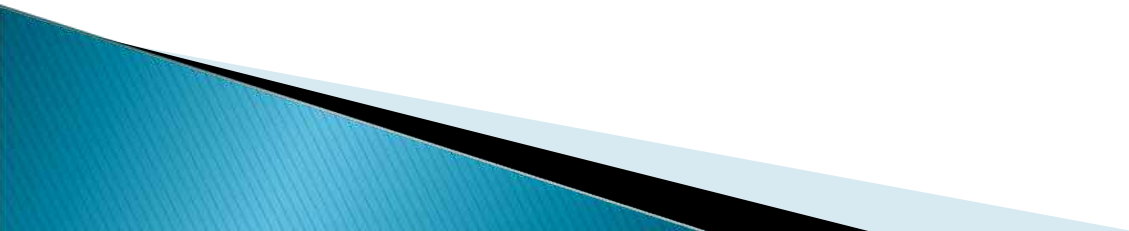
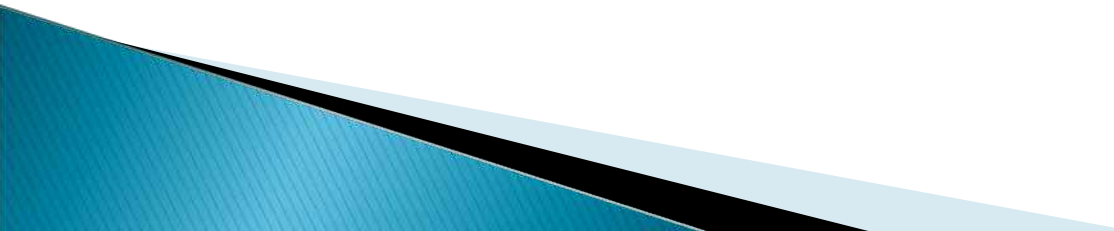


Cisco Device Configuration

(To Facilitate Monitoring)



Topics

- ▣ CLI modes
 - Accessing the configuration
 - Basic configuration (hostname and DNS)
 - Authentication and authorization (AAA)
 - Log collection
 - Time Synchronization (date/timezone)
 - SNMP configuration
 - Cisco Discovery Protocol (CDP)
- 

CLI Modes

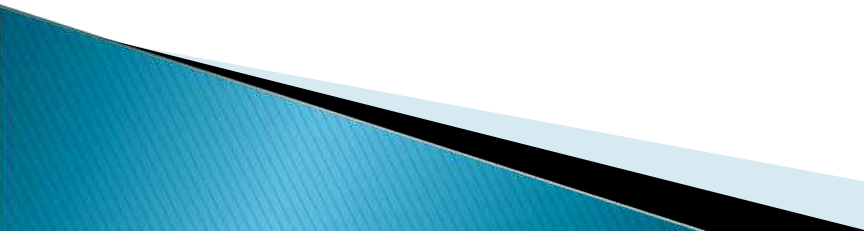
- ▶ User EXEC
 - Limited access to the router
 - Can show some information but cannot view nor change configuration

```
rtr>
```

- ▶ Privileged EXEC
 - Full view of the router's status, troubleshooting, manipulate config, etc.

```
rtr> enable
```

```
rtr#
```



Accessing the configuration

- ▶ There are two configurations:
 - *Running config* is the actual configuration that is active on the router
 - Stored in RAM (will be gone if router is rebooted)
 - ```
rtr# configure terminal
rtr(config)#end
rtr# show running-config
```
  - *Startup config*
    - Stored in NVRAM (Non-Volatile RAM)
  - ```
rtr# copy running-config startup-config
rtr# show startup-config
```

Basic configuration (hostname and DNS)

- Assign a name

- `rtr(config)# hostname pcx-pcl-rtr`

- Assign a domain

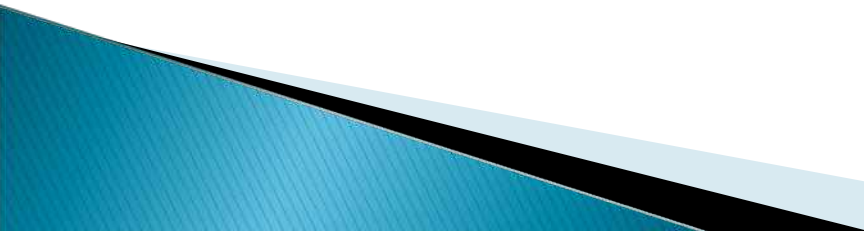
- `rtr(config)# ip domain-name ws.nsrc.org`

- Assign a DNS server

- `rtr(config)# ip name-server 8.8.8.8`

Or else disable DNS entirely (your choice):

`rtr(config)# no ip domain-lookup`



Authentication and authorization

- ▶ Configure passwords in the most secure manner.

- Use the improved method which uses hash function

□ Example:

```
#enable secret wer56$21
```

```
#user admin secret sdf!231
```

Authentication and authorization

- ▶ Use SSH, disable *telnet* (only use telnet if no other option)

```
#line vty 0 4
  transport input ssh
```

- ▶ Configuring with a 2048 byte key:

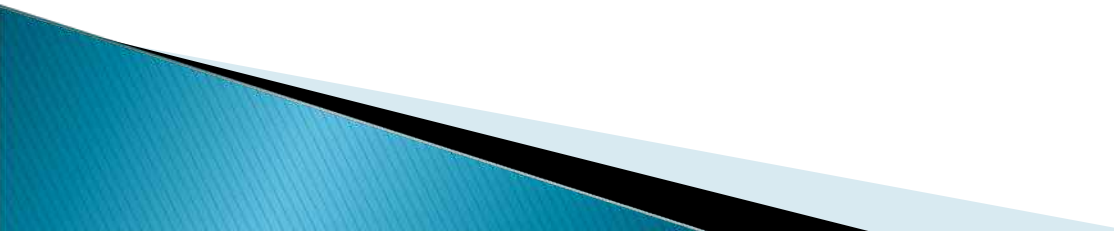
```
#aaa new-model
#crypto key generate rsa modulus 2048
```

- ▶ Verify key creation:

```
#show crypto key mypubkey rsa
```

- ▶ Restrict to only use SSH version 2. Optionally register events:

```
#ip ssh logging events
#ip ssh version 2
```



Log collection (syslog)

- ▶ Send logs to the *syslog* server:

```
#logging 10.0.0.5
```

- ▶ Identify what channel will be used (local0 to local7):

```
#logging facility local5
```

- ▶ Up to what priority level do you wish to record?

```
#logging trap <logging_level>
```

<0-7>			Logging severity level
alerts	Immediate action needed	(severity=1)	
critical	Critical conditions	(severity=2)	
debugging	Debugging messages	(severity=7)	
emergencies	System is unusable	(severity=0)	
errors	Error conditions	(severity=3)	
informational	Informational messages	(severity=6)	
notifications	Normal but significant conditions	(severity=5)	
warnings	Warning conditions	(severity=4)	

Time synchronization

It is essential that all devices in our network are time-synchronized

In config mode:

```
# ntp server pool.ntp.org  
# clock timezone <timezone>
```

If your site observes daylight savings time you can do:

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

Verify

```
# show clock
```

```
11:20:44.470 CMT Tue Aug 3 2010
```

```
# show ntp status
```

```
Clock is synchronized, stratum 3, reference is 4.79.132.217  
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**18  
reference time is D002CE85.D35E87B9 (11:21:09.825 CMT Tue Aug 3 2010)  
clock offset is 2.5939 msec, root delay is 109.73 msec  
root dispersion is 39.40 msec, peer dispersion is 2.20 msec
```

SNMP Configuration

- ▶ Start with SNMP version 2
 - It's easier to configure and understand
 - Example:

```
rtr(config)#snmp-server community NetManage ro 99  
r10(config)#access-list 99 permit 10.10.0.0 0.0.0.255  
r10(config)#access-list 99 permit 10.10.254.0 0.0.0.255
```

SNMP Configuration

- ▶ Later on, we recommend utilizing SNMP version 3:
 - Has access protection and encryption

- ▶ **Configuring SNMP v3:**

```
snmp-server view <view> <MIB family> included
snmp-server group <group> v3 auth read <view>
snmp-server user <user> <group> v3 auth <hash> <password> [ priv des56 <key> ]
```

- **Example:**

Configure a user with complete access to the SNMP tree, read only.

Password is hashed via MD5 (Auth) and without encrypting the SNMP response:

```
snmp-server view ro-view internet included
snmp-server group ro-group v3 auth read ro-view
snmp-server user admin ro-group v3 auth md5 nsrsc
```

Checking SNMP configuration

- ▶ From a Linux machine, try:

```
snmpwalk -v2c -c NetManage gw sysDescr
```

```
snmpwalk -v3 -a MD5 -A nsrc -l authNoPriv -u admin gw sysDescr
```

Configuring Cisco Discovery Protocol (CDP)

- Enabled by default in most modern routers
- If it's not enabled:
 - `cdp enable`
 - `cdp run` in older CISCO IOS versions
- To see existing neighbors:
 - `show cdp neighbors`
- Tools to visualize/view CDP announcements:
 - `tcpdump`
 - `cdpr`
 - Wireshark