CISCO IOS - Konfigurera åtkomst

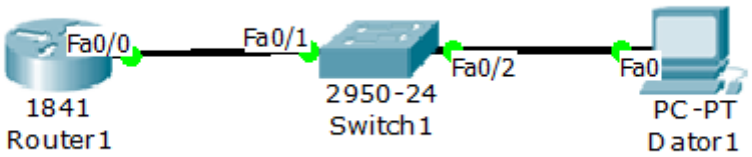
I denna laboration kommer vi titta på hur man konfigurerar åtkomst till nätverksutrustning som kör CISCO IOS. Laborationen kan antigen göras med fysisk labbutrustning eller med ett simuleringsprogram som *Packet Tracer (https://www.netacad.com/web/about-us/cisco-packet-tracer)* eller *GNS3* (http://www.gns3.net/). Vi kommer att utgå från användandet av *Packet Tracer* och/eller en fysisk labbmiljö. Fokus är att snabbt komma igång med användandet av nätverksutrustning från CISCO.

Antal: Enskilt eller i större grupp ifall fysisk labbutrustning används.

Material: En dator med programmet *Packet Tracer* eller en dator med serieport (eller serieportsadapter), CISCO router, switch och nätverkskablar (TP-kablar).

Tips: Titta på genomgångarna om CISCO IOS och introduktion till *Packet Tracer* på hemsidan. Samt tidigare laborationer då de till stor del bygger på varandra.

Topologi



Enhet	Gränssnitt	IP-adress	Nätmask	Default-Gateway	Switch port
Dator1	Fa0	192.168.0.10	255.255.255.0	-	Fa0/2
Router1	Fa0/0	192.168.0.1	255.255.255.0	-	Fa0/1
Switch1	VLAN1	192.168.0.5	255.255.255.0	-	-

Utförande: Används Packet Tracer så sker konfigurationen av enheterna via fliken *CLI* för respektive enhet. Används fysisk utrustning så sker konfigurationen via seriekabel och terminalprogram. Vi ska konfigurera enheterna för olika typer av åtkomst via nätverket. Detta innefattar en hel del säkerhet och för mer information om detta rekommenderas *CCNA Security* kursen. För att kunna konfigurera SSH i den fysiska miljön så gäller det att den CISCO IOS version som används har stöd för detta, k9 (crypto) image enligt cisco.com. Saknas kommandon så beror det på just detta.

1. Koppla samman enheterna enligt topologin. (används Packet Tracer så finns det en färdig projektfil där steg 1-3 redan är gjort).
2. Konfigurera IP-inställningar för Dator1
3. Konfigurera IP-inställningar för Router1
   enable
   configure terminal
   interface fastEthernet 0/0
   ip address 192.168.0.1 255.255.255.0
   no shutdown
   exit
4. Vi börjar med att konfigurera ett meddelande som kommer att visas då man ansluter till routern, så kallad *banner*. Rekommendationen är att alltid ha ett sådant meddelande som

informerar om att obehöriga äger ej tillträde. Vi skapar detta med följande kommando i Global Configuration läge:
banner login "Access for authorized users only. Please enter your username and password."

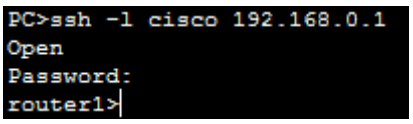
5. Nästa rekommenderade steg är att alltid sätta ett lösenord för åtkomst till *Privileged EXEC* läget. Detta görs med:
   enable secret cisco1234
   Nu skapas lösenordet *cisco1234* som blir MD5-krypterat. Det går att använda ett annat alternativ som skapar ett okrypterat lösenord men det är ej rekommenderat då man kan se lösenordet i klartext om man tittar i konfigurationsfilerna. Med kommandot **service password-encryption** så krypteras alla lösenord i systemet vilket kan vara bra att göra i ”skarpt” läge. Skulle en obehörig få fysisk åtkomst till routern så kan har vi nu skydd från enkel åtkomst via seriekabel.
6. Oftast så vill man kunna administrera enheter via nätverket. Ett sätt är att konfigurera åtkomst via telnet. För att aktivera detta på routerns skriver vi:
   line vty 0 4
   password cisco4321
   login
   Första raden aktiverar terminalåtkomst för *line* 0 till 4 dvs. 5 logiska anslutningar tillåts samtidigt (VTY, Virtual Terminal Line). Följande kommando sätter lösenord för åtkomst när man loggar in. Efter detta tillåts både telnet och SSH protokollet (mer om detta senare).
7. Nu ska vi testa att ansluta till routern via nätverket (telnet). Dator1 behöver en telnetklient. Det går bra med t.ex. *PuTTY*. Används Packet Tracer eller äldre version av Windows (XP och äldre) så kan vi starta kommadotolken och ansluta med kommandot
   telnet 192.168.0.1
   I Packet Tracer ser det ut såhär:

```
PC>telnet 192.168.0.1
Trying 192.168.0.1 ...Open
 test

User Access Verification

Password:
```

   Logga in med lösenordet vi satte (*cisco4321*). Prova sedan att **enable** kommandot och kontrollera att lösenorder *cisco1234* krävs. Avsluta med **exit**
8. Som ni säkert vet så är telnet okrypterat och därmed inte säkert. Ett betydligt bättre alternativ är protokollet *SSH (Secure Shell)*. Detta aktiveras på följande sätt.
   Ange följande kommandon på routern:
   hostname router1
   aaa new-model
   username cisco secret 0 ssh1234
   ip domain-name test.com
   crypto key generate rsa
   ange **1024**
   ip ssh time-out 60
   ip ssh authentication-retries 2
   Kommentarer: Vi börjar med att sätta hostname ifall detta inte redan är gjort. Nästa kommando aktiverar *AAA* (Authentication, Authorization and Accounting) vilket ger massa fler möjligheter till övervakning och kontroll som vi inte tar upp nu. Nästa kommando skapar ett användarnamn och lösenord (MD5-krypterat), nollan betyder att vi matar in lösenordet i

klartext. Nästa kommando konfigurerar DNS-domän namn för routern. Med crypto-kommandot genereras krypteringsnycklarna som krävs för SSH. En nyckellängd på minst 1024 bitar rekommenderas. De två sista kommandona aktiverar SSH och konfigurerar timeout och antal autentiseringsförsök som tillåts.

9. När detta är gjort så har vi startat en SSH-server på routern och den tillåter sedan innan *line* åtkomst via både telnet och ssh. Oftast vill man begränsa så att man enbart tillåter ssh-protokollet. Detta görs med:
   line vty 0 4
   transport input ssh
   Med transport kommandot anger vi att vi enbart accepterar ssh-protokollet för inkommande anslutningar vilket per automatik nekar åtkomst via telnet.
10. Kontrollera att vi kan ansluta till routern med SSH. För detta krävs en SSH-klient till datorn ifall vi gör labben i fysisk miljö (t.ex. *PuTTY*). I Packet Tracer så klickar vi på Dator1 och väljer *Command Prompt*. Anslut till routern med följande kommando:
    ssh –l cisco 192.168.0.1



    Med växeln **–l** anges inloggningsnamn, *cisco* ange lösenordet *ssh1234*
11. Nu när vi konfigurerat åtkomst till routern så är det dags att göra samma med switchen. Det som skiljer är att vi inte har ett specifikt interface som vi kan konfigurera IP-inställningar för då switchen jobbar på lager 2. Det vi kan göra är att sätta IP-inställningar för ett logiskt interface nämligen för ett VLAN. Vi kommer nu att konfigurera switchen för åtkomst via SSH via VLAN1 vilket som standard är det VLAN som alla portar är anslutna till.
    Anslut till switchen och ange följande:
    enable
    configure terminal
    enable secret cisco1234
    interface vlan 1
    ip address 192.168.0.5 255.255.255.0
    no shutdown
    exit
    hostname switch1
    username cisco secret 0 ssh1234
    ip domain-name test.com
    crypto key generate rsa
    ange **1024**
    ip ssh time-out 60
    ip ssh authentication-retries 2
    line vty 0 4
    transport input ssh
    login local
    Ser i stort sett ut som tidigare med undantag att AAA inte stöds i den version av CISO IOS som körs i switchen om vi använder Packet Tracer. En lokal användare, *cisco* med lösenordet *ssh1234,* skapas precis som innan och med det sista kommandot **login local** så anger vi att vi ska använda lokala användare vid anslutning via vty.
12. Kontrollera att det går att ansluta till switchen med SSH via nätverket precis som i steg 10.
13. Redovisa resultatet för handledaren.

Sammanfattning kommandon

Kommando	Beskrivning
enable secret cisco1234	Lösenordskyddar Privileged EXEC mode
username cisco secret 0 ssh1234	Skapar en lokal användare med lösenord
aaa new-model	Aktiverar AAA
ip domain-name test.com	Anger domännamn
crypto key generate rsa	Generera krypteringsnyckel som krävs för SSH
ip ssh time-out 60	Aktiverar SSH sätter timeout till 60 sekunder
ip ssh authentication-retries 2	Sätter maximala anslutningsförsök till 2
line vty 0 4	Aktivera terminalåtkomst för 5 (0-4) ”lines”
transport input ssh	Begränsar inkommande linjeprotokoll till SSH
login local	Anger att vi ska använda lokala konton för åtkomst
banner login ”text”	Skapar ett välkomstmeddelande

Svart = EXEC kommando, Blå = Global Configuration, Grön = Interface Configuration, Orange = funkar alltid, Rött = Line configuration

Detta skall du kunna efter genomförd labb:

- ✓ Skapa ett välkomstmeddelande
- ✓ Begränsa/skydda åtkomst till Privileged EXEC mode
- ✓ Konfigurera en router eller switch för nätverksåtkomst via telnet
- ✓ Konfigurera en router eller switch för nätverksåtkomst via SSH
- ✓ Ansluta till en enhet via telnet eller SSH