

CCNA 200-301

SWITCH CLI PROTEGGERE L'ACCESSO

INTRODUZIONE

ACCESSO ALLA CLI

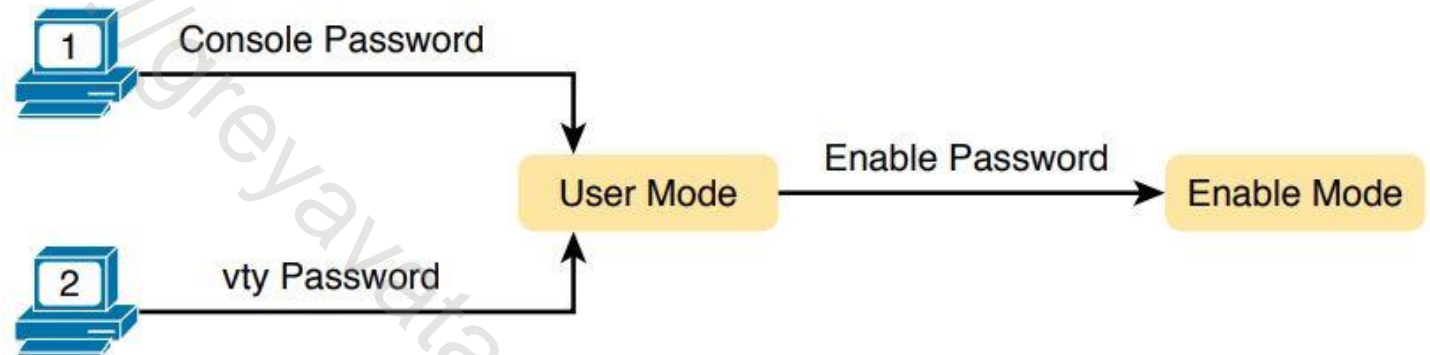
- Per default, l'accesso agli switch Cisco Catalyst è consentito tramite la Console port, prima in USER mode e successivamente in configurazione senza nessun tipo di sicurezza.
- Questo ha senso perché per accedere tramite console port si deve avere un accesso fisico allo strumento.
- Successivamente per facilitare la gestione bisogna implementare un accesso remoto ai dispositivi, a questo livello bisogna quindi proteggere i devices.

COSA FARE PER ACCEDERE IN MODO SICURO ALLO SWITCH

1. Rendere sicuro l'accesso in user mode attraverso la console utilizzando una password.
2. Rendere sicuro l'accesso al privileged mode tramite l'uso di un utente locale
3. Rendere sicuro l'accesso al privileged mode tramite un server di autenticazione
4. Assicurare un accesso remoto tramite ~~telnet~~ **SSH**

SCHEMA DI ACCESSO

- L'accesso al dispositivo può essere effettuato tramite console (porta fisica presente sullo switch)
- Successivamente si può accedere in modo remoto tramite interfacce virtuali chiamate VTY

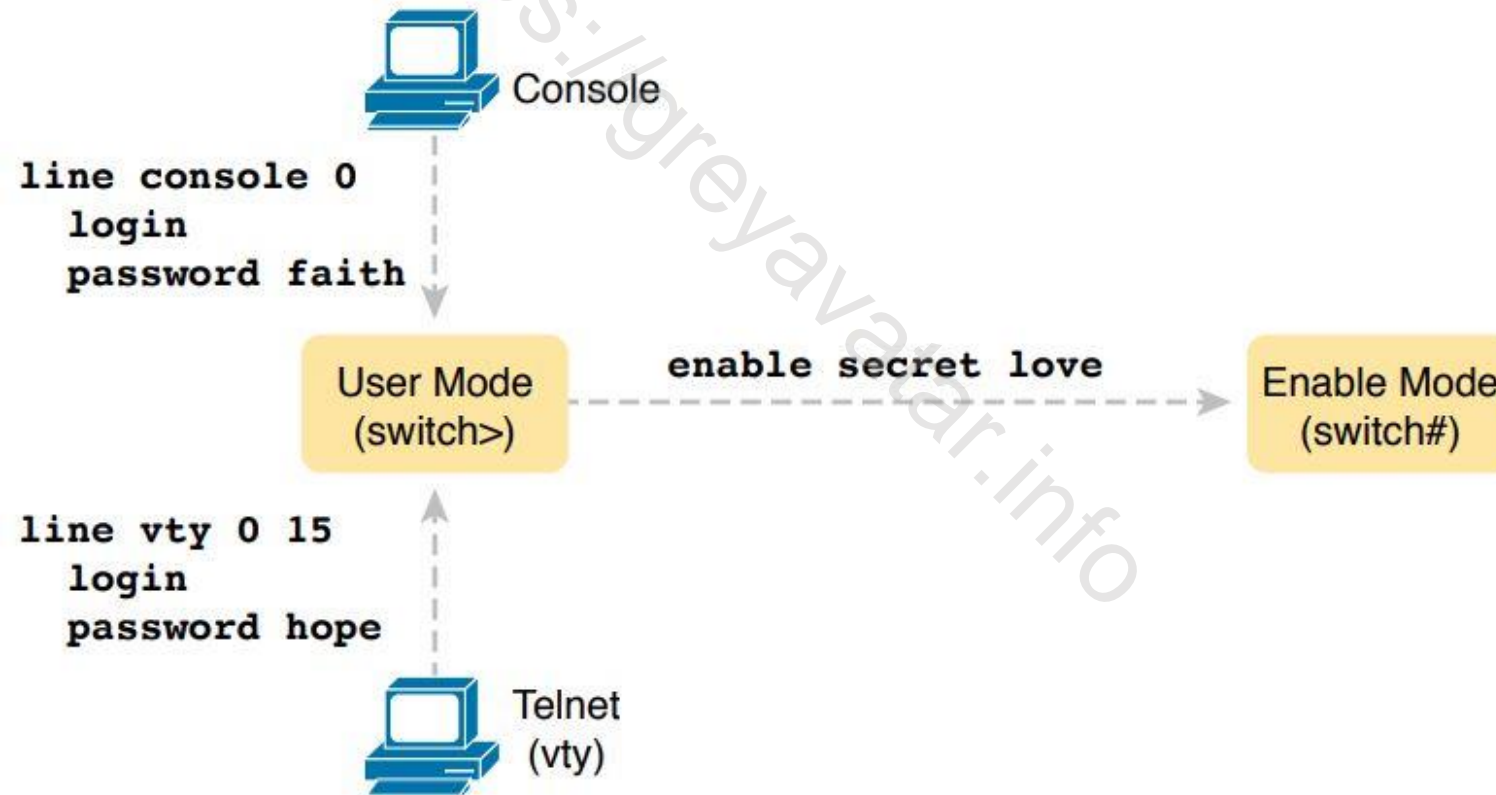


ACCESSO ALLA CONSOLE TRAMITE PASSWORD

- Collegare il pc alla console port dello switch
- Entrare in modalità privilegiata (**enable**)
- Selezionare l'interfaccia console (**line console 0**)
- Inserire una Password (password <**PASSWORD**>)
- Abilitare il login tramite l'uso di password condivisa sull'interfaccia console (**login**)

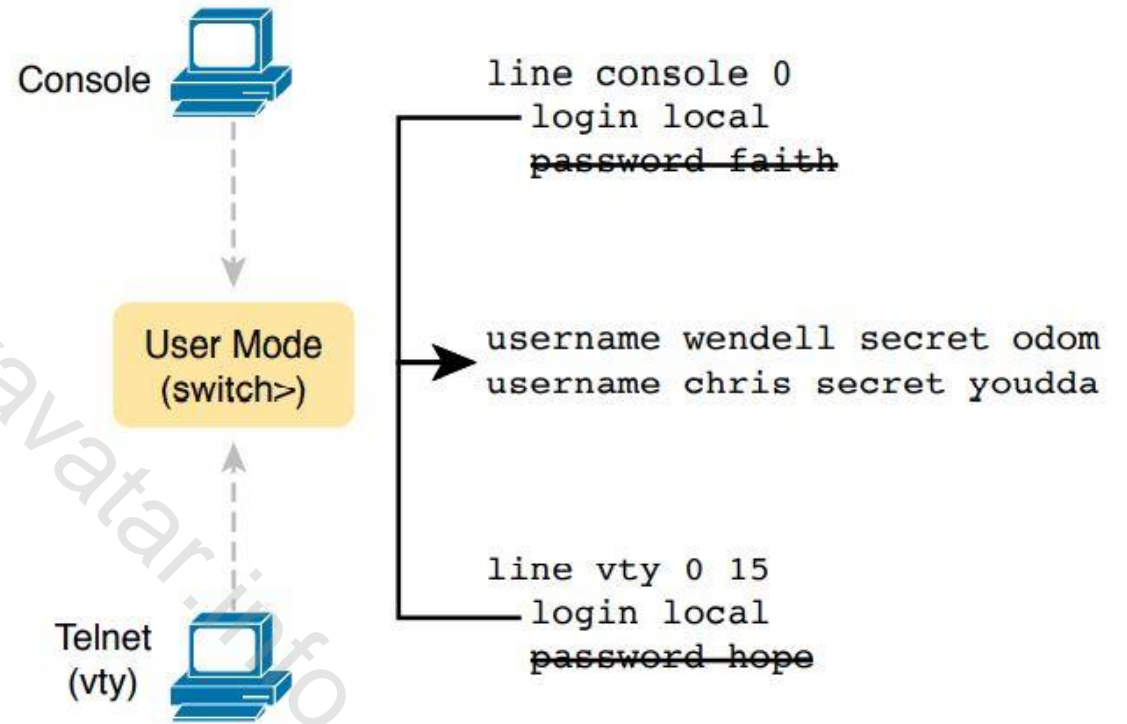
ACCESSO AL PRIVILEGED MODE TRAMITE SECRET

- Partendo dal collegamento tramite console
- Dalla modalità Privileged nella configurazione globale (**enable secret <Secret>**)



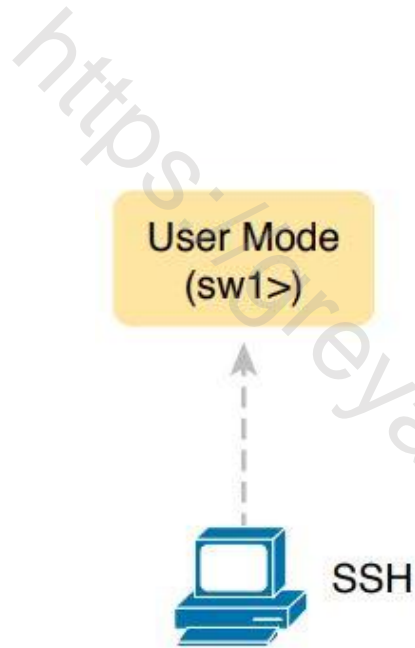
ACCESSO CON UTENTE LOCALE

- Oltre alla password condivisa è possibile garantire l'accesso alla console e vty tramite utenti locali.
- Non è possibile sostituire l'accesso alla modalita ENABLE utilizzando un utente locale.



SSH ACCESSO SICURO

- Per motivi di sicurezza è sconsigliato l'utilizzo di Telnet in quanto il traffico utilizzando tale protocollo è in chiaro e vulnerabile ad attacchi del tipo man in the middle.



```
hostname sw1
ip domain-name example.com
! Next Command Uses FQDN "sw1.example.com"
crypto key generate rsa
```

Local Username Configuration (Like Telnet)

```
username wendell secret odom
username chris secret youdda
!
line vty 0 15
  login local
```


SSH PASSI PER LA CONFIGURAZIONE

1. Configurare lo switch per generare una coppia di chiavi Pubblica-Privata da usare per la crittografia.
 1. Impostare l'hostname **hostname <name>**
 2. Inserire il domain name che insieme al nome dello switch completa il FQDN **ip domain-name <name>**
 3. Usare il comando **crypto key generate rsa** nella configurazione globale per generare la chiave RSA
2. Usa il comando **ip ssh version 2** per forzare l'uso della versione 2 di SSH anche per quei dispositivi che implementano anche la versione 1
3. Configura le VTY per accettare solo SSH ed escludere Telnet **transport input ssh** comando da utilizzare dopo aver selezionato le VTY
4. ATTENZIONE senza il comando **login local** l'autenticazione non viene richiesta

AAA SERVER RADIUS

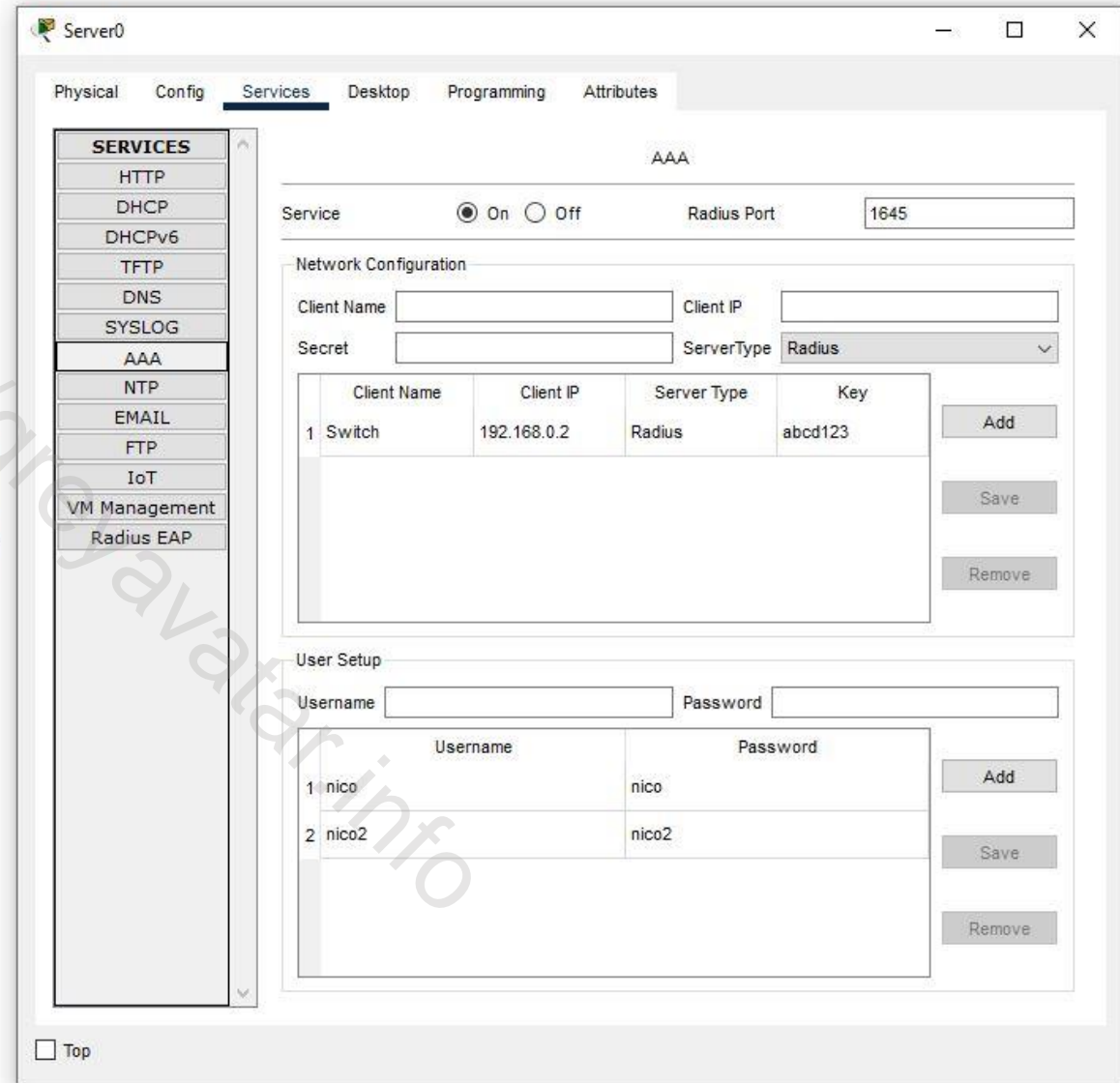
- L'utilizzo di utenti locali per il login ai dispositivi diventa un incubo per gli amministratori che dovrebbero impostare gli utenti su tutti i device in uso per poi modificarli al bisogno.
- Una possibilità che facilita la gestione è impostare un server di autenticazione RADIUS dal quale prelevare gli utenti per l'autenticazione. Gli stessi utenti possono essere usati per più servizi.

RADIUS CONFIGURAZIONE PACKET TRACER

1. Impostare un utente di backup in caso di problemi di comunicazione con il server **username <username> secret <Password>**
2. Identificare il server radius **radius-server host <ip>**
3. Identificare la chiave di accesso **tacacs-server key tacacspa55**
4. Impostare il nuovo sistema di controllo degli accessi **aaa new-model**
5. Impostare l'autenticazione utilizzando il server radius, il database locale sarà lo l'opzione di backup **aaa authentication login default group radius local**

PACKET TRACER SERVER AAA

- Packet Tracer tramite l'inserimento di un device server permette di simulare il servizio AAA



The screenshot shows the configuration window for 'Server0' in Packet Tracer, specifically the 'Services' tab. The 'AAA' service is selected and configured as follows:

- Service:** On (radio button selected)
- Radius Port:** 1645
- Network Configuration:**
 - Client Name:** [Empty]
 - Client IP:** [Empty]
 - Secret:** [Empty]
 - ServerType:** Radius
 - Table:**

	Client Name	Client IP	Server Type	Key	
1	Switch	192.168.0.2	Radius	abcd123	Add
 - Buttons:** Add, Save, Remove
- User Setup:**
 - Username:** [Empty]
 - Password:** [Empty]
 - Table:**

	Username	Password	
1	nico	nico	Add
2	nico2	nico2	
 - Buttons:** Add, Save, Remove

At the bottom left of the window, there is a 'Top' button.