# Comandi per configurare un dispositivo Cisco

Entrare in modalità exec  privilegiato :

R1 > **enable**

R1#

Entrare in modalità di configurazione globale:

R1 # **config terminal**

R1(config) #

Assegnare  un nome all' host :

R1(config) # **hostname** <inserire il nome desiderato>

Configurare  password di enable ( exec privilegiato) :

R1(config)#**enable password** <password desiderata>

R1(config)#**enable secret**  <password desiderata>

R1(config)#**exit**

Configurare una password di console e sulle linee vty:

R1(config)#**line console 0  oppure  line vty 0 4**

R1(config-line)#**password**  <password desiderata>

R1(config-line)#**login**

R1(config-line)#**exit**

R1(config)#

**NB  per ottenere le password crittate :**
**service password-encryption**

Per ottenere le password in chiaro :

R1(config)#service password

Far apparire un messaggio del giorno :

R1(config)#**banner motd  #**<inserisci testo>**#**

Configurare il R1 per non tentare di risolvere i nomi host utilizzando un server DNS :

R1(config)#**no ip domain lookup**

Configurare in modo che i messaggi della console non interferiscano con l'input di comando :

R1(config)#line console 0
R1(config-line)#logging synchronous

Vedere la configurazione di running :

R1#**show running-config**

Configurare l'interfaccia seriale sul R1 :

R1(config)#**interface serial 0/0/0**
R1(config-if)#**description WAN link to R2**
R1(config-if)#**ip address** <indirizzo ip> <maschera di rete>
R1(config-if)#**clock rate 64000**
R1(config-if)#**no shutdown**
R1(config-if)#**exit**

Vedere le informazioni relative all'interfaccia seriale :

R1#**show interfaces serial 0/0/0**

Configurare l'interfaccia ethernet 0/0 :

R1(config)#**interface FastEthernet 0/0**
R1(config-if)#i**p address** <indirizzo ip> <maschera di rete>
R1(config-if)#**no shutdown**
R1(config-if)#**exit**
R1(config)#**exit**

Vedere le informazioni relative all'interfaccia ethernet :

R1#**show interfaces FastEthernet 0/0**

Salvare la configurazione :

R1#**copy running-config startup-config**
R1#**copy startup-config running-config**

Controllare la running-config e la startup-config :

R1#**show running-config**
R1#**show startup-config**

Creare degli utenti forniti di password :

R1(config)#**username**<nome>**password/secret**<inserisci password>

Comando per l'instradamento in modo statico del R1:

R1(config)#**ip route** <rete da instradare> <maschera di rete> <nome dell'interfaccia>

Cancellare la configurazione di startup/running:

R1#**erase startup-config / running-config**

## Configurare un server DHCP:

1) Escludere gli indirizzi prima di configurare un DHCP

R1(config)#**ip dhcp excluded-address** < indirizzi da escludere>

2) Nome al pool di indirizzi:

R1(config)#**ip dhcp pool** <nome del pool di indirizzi>

3) Specificare la rete alla quale appartengono gli indirizzi:

R1(dhcp-config)#**network** <indirizzo di rete> <maschera di rete>

4) Specificare il nome di dominio:

R1(dhcp-config)#**domain-name** <nome di dominio desiderato>

5) Specificare l'indirizzo di IP del server DNS:

R1(dhcp-config)#**dns-server** <indirizzo DNS> <indirizzo DNS>

6) Indicare il Default Gateway:

R1(dhcp-config)#**default-gateway** <indirizzo di gateway>

7) Indicare il tempo di "affitto" degli indirizzi:

R1(dhcp-config)#**lease** {giorni [ore] [minuti] | infinito}
R1(dhcp-config)#**end**

Mostra le macchine direttamente connesse al R1 CDP (CiscoDescoveryProtocol):

R1#**show cdp neighbors**

Mostra le macchine direttamente connesse al R1 CDP in dettaglio (CiscoDescoveryProtocol):

R1#**show cdp neighbors details**

Disabilitare/abilitare il CDP :

R1#**no cdp run** / **cdp run**

Disabilitare/Abilitare il CDP su una sola interfaccia:

R1(config)#**interface** <nome della porta con relativa posizione>
S1(config-if)#**no cdp enable** / **cdp enable**

Configurare più porte con gli stessi parametri:

R1(config)#**interface range** fa0/1 - 18 ( blank prima e dopo il - )

Configurare la vlan di gestione:

S1(config)# **interface vlan 1**
S1(config)# description "lan management"
S1(config-if)#**ip address** <indirizzio di ip> <maschera di rete>
S1(config-if)#**no shutdown**
S1(config-if)#**exit**
S1(config)#**ip default-gateway** <default gateway>

METODI PER RENDERE SICURA UNA PORTA DI UNO SWITCH

La sicurezza delle porte è disabilitata di default, per abilitarla é necessaria l'istruzione switchport port-security che senza nessuna ulteriore specifica configura il port security dinamico. I metodi sono tre:

**Port security dinamico**:gli indirizzi MAC vengono appresi dinamicamente al passaggio dei frame dalla porta e memorizzati solo nella MAC table quindi gli indirizzi si perdono allo spegnimento o riavvio dello switch.

S1(config)# **interface** fa0/1
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport port-security**
S1(config-if)# **switchport port-security maximum** 3 ( opzionale )
S1(config-if)# **switchport port-security violation {protect | restrict | shutdown}** ( opzionale )
S1(config-if)# **exit**

**Port security statico**: l'amministratore specificata i mac ammessi nella running-config. I mac address vengono inseriti nella mac-table e di conseguenza se lo switch viene riavviato vanno persi a meno di un salvataggio della running-config.

S1(config)# **interface** fa0/2
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport port-security**
S1(config-if)# **switchport port-security mac-address** hhhh.hhhh.hhhh
S1(config-if)# **switchport port-security maximum** 3 ( opzionale )
S1(config-if)# **switchport port-security violation {protect | restrict | shutdown}** ( opzionale )
S1(config-if)# **exit**

**Port security sticky** : gli indirizzi vengono appresi dinamicamente e vanno sia in MAC table che in running config. Questo metodo ha i vantaggi della port security dinamica, ( apprende al passaggio dei frame il mac-address ) al fatto che vengono registrati anche in running config.

S1(config)# **interface** fa0/1
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport port-security**
S1(config-if)# **switchport port-security mac-address sticky**
S1(config-if)# **switchport port-security maximum** 6 ( opzionale )
S1(config-if)# **switchport port-security violation {protect | restrict | shutdown}** ( opzionale )
S1(config-if)# **exit**

*maximum 6* vuol dire che saranno permessi i primi 6 mac address che attraversano la porta . Se vengono configurati meno indirizzi i restanti sono switchport port-security di default.

Conseguenze relative alla violazione di una porta

Una violazione della sicurezza si verifica in una di queste situazioni:

- Quando viene raggiunto il numero massimo di indirizzi MAC sicuri su una porta protetta e il mac address del mittente del traffico in ingresso è diverso da uno degli indirizzi MAC sicuri identificati.

- Se il traffico con un indirizzo MAC sicuro configurato o appreso su una porta sicura tenta di accedere ad un'altra porta sicura nella stessa VLAN.

Attraverso il comando **switchport port-security violation** l'amministratore può configurare tre modi diversi di comportamento rispetto alle volazioni :

**Protect**: Elimina i pacchetti con indirizzi mac mittenti sconosciuti finché non si rimuove un numero sufficiente di indirizzi MAC sicuri in modo da scendere al di sotto del valore massimo definito.
**Restrict**: Elimina i pacchetti con indirizzi mac mittenti sconosciuti finché non si rimuove un numero sufficiente di indirizzi MAC sicuri in modo da scendere al di sotto del valore massimo definito.. Viene notificata la violazione della sicurezza aumentando il SecurityViolation counter.
**Shutdown:** In questa modalità (predefinita), una violazione manda in shutdown la porta e il contatore delle violazioni viene incrementato e viene inviato un errore SNMP.

Come cancellare i MAC appresi e memorizzati nella running-config

**reboot**
**no switchport port-security**
**clear port-security sticky interface <id> access**
**shutdown**
**no shutdown**

Verificare la sicurezza della porta:

S1#**show port-security**

| Secure Port | MaxSecureAddr (Count) | CurrentAddr (Count) | SecurityViolation (Count) | Security Action |
|---|---|---|---|---|
| Fa0/1 | 2 | 0 | 1 | Shutdown |
| Fa0/2 | 2 | 2 | 0 | Restrict |
| Fa0/3 | 2 | 1 | 0 | Restrict |

S1# **show port-security address**

Secure Mac Address Table

| Vlan | Mac Address | Type | Ports |
|---|---|---|---|
| 1 | 000B.BE87.8001 | DynamicConfigured | FastEthernet0/1 |
| 1 | 0000.1111.2222 | SecureConfigured | FastEthernet0/2 |
| 1 | 000C.CF2E.D2A2 | DynamicConfigured | FastEthernet0/2 |
| 1 | 70A9.CA91 | SecureSticky | FastEthernet0/3 |

S1# **show port-security interface fastethernet 5/1**

Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity

SecureStatic address aging: Enabled
Security Violation count: 0

Configurazione del tipo di comunicazione e velocità di un'interfaccia

R1(config)#**interface FastEthernet 0/0**
R1(config-if)#**duplex full** | **duplex half** | **duplex auto**
R1(config-if)#**speed 100** | **speed 10** | **speed 1000** | **speed auto**

Configurazione dell ' SSH

S1# **configure terminal**
S1(config) # **ip domain-name** *cisco.com*
S1(config) # **crypto key generate rsa**
S1(config) # **username** *admin* **secret** *password*

S1(config) # **line vty 0 15**
S1(config-line) # **transport input ssh**
S1(config-line) # **login local**
S1(config-line) # **exit**
S1(config) # **ip ssh version 2**
S1(config) # **exit**
S1#

Cancellazione della coppia di chiavi rsa e disabilitazione dell' SSH

S1(config) # **crypto key zeroize rsa**