TEIN2 Kick-Off Workshop

Basic Routing

Iljoon Hwang

Yasuo Tsuchimoto

Course structure (1)

- Time table
  - 9:00 – 10:30
  - 10:45 – 12:15
  - 13:30 – 15:00
  - 15:15 – 16:45
- Day 1
  - Router Management
  - Security
  - Network Management

Course structure (2)

- Day 2
  - RIP
  - OSPF
  - Introduction of BGP
- Day 3
  - Basic BGP Configuration

Router Management

How to play with Cisco router

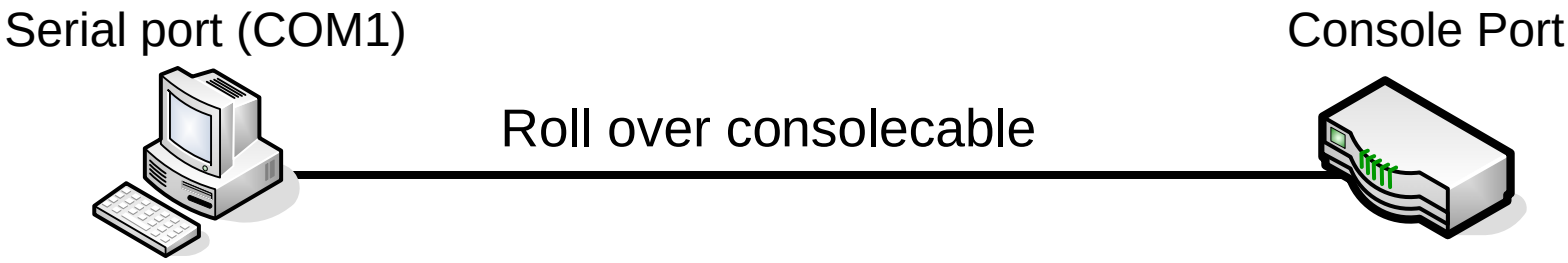
- Console
  - Using serial port of computer
  - Dumb terminal
  - Terminal emulator
- AUX
  - Connect modem
  - Accept access through modem
- Via network
  - telnet
  - http
  - Must be configured network properly

Terminal emulator

- Emulate dumb terminal
  - tip, cu or kermit as UNIX applications
  - Teraterm or Hyperterm as Windows applications
- How to configure the terminal emulator
  - COM port or Device name
  - Speed (9600)
  - Databit (8)
  - Parity (NONE)
  - Stop bit (1)
  - Flow control (NONE)

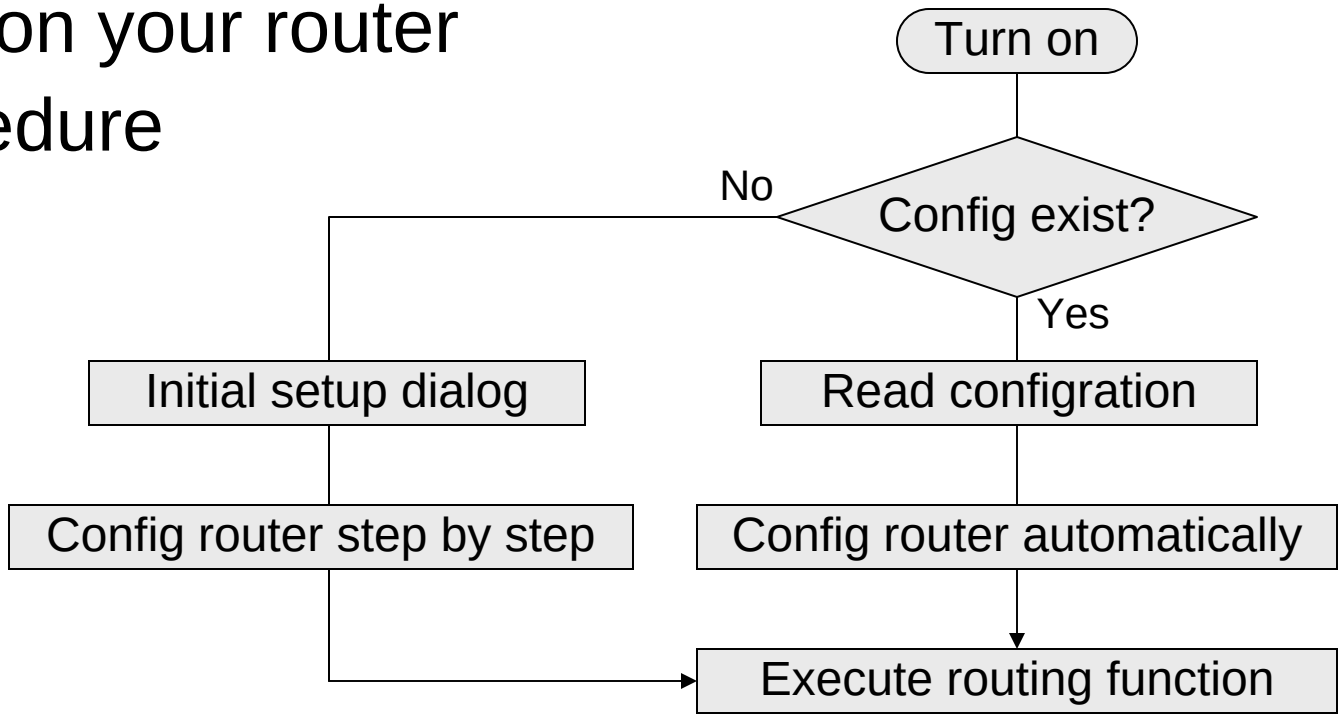
Before you turn on your Cisco router

- Please connect your router and pc with roll over cable
  - Console port on router side
  - Serial port on PC side
- Execute terminal emulator



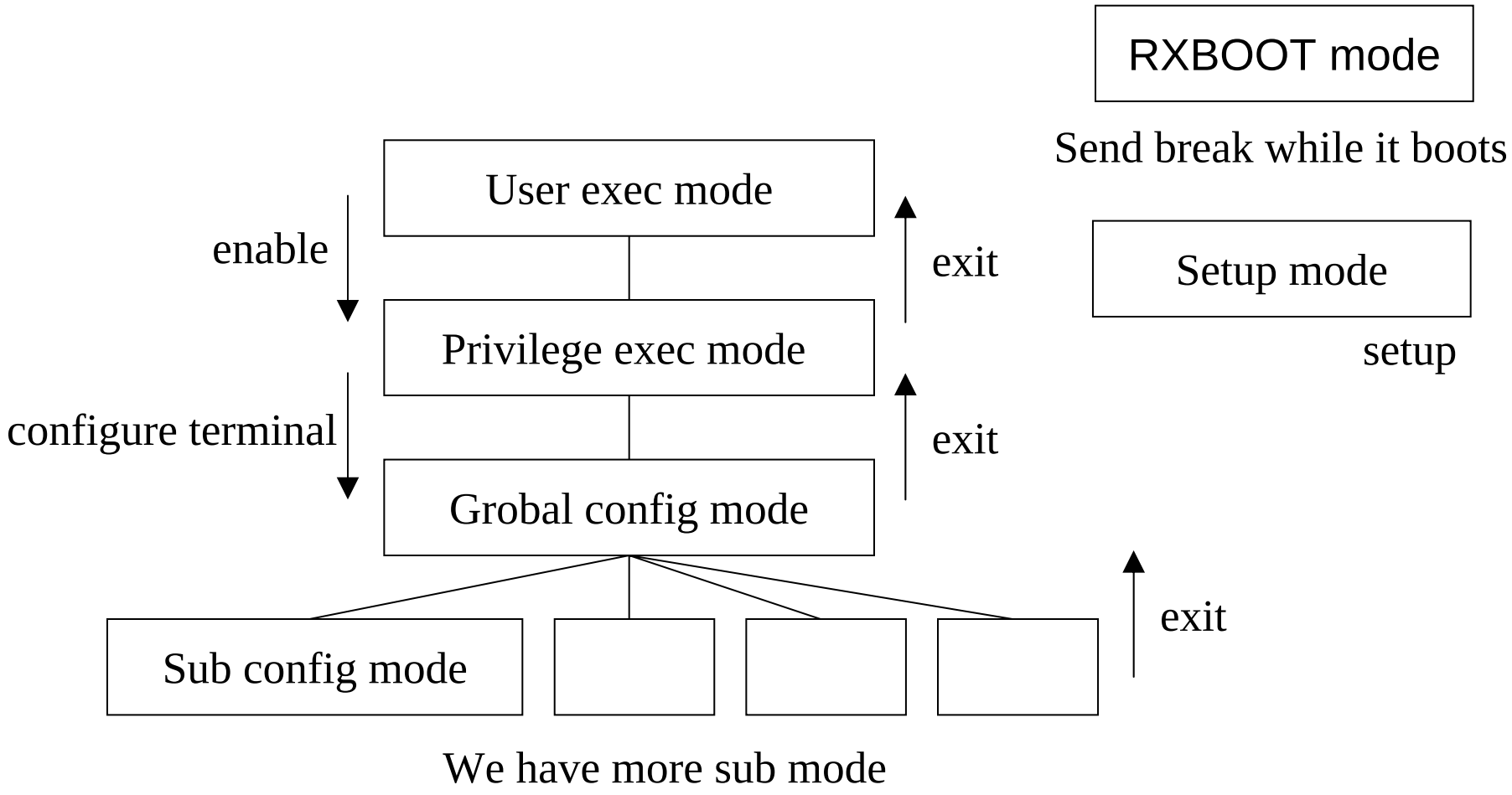
Turn on your router

- Then turn on your router
- Boot procedure



- Type Ctrl-C to avoid initial setup dialog

Several mode on cisco router



prompt

- User exec mode

  Router>
- Privilege exec mode

  Router#
- Global configuration mode

  Router(config)#
- Sub config mode

  Router(config-submode)#

Let’s start to play with a router

Basic Cisco router operation

- Use command line interface
  - All configuration should be done from CLI
  - Please remember basic commands

Command line editing

Tab	Completes the command
?	List the available commands
Ctrl-b	Move the cursor to the left
Ctrl-f	Move the cursor to the right
Ctrl-a	Move cursor to the beginning of the line
Ctrl-e	Move cursor to the end of the line
Ctrl-p and Ctrl-n (↑ and ↓)	Move up and down in the hisotry buffer
Ctrl-d	Delete one character over the cursor
Ctrl-k	Delete all charactors from the cursor to the end of line

Command line string search

- Output modifier

```
cisco1.fujisawa#show hardware ?
  |  Output modifiers
  <cr>
```

- Output modifier works as a UNIX pipe

```
cisco1.fujisawa#show running-config | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
```

How to read the config file

- To read running configuration

  show running-config

- To read stored configuration

  show startup-config

※ please run this command under the privilege mode

Structure of configuration file (1)

```
Current configuration : 2657 bytes
version 12.2
service password-encryption
!
hostname cisco3.fujisawa
!
enable secret 5 $1$RXPo$fA6UvqJCcATYIdVs/7RNO1
enable password 7 062E1735665B07320A
!
username wide privilege 15 password 7 151D190D4839242A7D6A
clock timezone JST 9
ip subnet-zero
no ip source-route
ip name-server 203.178.136.36
ip name-server 203.178.136.62
!
interface Ethernet0
 description Fujisawa-2.net
 ip address 203.178.137.114 255.255.255.240
 no ip proxy-arp
 no cdp enable
!
interface Serial0
 description TRL (to 192.156.220.69)
 bandwidth 128
 ip unnumbered Ethernet0
 encapsulation ppp
 shutdown
 no cdp enable
!
```

Global configuration

Interface configuration

Structure of configuration file (2)

```
router rip
 version 2
 passive-interface Serial0
 passive-interface Serial1
 network 203.178.137.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.178.137.113
ip route 192.156.220.0 255.255.255.0 Serial0
ip route 202.25.80.0 255.255.240.0 Serial1
no ip http server
ip pim bidir-enable
!
line con 0
 exec-timeout 15 0
 password 7 0209165A4715002F1917
 login local
 escape-character 3
line aux 0
 access-class 2 in
 exec-timeout 15 0
 password 7 130A0513471F0B247E7D
 login
 transport input all
 escape-character 3
line vty 0 4
 access-class 2 in
 exec-timeout 15 0
 password 7 0700334D021A160B424B
 login local
 escape-character 3
!
end
```

Routing configuration

IP related configuration

Console configuration

AUX configuration

VTY configuration

IOS Software management

IOS software management

- IOS is kept in flash memory
  - Use command to check the flash

```
# show flash

System flash directory:
File  Length   Name/status
  1   16422664  c2500-is-l.122-15.T13.bin
[16422728 bytes used, 354488 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

Basic idea of IOS software management

- Backup the IOS to TFTP server
- Download the new IOS from TFTP server
- Reload the router
- Check status of flash memory
  - READ / WRITE
  - READ ONLY

We need to set up the network connectivity

Setting up the interface

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface ethernet 0
Router(config-if)#ip address 192.168.0.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
*Mar  1 00:10:55.983: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
Router(config-if)#exit
Router(config)#exit
Router#
*Mar  1 00:11:06.003: %SYS-5-CONFIG_I: Configured from console by console
```

Assign IP address to PC

- Check the network connections
  - Use property of Local Area Connection
  - Check the property of Internet Protocol
    - You can assign IP address on this window
  - Please assign
    - IP address: 192.168.0.2
    - Subnetmask: 255.255.255.0
- Execute tftp server
  - WinAgents TFTP Server
  - http://www.tftp-server.com/

Backup IOS on your router

```
Router#copy flash tftp
Source filename []? c2500-is-l.122-15.T13.bin
Address or name of remote host []? 192.168.0.1
Destination filename [c2500-is-l.122-15.T13.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                (snip)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
16422664 bytes copied in 305.040 secs (53838 bytes/sec)
Router#
```

- This command copy IOS to tftp server
- If it is not working
  - Please make sure that you run tftp server and firewall

Erase IOS

```
Router(boot)#erase flash

System flash directory:
File  Length   Name/status
  1   16422664  c2500-is-l.122-15.T13.bin
[16422728 bytes used, 354488 available, 16777216 total]

Erase flash device? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
ee ...erased
Router(boot)#
```

- Check the configuration register
  - 0x2102 normal
  - 0x2101 change flash READ/WRITE mode
  - 0x2142 ignore NVRAM

  Router#show hardware

How to change configuration register

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#config-register 0x2101
Router(config)#exit
Router#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

Router(boot)>show flash

System flash directory:
File  Length   Name/status
  1   16422664  c2500-is-l.122-15.T13.bin
[16422728 bytes used, 354488 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

Router(boot)>
```

Download IOS from tftp server

Router(boot)#copy tftp flash

System flash directory:
No files in System flash
[0 bytes used, 16777216 available, 16777216 total]
Address or name of remote host [255.255.255.255]? 192.168.0.1
Source file name? c2500-is-l.122-15.T13.bin
Destination file name [c2500-is-l.122-15.T13.bin]?
Accessing file 'c2500-is-l.122-15.T13.bin' on 192.168.0.1...
Loading c2500-is-l.122-15.T13.bin from 192.168.0.1 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]

Copy 'c2500-is-l.122-15.T13.bin' from server
  as 'c2500-is-l.122-15.T13.bin' into Flash WITH erase? [yes/no]yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
ee ...erased
Loading c2500-is-l.122-15.T13.bin from 192.168.0.1 (via Ethernet0): !!!!!!!!!!!!
!!!

Don’t forget to change back the configuration register

Boot from TFTP server

- You can read IOS on tftp server on boot

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#boot system tftp c2500-is-l.122-15.T13.bin 192.168.0.1
Router(config)#exit
Router#

#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by cisco Systems
2500 processor with 14336 Kbytes of main memory

%SYS-4-CONFIG_NEWER: Configurations from version 12.2 may not be correctly under
stood.
Loading c2500-is-l.122-15.T13.bin from 192.168.0.1 (via Ethernet0): !!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Configuration management

Back up router configuratoin

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.0.1
Destination filename [router-confg]?
!!
436 bytes copied in 4.388 secs (99 bytes/sec)
Router#
```

Restore configuration

```
Router#copy tftp running-config
Address or name of remote host []? 192.168.0.1
Source filename []? router-confg
Destination filename [running-config]?
Accessing tftp://192.168.0.1/router-confg...
Loading router-confg from 192.168.0.1 (via Ethernet0): !
[OK - 436 bytes]

436 bytes copied in 10.268 secs (42 bytes/sec)
Router#
*Mar  1 00:03:08.723: %SYS-5-CONFIG_I: Configured from tftp://192.168.0.1/router
-confg by console
```

Compress configuration

- If NVRAM is not large enough for configuration
  - You can compress configuration

  Router(config)# service compress-config

  - If it is not necessary to compress
    - You should not use this function
  - Or try to use newer IOS
    - Newer IOS may have better syntax to describe the configration

System logging

Logging

- Syslog is the UNIX tool which can keep logs
- One syslog server can hold several cisco’s log

- Please check your system has syslog or not

syslog configuration

- Configuration file : /etc/syslog.conf

```
local6.*                    /var/log/cisco.log
```

- Check the syslog option
  - You must put “-r” option to receive the data from network
- Check the firewall configuration, too
  - iptables may refuse the data from network

syslog configuration (2)

- syslogd option
  - /etc/sysconfig/syslogd

  SYSLOGD_OPTIONS="-r -m 0"

- iptables
  - /etc/sysconfig/iptables

  -A INPUT –p udp –dport 514 –s 192.168.0.2 –j ACCEPT
  - Restart iptables

  # service iptables restart
  - Check the current filter list

  # iptables -L

Commands for logging

no logging console
logging trap debugging
logging facility local0-7
logging syslog server' IP address

service timestamps debug
service timestamps log

datetime	put the date and time
Msec	put the
localtime	use the local time
show-timezone	put timezone info on log

Interface configuration

Interface configuration

- Use interface command to configure interface
  - Please don’t forget “no shutdown”
- Basic interface configuration
  - Configure IP address and netmask
  - Specify the usage
  - Configuration for security
  - Configuration for routing protocol

Standard interface configuration

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface ethernet0
Router(config-if)#ip address 192.168.0.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#description to Lab main switch
Router(config-if)#no ip redirects
Router(config-if)#no ip directed-broadcast
Router(config-if)#no ip proxy-arp
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

IP unnumbered

- When we use point to point link
  - We can configure the network with IP unnumbered
  - The network must be point-to-point
  - We should set up the loopback interface

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial0
Router(config-if)#ip unnumbered loopback 0
Router(config-if)#no ip redirects
Router(config-if)#no ip directed-broadcast
Router(config-if)#no ip proxy-arp
Router(config-if)#description To TEIN2 Vietnam NOC
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Loopback interface

- Cisco router refers loopback interface for…
  - BGP Update source
  - Router ID for routing protocol
  - NTP source interface
  - Syslog source interface

As far as we need to distinguish router,
we can use loopback interface

Configuration of loopback interface

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface loopback 0
Router(config-if)#description Loopback interface on JProuter
Router(config-if)#ip address 10.0.0.1 255.255.255.255
Router(config-if)#no ip redirects
Router(config-if)#no ip directed-broadcast
Router(config-if)#no ip proxy-arp
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Interface status checking

```
Router#show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e3e.488c (bia 00e0.1e3e.488c)
  Description: to Lab main switch
  Internet address is 192.168.0.2/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:34, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     166 packets input, 26670 bytes, 0 no buffer
     Received 114 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1492 packets output, 152504 bytes, 0 underruns
     48 output errors, 0 collisions, 6 interface resets
     0 babbles, 0 late collision, 0 deferred
 48 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Check the statistics summary

```
Router#  show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface            IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
-----------------------------------------------------------------------
* Ethernet0              0     0    0     0     0    0     0    0    0
* Loopback0              0     0    0     0     0    0     0    0    0
  Serial0                0     0    0     0     0    0     0    0    0
  Serial1                0     0    0     0     0    0     0    0    0
* Virtual-Access1        0     0    0     0     0    0     0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
Router#
```

Time Adjust

NTP

- Network Time Protocol
  - It is very important to adjust the timer
  - NTP is useful protocol

- Configuration

Router(config)# ntp peer 192.168.0.1

Router(config)# ntp server 192.168.0.1

Check NTP configuration

Router#show ntp status

Router#show ntp associations

Securing the router

Shutdown unnecessary service(1)

- Disable finger function
  Router(config)#no ip finger
  Router(config)#no service finger (12.0 or later)
- Disable X.25 PAD
  - Under the recent version of IOS, this is default
  Router(config)#no service pad
- Disable all service below 20
  Router(config)#no service udp-small-servers
  Router(config)#no service tcp-small-servers
- Disable bootp server
  Router(config)#no ip bootp server
- Disable http server
  Router(config)#no ip http server

Shutdown unnecessary service(2)

Router(config-if)#no ip redirects

The router will not send redirect message through the same interfaceon with it was recieved

Router(config-if)#no ip directed-broadcast

Disable the translation of directed broadcast to physical broadcast. We can prevent the smurf attack.

Router(config-if)#no ip proxy-arp

Disable proxy arp function, which backbone router won’t use this function

Disable CDP

- Cisco Discovery Protocol
  - CDP can find the Cisco router on right next

  Router#show cdp neighbors detail
- Disable CDP within an entire router

  Router(config)# no cdp run
- Disable CDP within single interface

  Router(config-if)# no cdp enable

Login banners

- You may not need to set up banners
  - But it is easy to find out which router you're logged in
  - You MUST not put any information such as…
    - Some information which someone can guess username or password
    - Router model and hardware information

Configuration of banner

```
Router(config)#banner login $
Enter TEXT message.  End with the character '$'.
            === TEIN2 Network Router ===

      * please disconnect if your are not an operator of TEIN2 network
      * If you have any question about TEIN2 Network, please contact
        info@tein2.net

$
Router(config)#exit
Router#
```

How does it look like?

```
% telnet 192.168.0.2
Trying 192.168.0.2...
Connected to 192.168.0.2.
Escape character is '^]'.

            === TEIN2 Network Router ===

        * please disconnect if your are not an operator of TEIN2 network
        * If you have any question about TEIN2 Network, please contact
          info@tein2.net



Password required, but none set
Connection closed by foreign host.
%
```

Protect password

- To be a privileged user
  - enable password
    - Very weak, reversible, MUST NOT used
    - But better to remain if the boot ROM is older than 11.x
  - enable secret
    - Non reversible
    - Strong password
- Other password can be encrypted

  Router(config)#service password-encryption
  - This is also reversible
  - But it is better than nothing

Router access (1)

- Protect your console and VTY
  - All interface should be configured timeout timer

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#exec-timeout 10 0
Router(config-line)#line aux 0
Router(config-line)#exec-timeout 10 0
Router(config-line)#line vty 0 4
Router(config-line)#exec-timeout 10 0
Router(config-line)#exit
Router(config)#exit
Router#
```

- TCP-keepalive should be configured

```
Router(config)#service tcp-keepalives-in
```

Router access (2)

- Access lists on the VTY ports
  - We can limit the access to the VTY ports
  - Telnet should be accepted from secure network
  - Or use ssh if possible

```
Router(config)#access-list 10 permit 203.159.0.0 0.0.255.255
Router(config)#access-list 10 permit 203.178.143.0 0.0.0.255
Router(config)#access-list 10 deny any

Router(config-line)#access-class 3 in
```

User authentication

- Cisco router provide authentication
  - user exec mode without authentication
  - user exec mode with only password
- We should set up user/password authentication
- Defining user

  Router(config)#username tsuchy password 7 xxxxxxxx

  Router(config)#username iljoon password 7 yyyyyyyy
- Set up authentication

  Router(config-line)#login local

Connecting the new router

1. Switch on
2. Set the router hostname
3. Set the password
4. Disable unnecessary services
5. Set banner
6. Configure access lists
7. Connect the router into the network
8. Configure interface
9. Configure routing protocol
10. Configure time server and logging

Non-technical side of network management

Important point of network operation

- Good organization
- Attention to detail
- Good record keeping
- Good problem solving skills
- Good team abilities
- Good communication skills

Establishing trouble ticket system

- It is easy to share the information
  - Easy to use, usually web based application
  - You can keep the record as long as possible
  - On-line base
    - Search / paperless
  - Check the statistics of trouble
  - Cross-referencing
    - One problem can be referred by several tickets
  - Everyone can check what is happening on network
  - Other operator can take care other’s issue

What should be in the TB?

- Important information is…
  - Time-in, Time-out
  - Taken-by
  - Called-by, Contact
  - Problem description
  - Current status
  - Updates
  - Resolution