Advanced Registry Operations Curriculum

Cisco/HP Configuration Elements

Overview

- Basic things that we need to make sure are configured on a Cisco routers, Cisco switches and HP switches 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

Cisco equipment

Accessing the device

1. ssh tldadmin@192.168.10X.1
2. You are in “user mode”

```
rtr>
```

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

```
rtr>enable
rtr#conf t
rtr(config)#
```

(class pw tldadmin!)

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 TLDX-RTR.TLDX
```

DNS configuration

In config mode on the router:

```
ip domain-name tldX
ip name-server 192.168.80.10
```

Replace the “X” in “.tldX” with the number of your network.

NTP + time configuration

In config mode:

```
ntp server 192.168.80.5   (*)
clock timezone XXXX 3
```

If needed:

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

Replace “XXXX” with the timezone abbreviation for the location of your router.

Verify:

```
rtr>show clock
```

(*) Alternate is “pool.ntp.org”

SSH (Note: already enabled here)

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 tldadmin secret 0 \
       tldadmin!
```

…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 192.168.10X.30
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 XX
# snmp-server enable traps config
# snmp-server enable traps envmon
# snmp-server enable traps config-copy
# snmp-server enable traps syslog
# snmp-server host 192.168.10X.1 public
```

- Replace xxxxxxxx with the private community string chosen in class.
- Replace “XX” with an abbreviation for your location.
- Replace “10X” with the number of your network.

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
```

HP switches

Accessing

- Using telnet or ssh (telnet by default)
- By default, no user, only a password:

```
Password: ******
SW1 - HP 2510-G#
```

- Menu mode: not all options available!
- Shell mode: similar to Cisco IOS shell
  - i.e.: spanning-tree not enabled by default, and cannot be enabled via the menu:

```
SW1 - HP 2510-G# conf t
SW1 - HP 2510-G(config)# spanning-tree
```

Hostname

- Like Cisco, but specify FQDN:

```
SW1# conf t
SW1 (config)# hostname sw1.mgmt
SW1 (config)# ^Z
SW1#
```

DNS

- HP layer 2 switches don't support DNS resolution

NTP

```
SW1# conf t
SW1 (config)# sntp server 192.168.80.5
SW1 (config)# sntp server unicast
SW1 (config)# ^Z
SW1#
```

SSH

```
SW1 (config)# crypto key generate ssh
Installing new RSA key.  If the key/
  entropy cache is depleted, this could
  take up to a minute.
SW1 (config)# ip ssh
SW1 (config)# no telnet-server
SW1 (config)# ^Z
SW1# write mem
SW1#
```

- SSH is now enabled – by default the user you log in as is ignored, only the password matters. TELNET IS DISABLED!

Syslog

```
SW1 (config)# logging 192.168.10X.30
SW1 (config)# logging facility local5
SW1 (config)# ^Z
SW1# write mem
```

SNMP

```
SW1 (config)# snmp-server community xxx
SW1 (config)# ^Z
SW1# write mem
```

- By default, community is RO (read only)

CDP and LLDP/802.1ab

- HP eqpt. supports both Cisco's discovery protocol (CDP) as well as the open standard 802.1ab (LLDP – Link Layer Discovery Protocol)
- By default, CDP is enabled

```
SW1 (config)# cdp run
SW1 (config)# cdp enable 1-24
SW1 (config)# ^Z
SW1# write mem
```

Questions?

?