



# Programme Opérations de registre avancées

## Eléments de configuration Cisco



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

# Présentation générale

- Les éléments de base pour une gestion correcte du réseau sont configurés sur un routeur (et commutateur) Cisco
- Ceci concerne naturellement les équipements réseau d'autres constructeurs ainsi que les serveurs et stations de travail.

# Éléments

- Hostname :** nom d'hôte de l'installation
- SSH :** activation de **Secure SHell**
- DNS :** consultations de noms de domaine  
(**Domain Name Server**)
- NTP :** protocole d'heure réseau  
(**Network Time Protocol**)
- Syslog :** messages **System log**
- SNMP :** configuration SNMP
- Déroutements SNMP :** où envoyer les déROUTements
- CDP:** protocole de découverte de réseau  
(**Cisco Discovery Protocol**)

# Accès au routeur

1. `ssh user@router`

2. Vous êtes en “mode utilisateur”

```
rtr>
```

3. Si votre utilisateur bénéficie de privilèges, passez en “mode privilégié” :

```
rtr>enable      (un mot de passe peut être nécessaire)
```

```
rtr#conf t
```

```
rtr(config)#
```

4. Saisissez les commandes de configuration.

5. Quittez en enregistrant /construisant votre nouvelle configuration

```
rtr(config)#exit
```

```
rtr#wr mem
```

# Nom d'hôte

- Nous utilisons de préférence le nom de domaine FQDN complet (**Fully Qualified Domain Name**).
- En mode config sur le routeur

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

**OU**

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

# Configuration DNS

En mode config sur le routeur :

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

remplacez le “X” de “.tldX” par votre numéro de réseau.

# NTP + configuration d'heure réseau

## En mode config :

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

## Si nécessaire :

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

Remplacez "XXXX" par l'abréviation de la zone horaire du routeur.

## Vérifiez :

```
rtr>show clock
```

# SSH

Seule la version crypto de l'IOS/CatOS dispose du support SSH – il existe des restrictions d'exportation... En mode config :

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

...est nécessaire pour pouvoir activer le SSH.

Vérifiez la création avec :

```
sh crypto key mypubkey rsa
```

Utilisez au moins 768 bits, requis par OpenSSH.

# SSH (suite)

**Activez ssh (en désactivant telnet) sur les lignes vty**

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

**SSH est maintenant activé**

Telnet n'est pas nécessairement désactivé !

- Utilisez des ACL pour le vérifier

# Syslog

**En mode config, activez logging sur votre machine NOC (X désigne votre réseau)**

```
rtr(config)#logging 192.168.75.20  
rtr(config)#logging facility local5  
rtr(config)#logging trap debugging
```

# SNMP

## En mode config :

```
# snmp-server community xxxxxxxxxx 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
```

- Remplacez xxxxxxxx par la chaîne communautaire privée choisie pour l'atelier.
- Remplacez "XX" par une abréviation désignant votre site.
- Remplacez "10X" par votre numéro de réseau.

# CDP

## Protocole de découverte de Cisco

- Activé par défaut dans les versions IOS actuelles.
- Si tel n'est pas le cas, activez-le sur votre routeur avec "cdp enable" ou "cdp run" en mode configuration.
- tcpdump et des outils tels que cdpr montrent les annonces CDP
- Vérifiez les annonces des équipements voisins avec :

```
rtr>show cdp neighbors
```

# Des questions ?

