APRICOT 2010

Kuala Lumpur, Malaysia

Cisco Configuration Elements

Overview

- Basic things that we need to make sure are configured on a Cisco router (and switch) to do proper network management
- These apply to other network equipment manufacturers of course, and to servers and workstations

Elements

Hostname:	Hostname of the device
SSH:	Enable **S**ecure **SH**ell
DNS:	**D**omain **N**ame **L**ookup
NTP:	Time synchronization (**N**etwork **T**ime **P**rotocol)
Syslog:	**Sys**tem **log** messages
SNMP:	SNMP configuration
SNMP traps:	Where to send traps
CDP:	**C**isco **D**iscovery **P**rotocol

Access the router

1. ssh user@router
2. You are in “user mode”

   ```
   rtr>
   ```

3. If you’re user has the privileges, go to “privileged mode”

   ```
   rtr>enable     (might need pw)
   rtr#conf t
   rtr(config)#
   ```

4. Type in configuration commands.
5. Exit and save/build your new configuration

   ```
   rtr(config)#exit
   rtr#wr mem
   ```

Hostname

- Preferably we use the FQDN (**F**ully **Q**ualified **D**omain **N**ame).
- In config mode on the router

```
rtr(config)#hostname net-gw.XYZ.domain.name
```

or

```
rtr(config)#hostname net-sw-XYZ.domain.name
```

DNS configuration

In config mode on the router:

```
ip domain-name .mgmt.conference.apricot.net
ip name-server 169.223.142.3
```

NTP + time configuration

In config mode:

```
ntp server pool.ntp.org
clock timezone EEST 3
```

If needed:

```
clock summer-time XXX recurring \
last Sun Mar 2:00 last Sun Oct \
3:00
```

Verify:

```
rtr>show clock
```

SSH

Only crypto version of IOS/CatOS have support for SSH – there are export restrictions... In config mode:

```
rtr#aa new-model
rtr#crypto key generate rsa
rtr#username inst secret 0 xxxxxx
```

…above is required to be allowed to enable SSH. Verify creation with:

```
sh crypto key mypubkey  rsa
```

Use at least 768 bits - OpenSSH requires it

SSH continued

Enforce ssh (disabling telnet) on vty lines

```
rtr#conf t
rtr(config)#line vty 0 4
rtr(config)#transport input ssh
rtr(config)#^Z     (“exit” completely)
rtr#wr mem
```

SSH is now enabled

Telnet is not necessary disabled!

- Use ACLs to be sure of this

Syslog

In config mode, enable logging to your NOC machine (X is your network)

```
rtr(config)#logging 192.168.X.1
rtr(config)#logging facility local5
rtr(config)#logging trap debugging
```

SNMP

In config mode:

```
# snmp-server community xxxxxxxxx RW
# snmp-server community public RO
# snmp-server location KL
# snmp-server enable traps config
# snmp-server enable traps envmon
# snmp-server enable traps config-copy
# snmp-server enable traps syslog
# snmp-server host 169.223.142.x public
```

CDP

Cisco Discovery Protocol

- Enabled by default nowadays in current IOS versions.
- Otherwise, enable with ”cdp enable” or ”cdp run” in configure mode on your router.
- tcpdump and tools like cdpr will show you CDP announcements
- check neighbor announcement with:

```
rtr>show cdp neighbors
```

Questions?

?