

Cisco configuration elements

APRICOT 2008
Network Management
Taipei, Taiwan
February 20-24, 2008



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 secure shell
- DNS domain name lookup
- NTP time synchronization
- Syslog syslog messages
- SNMP SNMP configuration
- SNMP traps and where to send traps
- CDP Cisco discovery protocol

Hostname

- Use the FQDN preferably.
- In config mode:

```
hostname gw|sw-XYZ[.domain.name]
```

DNS configuration

- Config mode:

```
ip domain-name mgmt.conference.apricot.net
ip name-server 169.223.2.2
```

NTP + time configuration

- In config mode:

```
ntp server pool.ntp.org
clock timezone CWT 8
```

- If needed:

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

- Verify:

```
show clock
```

SSH

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

```
aaa new-model
crypto key generate rsa
username inst secret 0 xxxxxxxxxxx
```

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

```
sh crypto key mypubkey rsa
```

- Use at least 768 bits

SSH (2)

- Enforce ssh (disabling telnet) on vty lines:

```
host# conf t
host(config)# line vty 0 4
host(config-line)# transport input ssh
^Z
host#
```

- SSH is now enabled, and the telnet disabled

Syslog

- In config mode:

```
logging noc.mgmt.conference.apricot.net  
logging facility local5  
logging trap debugging
```

SNMP

- In config mode:

```
snmp-server community xxxxxxxxxx RW
snmp-server community apric0t08 RO
snmp-server location Taipei, room 403
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server host xxx (see cisco doc)
```

CDP

- Cisco Discovery Protocol
- Normally enabled by default nowadays
- Otherwise, enabled with "cdp enable"
- tcpdump and tools like cdpr will show you CDP announcements