# Sicurezza sui Cisco: Password e Privileged Levels

Per aumentare il livello di sicurezza del nostro router (switch) è possibile ovviamente fare uso di password ma anche dei così detti *Privileged Levels*.

## Le password

Per quanto riguarda le password ne esistono di due tipi: la **Enable Password** e le **Line Password**. La Enable Password è la password necessaria per passare allo stato di Privileged Mode mentre le Line Password proteggono da accessi esterni quali porta console, porta auxiliary e dal servizio telnet.

### La Enable Password

Possiamo impostare la Enable Password in due modi: uno sicuro e uno no. Ma è giusto affrontarli entrambi:

```
router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#enable password prova

router(config)#
```

Questo è il metodo insicuro poichè la password sarà ben visibile nella configurazione del router. Infatti:

```
router#sh run

..

..

enable password prova

!

..

..
```

Per ovviare a questo, abbiamo la possibilità di inserire la password e far sì che venga crittografata tramite il comando enable secret:

```
router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#enable secret prova2

router(config)#
```

Ecco che la password nella configurazione non sarà più visibile in chiaro ma bensì esclusivamente crittografata:

```
router#sh run

..

..

!

enable secret 5 $1$AWfn$JnM/50S9kiJoDEcUuFd4/.

..

..
```

## Le Line Password

Le Line Password, come detto precedentemente, proteggono il router dagli accessi esterni quali porta console, porta auxiliary (aux) e telnet. Guardiamo sul router quali interfacce possiamo configurare con il comando `line ?`:

```
router(config)#line ?

 <0-70>  First Line number

 aux  Auxiliary line

 console  Primary terminal line

 tty  Terminal controller

 vty  Virtual terminal
```

```
 x/y  Slot/Port for Modems

router(config)#
```

Possiamo anche guardare quante interfacce abbiamo di un certo tipo. Esempio:

```
router(config)#line tty ?

  <1-64> First Line number

router(config)#
```

oppure, altro esempio:

```
router(config)#line aux ?

  <0-0> First Line number

router(config)#
```

Attenzione: in questo caso con <0-0> non significa che non abbiamo nessuna porta Aux. 0-0 è solamente il range dal quale deduciamo che abbiamo una porta Aux. Anche perchè, altrimenti, non ci sarebbe risultato `aux Auxiliary line` con il comando `line ?`.

Il procedimento per assegnare una password a questi tre differenti tipi di porte (o meglio di accesso) è lo stesso:

```
router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#line aux ?

  <0-0> First Line number

router(config)#line aux 0

router(config-line)#login

% Login disabled on line 65, until 'password' is set

router(config-line)#password prova3

router(config-line)#end

router#
```

E così via per le altre:

```
router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#line con ?

<0-0> First Line number

router(config)#line con 0

router(config-line)#login

router(config-line)#password prova4

router(config-line)#end

router#
```

Per la porta console, mentre per la tty:

```
router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

router(config)#line vty ?

  <0-181> First Line number

router(config)#line vty 1

router(config-line)#password prova5

router(config-line)#end

router#
```

Tutte queste password saranno visibili con un `sh run`:

```
router#sh run

..

..

!

line con 0
```

```
 password prova4
 login
line aux 0
 password prova3
 login
line vty 0
 password cisco
 login
line vty 1
 password prova5
 login
line vty 2 4
 password cisco
 login
!
!
end
```

A questo punto ci si chiede: ok, per la Enable Password ho a disposizione enable secret per crittografare la password. E per le Line Password? In realtà non c'è un servizio dedicato per quest'ultima ma un servizio che crittografa tutte le password del router: password-encryption! Attiviamolo:

```
router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#service password-encryption
router(config)#end
```

```
router#
```

Bene, abbiamo attivato il servizio. Ricontrolliamo lo sh run e vedremo che service password-encryption è attivo e che naturalmente le password inserite in precedenza saranno tutte crittografate:

```
router#sh run

..

..

service password-encryption

!

..

..

!

line con 0

 password 7 15021903122B7F

 login

line aux 0

 password 7 03144904100E72

 login

line vty 0

 password 7 121A0C041104

 login

line vty 1

 password 7 140700041A057F

 login
```

```
line vty 2 4
 password 7 045802150C2E
 login
!
!
end
```

## I privilege Level

I privilege Level sono appunto vari livelli, per la precisione sedici (da 0 a 15), che consentono l'esecuzione o meno di determinati comandi. Di default i livelli usati nei router Cisco sono tre:

- Livello 0: usato molto raramente. Permette di usare i comandi enable, disable, exit, help, e logout.
- Livello 1: modalità non privilegiata, ovvero EXEC Mode. E' il livello di defaul al login; il prompt è *router*>.
- Livello 15: modalità privilegiata (Privileged EXEC Mode). E' il livello che ci si ritrova dopo aver inserito la password di enable. Il prompt è *router#*.

Oltre a questi tre livelli di default, abbiamo la possibilità di usare tutti gli altri (dal 2 al 14) specificando quali comandi rendere disponibili per ogni preciso livello! Per prima cosa, bisogna assegnare una password al livello che si intende abilitare:

```
router(config)#enable password level 10 prova

% Converting to a secret. Please use "enable secret" in the
future.

router(config)#
```

(Da notare la possibilità di criptare anche questo tipo di password con enable secret). Dopo di che specifichiamo i comandi che intendiamo rendere disponibili:

```
router(config)#privilege exec level 10 comando_1

router(config)#privilege exec level 10 comando_2

router(config)#privilege exec level 10 comando_3
```

```
(ecc ecc)
```
Salviamo poi la configurazione:

```
router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

router#
```
Bene, per usare quel livello, usiamo il comando enable numero_livello. Così:

```
router>enable 10

Password:

router#
```
Possiamo verificare che stiamo usando questo livello con show privilege:

```
router#show privilege

Current privilege level is 10

router#
```
Facciamo un esempio pratico: dobbiamo abilitare il debug di cdp ip. Per far notare la differenza e l'effettivo cambiamento:

```
router#debug ?

..

..

  cca           CCA activity

  cdapi           CDAPI information

  cdp           CDP information

  chat           Chat scripts activity

  cls           CLS Information
```

```
..

..

router#debug cdp ?

  adjacency   CDP neighbor info

  events    CDP events

  ip     CDP ip info

  packets    CDP packet-related information

router#
```

Bene, questi sono i comandi disponibili. Impostiamo ora un Privilege Level rendendo disponibile solo il debug cdp ip:

```
router(config)#enable password level 3 password

% Converting to a secret. Please use "enable secret" in the
future.

router(config)#

router(config)#privilege exec level 3 debug cdp ip
```

Bene, logghiamoci ora in questo Privilege Level e verifichiamo di aver a disposizione solo il comando debug cdp ip:

```
router#debug ?

  cdp   CDP information

  conn   Connection Manager information

router#debug cdp ?

  ip  CDP ip info

router#
```

Bene. Ricordo che si può uscire da un livello con il comando *disable numero_livello*.