

# Configuration des périphériques Cisco

(Pour faciliter la supervision)

Gestion et surveillance de Réseau



# Thèmes

- Modes CLI
- Accès à la configuration
- Configuration de base (nom d'hôte et DNS)
- Authentification et autorisation (AAA)
- Collecte des journaux
- Synchronisation temporelle (Date / fuseau horaire)
- Configuration SNMP
- Protocole CDP (Cisco Discovery Protocol)

# Modes CLI

- ▶ Mode utilisateur EXEC
  - Accès limité au routeur
  - Peut afficher des informations mais ne peut pas visualiser ni modifier la configuration
- ▶ Mode privilégié EXEC
  - Visualisation totale de l'état du routeur, dépannage, modification de la configuration, etc.

```
rtr>
```

```
rtr> enable
```

```
rtr#
```

# Accès au routeur

- ▶ Avant la mise en place de SSH
  - telnet 10.10.0.x
  - login “cisco” et “cisco” (utilisateur et mot de passe)
- ▶ L'utilisateur privilégié peut passer en mode privilégié :
  - `rtr>enable` (mot de passe par défaut : “cisco”)
  - `rtr#configure terminal`
  - `rtr(config)#`
- ▶ Saisissez des commandes de configuration
- ▶ Quittez et enregistrez la nouvelle configuration
  - `rtr(config)#exit`
  - `rtr#write memory`

# Accès à la configuration

- ▶ Il y a deux configurations :
  - *Running config* est la configuration active sur le routeur
    - Stockée dans la RAM (sera perdue en cas de redémarrage du routeur)

```
rtr# configure terminal (conf t)
```

```
rtr(config)#end
```

```
rtr# show running-config
```

- *Startup config (config de démarrage)*

- Stockée dans la NVRAM (RAM non volatile)

```
rtr# copy running-config startup-config (ou)
```

```
rtr# write memory (wr mem)
```

```
rtr# show startup-config (sh start)
```

# Configuration de base (nom d'hôte et DNS)

## ■ Attribuez un nom

- `rtr(config)# hostname rtrX`

## ■ Attribuez un domaine

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

## ■ Attribuez un serveur DNS

- `rtr(config)# ip name-server 10.10.0.254`

## ■ Ou, désactivez la résolution DNS

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

L'absence de dns est *très utile* pour éviter les attentes prolongées

# Authentification et autorisation

- ▶ Configurez les mots de passe de la manière la plus sûre.

- Utilisez la méthode améliorée faisant appel à la fonction de hachage

- Exemple :

```
#enable secret 0 wer56$21
```

```
#user admin secret 0 sdf!231
```

# Authentification et autorisation

- ▶ Utilisez SSH, désactivez *telnet* (utiliser telnet uniquement en l'absence d'autre possibilité)

```
rtr(config)#line vty 0 4  
rtr(config)#transport input ssh
```

- ▶ Configuration avec une clé de 2048 bits :

```
rtr(config)#aaa new-model  
rtr(config)#crypto key generate rsa
```

(la taille de la clé vous sera demandée)

- ▶ Vérifiez la création de la clé :

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

- ▶ Limitez l'utilisation uniquement à SSH version 2. Éventuellement enregistrez les événements :

```
rtr(config)#ip ssh logging events  
rtr(config)#ip ssh version 2
```

# Collecte des journaux (syslog)

- ▶ Envoyez les journaux au serveur *syslog* :  
`#logging 10.10.x.x`
- ▶ Identifiez le canal qui sera utilisé (local0 à local7):  
`#logging facility local5`
- ▶ Jusqu'à quel niveau de priorité souhaitez-vous enregistrer ?  
`#logging trap <logging_level>`

| <0-7> Niveau de gravité des messages de journalisation |                                      |             |
|--------------------------------------------------------|--------------------------------------|-------------|
| Urgences                                               | Système indisponible                 | (gravité=0) |
| Alertes                                                | Action immédiate requise             | (gravité=1) |
| critique                                               | Conditions critiques                 | (gravité=2) |
| erreurs                                                | Conditions d'erreur                  | (gravité=3) |
| avertissements                                         | Conditions d'avertissement           | (gravité=4) |
| notifications                                          | Conditions normales mais importantes | (gravité=5) |
| informatifs                                            | Messages informatifs                 | (gravité=6) |
| débogage                                               | Messages de débogage                 | (gravité=7) |

# Synchronisation

**Il est essentiel que tous les périphériques de notre réseau soient synchronisés**

**En mode config :**

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

**Pour utiliser l'heure UTC**

```
# no clock timezone
```

**Si votre site applique l'heure d'été, vous pouvez procéder comme indiqué ci-dessous :**

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

**Vérifiez**

```
# show clock
```

```
22:30:27.598 UTC Tue Feb 15 2011
```

```
# 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
```

# Configuration SNMP

- ▶ Démarrez avec SNMP version 2
  - C'est plus facile à configurer et à comprendre
  - Exemple :

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

# Contrôle de la configuration SNMP

- ▶ Avec une machine Linux (après installation des utilitaires snmp), essayez :

```
snmpwalk -v2c -c public 10.10.0.X sysDescr
```

# Configuration du protocole CDP (Cisco Discovery Protocol )

- Activé par défaut sur la plupart des routeurs modernes
- S'il n'est pas activé :
  - `cdp enable`
  - `cdp run` dans les versions plus anciennes de l'IOS de CISCO
- Pour voir les voisins existants :
  - `show cdp neighbors`
- Outils permettant de visualiser/afficher les annonces CDP :
  - `tcpdump`
  - `cdpr`
  - Wireshark

# Commutateurs HP

# Accès

- ▶ Utilisation de telnet ou ssh (telnet par défaut)
- ▶ Par défaut, pas d'utilisateur, seulement un mot de passe :
- ▶ Mot de passe : \*\*\*\*\*
- ▶ SW1#
- ▶ Mode menus : toutes les options ne sont pas disponibles !
- ▶ Mode shell : similaire au shell de l'IOS de Cisco
- ▶ c.-à-d., le Spanning Tree n'est pas activé par défaut, et ne peut être activé via le menu :
  - SW1# conf t
  - SW1(config)# spanning-tree

# Nom d'hôte

- ▶ Comme Cisco, mais spécifiez le nom de domaine complet (FQDN) :
  - SW1# conf t
  - SW1 (config)# hostname sw1.ws.nsrc.org
  - SW1 (config)# ^Z
  - SW1#

# DNS

- ▶ Les commutateurs HP de couche 2 ne prennent pas en charge la résolution DNS

# NTP

- SW1# conf t
- SW1 (config)# sntp server 10.10.0.254
- SW1 (config)# sntp server unicast
- SW1 (config)# ^Z
- SW1#

- SW1 (config)# crypto key generate ssh  
*Installation d'une nouvelle clé RSA. Si le cache de clé / entropie est épuisé, ceci peut prendre jusqu'à une minute.*
- SW1 (config)# ip ssh
- SW1 (config)# no telnet-server
- SW1 (config)# ^Z
- SW1# write mem
- SW1#
- ▶ SSH est maintenant activé – par défaut l'utilisateur utilisé pour se connecter est ignoré, seul le mot de passe importe. TELNET EST DÉSACTIVÉ !

# Syslog

- SW1 (config)# logging 10.10.x.x
- SW1 (config)# logging facility local5
- SW1 (config)# ^Z
- SW1# write mem

# snmp

- SW1 (config)# snmp-server community public
  - SW1 (config)# ^Z
  - SW1# write mem
- ▶ Par défaut, la communauté est en lecture seule (RO)

# CDP et LLDP/802.1ab

- ▶ Les équipements HP prennent en charge le protocole CDP (Cisco Discovery Protocol) ainsi que le standard ouvert 802.1ab (LLDP – Link Layer Discovery Protocol)
- ▶ Par défaut, CDP est activé
  - SW1 (config)# cdp run
  - SW1 (config)# cdp enable 1-24
  - SW1 (config)# ^Z
  - SW1# write mem

# Questions

?