host 205.224.122.3 eq telnet
    access-list 110 deny tcp any host 205.224.122.3 eq www
    access-list 110 deny tcp any host 205.224.122.3 eq finger
    access-list 110 deny tcp any host 205.224.122.1 eq ftp
    access-list 110 permit ip any any
    access-list 110 permit tcp any any
  - Apply it to interface
    ip access-group 110 in (serial Interface)
    access-class 4 in (vty)
Manage router logs

- Logs
  - Directly on the router
  - To a remote server with `syslogd` (Unix)

- Logs formats
  
  Mm/dd/yyyy:hh/mm/ss:MLS-Mnemonic:description
  
  Oct 30 23:21:13.827: %MLS-3-LINK-3-UPDOWN: Interface Async75, changed state to down

- Message Log System (MLS) severity

<table>
<thead>
<tr>
<th>0 – Emergency</th>
<th>3 – Error</th>
<th>6 – Informational</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Alert</td>
<td>4 – Warning</td>
<td>7 – Debugging</td>
</tr>
<tr>
<td>2 – Critical</td>
<td>5 – Notification</td>
<td></td>
</tr>
</tbody>
</table>
Router logs

- **stup**
  - **Logging on the router**
    - set logging session [console] enable
    - set logging timestamp
    - set logging level all 5
    - set logging buffer size of the buffer that store logs

- **Logging on a unix server**
  - **On the server side**
    - Verify that syslogd is uninstalled and running
    - Add the line bellow to /etc/syslogd.conf
      user.debug /var/log/cisco.log
    - create the file cisco.log and give it the good right
    - restart syslogd
  - **On the router side**
    - set logging server ip_adresse
Password recovery

- Password loss:
  - Save the current register configuration: it is usually 0x2102 or 0x102
  - Restart the router and press Break (Alt+break – depend on which terminal you are using) within the 60s after the boot process begins to stop the boot process from flash.
  - `ROMMON> confreg 0x2142 (boot from flash without loading configuration)`
  - Enter `reset` at the prompt >
  - Answer `no` to the autoconfig question
Password recovery (cont'd)

Router>enable
Router# config mem
Router#sh run
Router#config term
Router(config)#enable secret "new passwd"
Router(config)# config-register 0x2102
Router#wr mem

Reboot the router