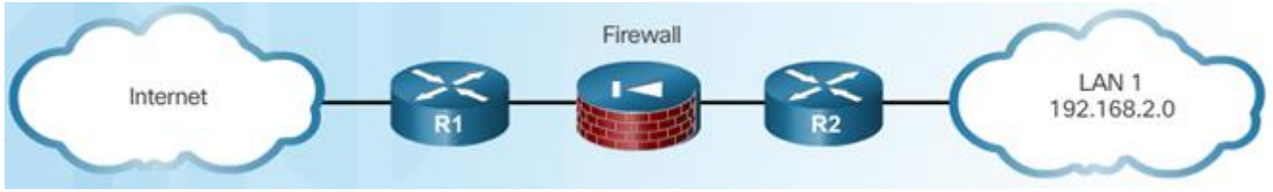
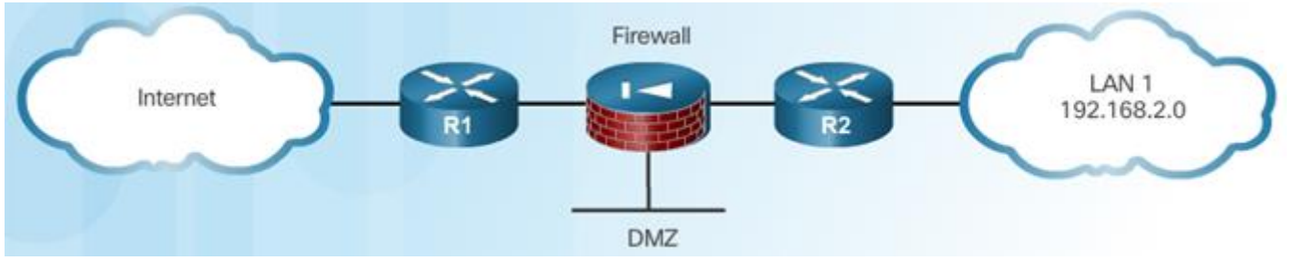

DIGINTO
Nätverkssäkerhet

AAA – grunder

Säkerhet för nätverksinfrastruktur

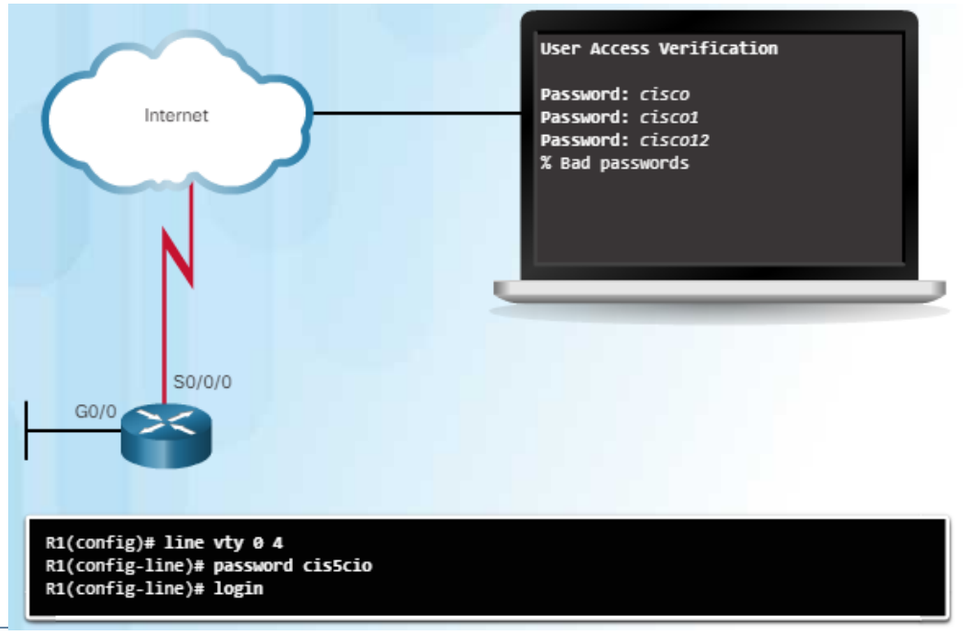
- Vad för sökerhetspolicy bör ha en router som ansluter ett nätverk till Internet?
- Säkrare med en router till och en brandvägg mellan de.
- Hur ska nätverkshanterare i ett nätverk säkras?
- Enskilda säkerhetskonfigurationer per nätverkshanterare?
- Vilka risker utsätts ett nätverk anslutet till Internet?
- Cybergkriminella
- Felaktiga konfig
- Fel nätverksdesign
- Fel protokoll
- Fel mjukvara

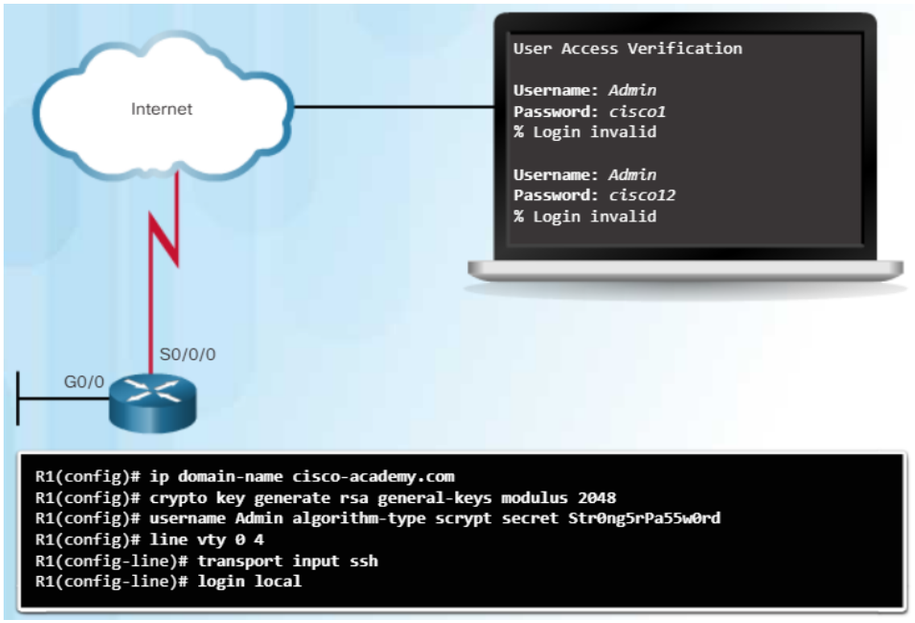




Fjärråtkomstautentisering

- Inloggnings- och lösenord på konsolporten, vty-linjer och aux-portar.
- Men den är också den svagaste och minst säkra.
- SSH kräver ett användarnamn och ett lösenord, som båda är krypterade under överföringar.
- Den lokala databasmetoden ger ytterligare säkerhet.
- Användarnamnet registreras i den lokala databasen när en användare loggar in.
- Den lokala databasen måste konfigureras manuellt.





Osäker fjärråtkomstautentisering

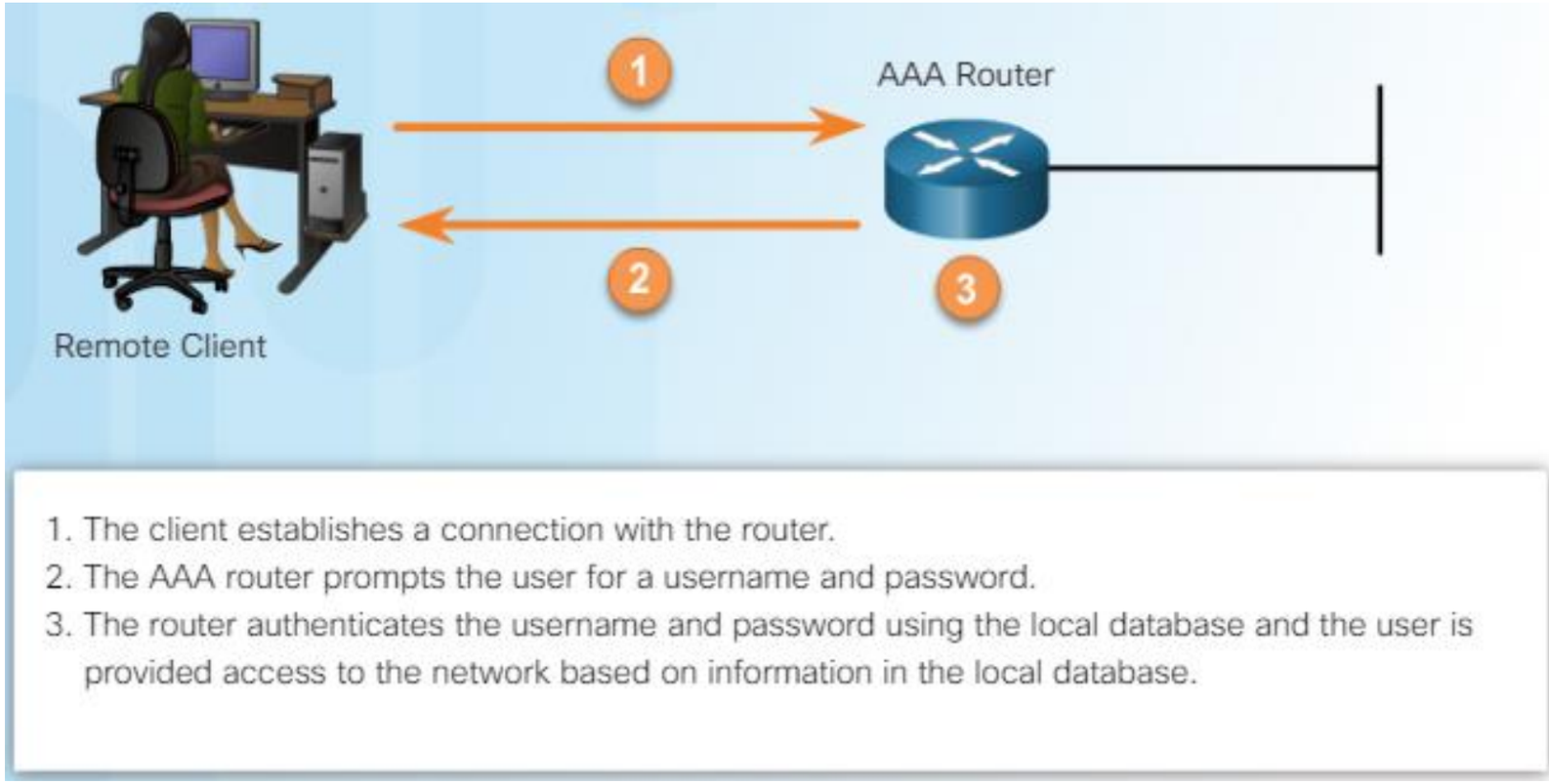
- enable
- conf t
- hostname R1
- enable secret ensecPa55
- int g0/0
- ip address 20.20.20.1 255.255.255.252
- no shut
- exit
- int g0/1
- ip address 10.10.10.1 255.255.255.0
- no shut
- exit
- ip domain-name diginto.se
- crypto key generate rsa general-keys modulus 2048
- ip ssh version 2
- username Admin01 secret RAsecPa5501
- line vty 0 4
- transport input ssh
- login local
- exit
- ip route 30.30.30.0 255.255.255.0 20.20.20.2
- end

AAA - grunder

- Dagens nätverk är globala och det är mer dynamiska än någonsin
- De kräver avancerade säkerhetssystem grundat i viktiga principer:
  - “Vem eller vad är du?”
  - “Vad är du tillåten att göra?”
  - “Vad gjorde du?”
- AAA är ett sätt att kontrollera vem som får åtkomst till ett nätverk (autentisera), vad de kan göra medan de är där (auktorisera) och att granska vilka åtgärder de utförde när de kom åt nätverket (redovisning).
  - Authenticaton
  - Authorization
  - Accounting
- Det är inte klart när termen AAA först fick acceptans, men redan i ett dokument från IEEE från 1983 finner “Authentication, Authorization, Accounting”

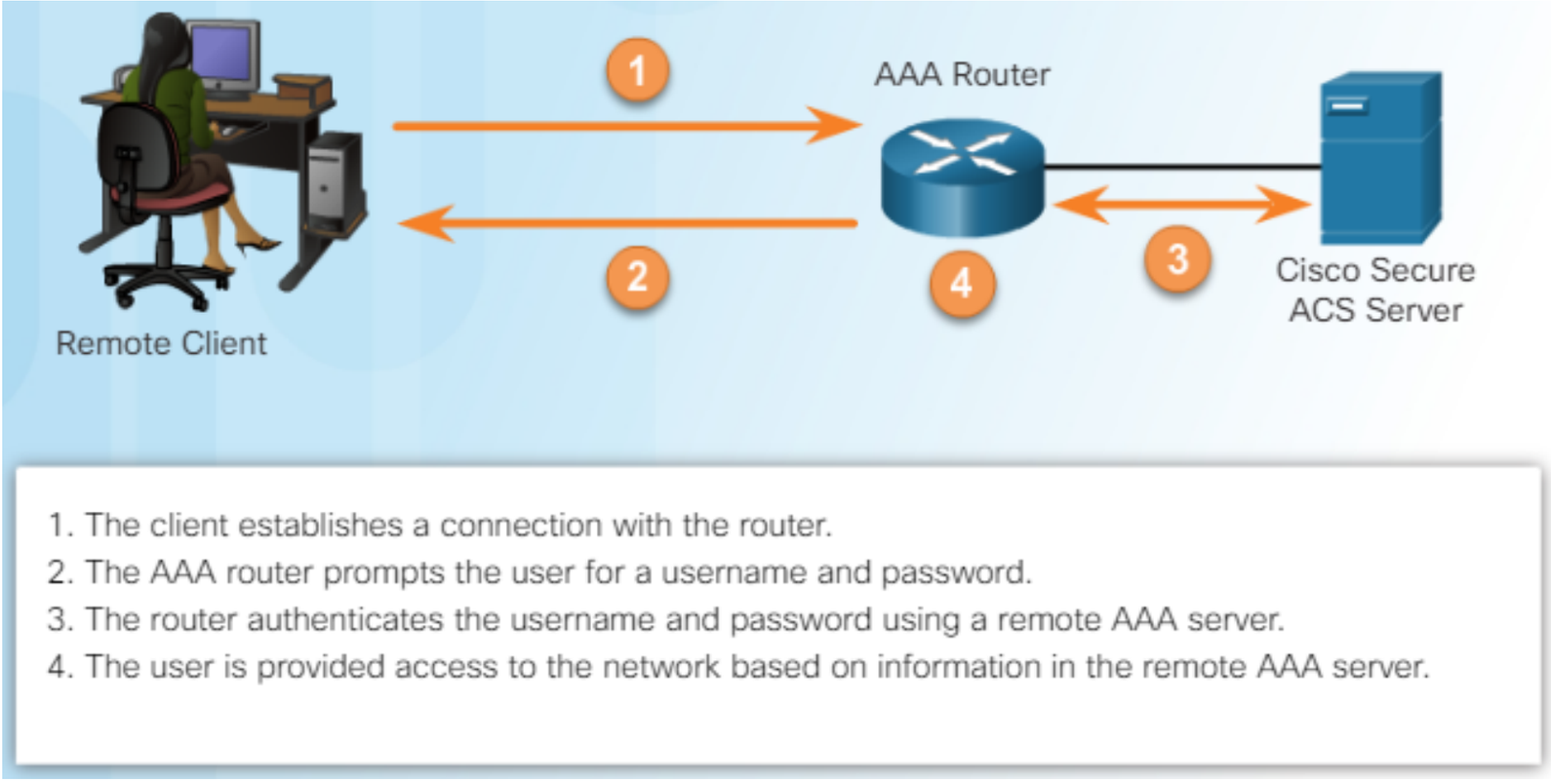
AAA - Autentiseringssätt

- Cisco tillhandahåller två vanliga sätt för att implementera AAA-tjänster:
- *Lokal AAA-autentisering* - Användarnamn och lösenord lagras lokalt i Cisco-routern och användare autentiserar sig mot den lokala databasen.
- Lämplig metod för små nätverk.



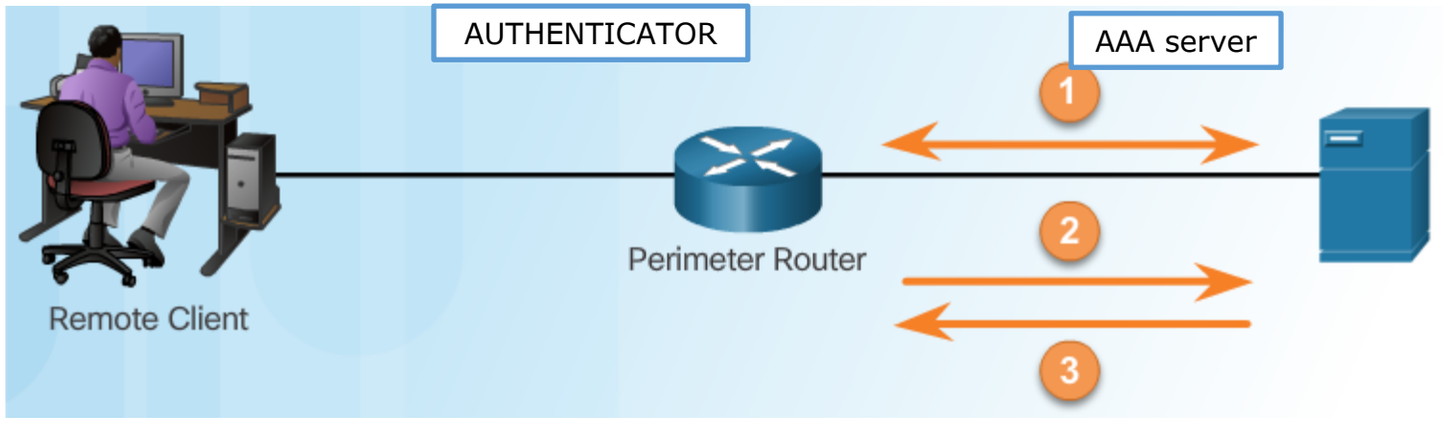
AAA - Autentiseringssätt

- *Serverbaserad AAA-autentisering* - Den centrala AAA-servern innehåller användarnamn och lösenord för alla användare.
- Routern använder antingen RADIUS eller TACACS+ för att kommunicera med AAA-servern.
- När det finns flera routrar och switchar är serverbaserad AAA mer lämplig.



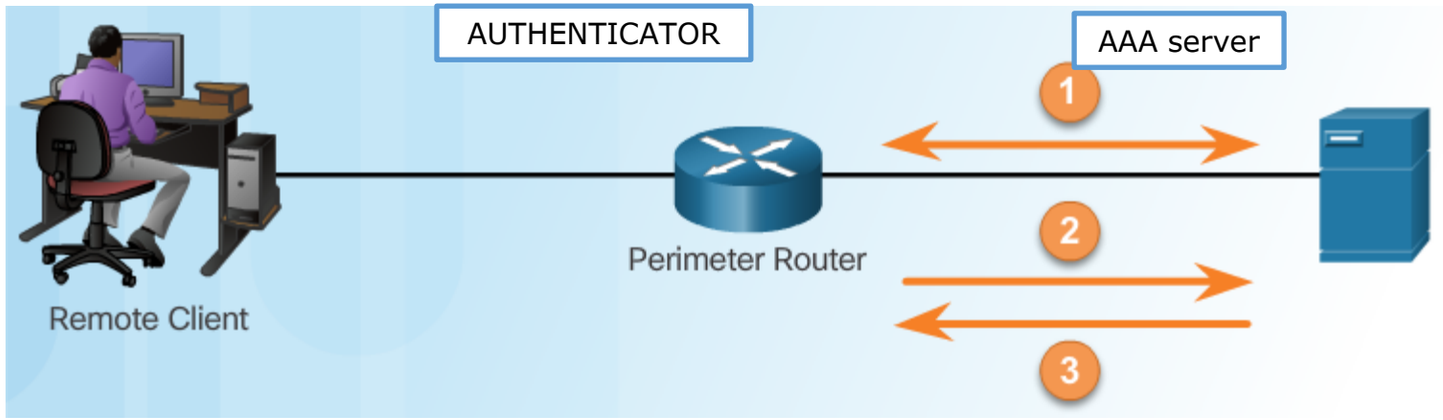
AAA - Auktorisering

- När autentisering har bekräftat inloggningsuppgifter upprättas en session mellan klienten och den autentiserande server.
- Auktorisation avser processen i vilken definieras användarens åtkomst till nätverket och dess resurser.
- Användare kan få olika behörighetsnivåer som begränsar deras åtkomst till nätverket och tillhörande resurser.
- Det kan hända att användare autentiseras och tillåtas a starta en session men ändå kan klienten nekas åtkomst till någon specifik nätverksresurs.



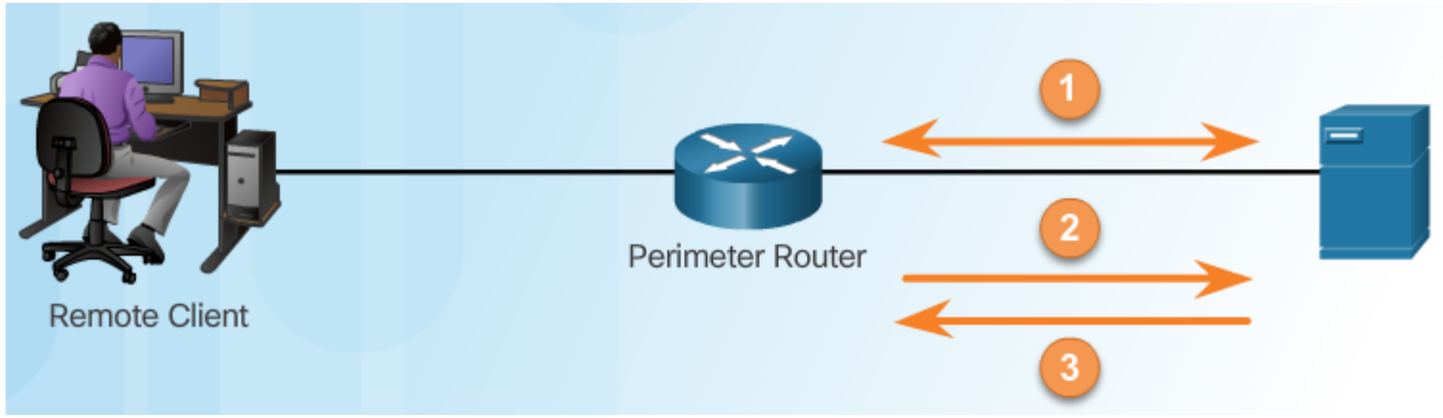
AAA - Granskning

- Detta är processen som håller reda på användarens aktivitet när den är ansluten till ett system.
- Granskningen inkluderar anslutningstiden, åtkomstplatser, datatrafik, mm.
- Några intressanta granskningsaspekter:
- Nätverk, anslutning, exekveringsläge, systemåtkomst, mest använda kommando, resursanvändning.
- Syftet är att definiera beteende, överträdelser, resursanvändning.
- Att spåra tillbaka till händelser som ledde fram till en attackvektor kan vara mycket värdefullt för en analys och förebyggande säkerhetspolicy.



AAA - Granskning

- Nätverksgranskning - samlar in information för alla PPP-sessioner (Point-to-Point Protocol), inklusive paket- och byte-räkningar.
- Anslutningsgranskning - samlar in information om alla utgående anslutningar från AAA-klienten, såsom Telnet eller SSH.
- Exekveringsgranskning - fångar information om terminal-sessioner på servern, användarnamn, datum, start- och stopptider och IP-adress.
- Systemgranskning - samlar in information om alla händelser på systemnivå
- Kommandogranskning - fångar detaljerad information över kommandon som körs, samt datum och tidpunkt då varje kommando exekverades och användaren som exekverade det.



Lokalt AAA - autentisering

- Steg 1. Lägg till användarnamn och lösenord i den lokala databasen.
- Steg 2. Aktivera AAA globalt på routern.
- Steg 3. Konfigurera AAA-parametrar på routern.
- Steg 4. Bekräfta och felsök AAA-konfigurationen.
- *aaa new-model* automatiskt sätter den lokala databasen igång det därför bör man skapa användare innan detta kommando exekveras.
- *aaa authentication login* tillåter inloggning via konsol- eller vty-terminaler.
- *default* gäller för alla linjer, utom de som har en annan konfiguration som åsidosätter default.
- *local-case* betyder att lösenordet och användarnamnet är skiftlägeskänsliga.


```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aa authentication login default local-case
R1(config)#
```

Lokalt AAA - autentisering

- För flexibilitet kan olika autentiseringsmetoder tillämpas på olika interface och linjer med kommandot *aaa authentication login*.
- Till exempel kan en administratör tillämpa en speciell inloggning för SSH och sedan ha default inloggningsmetoden för linjekonsolen.
- Den lokala databasen SSH-LOGIN används för autentisering via vty.
- Alla andra linjer skulle använda den lokala databasen och kommandot *enable* som reserv om det inte fanns några databasposter på enheten.
- När en anpassad autentiseringsmetodlista tillämpas på ett interface och om man ångrar konfigurationen exekvera kommandot *no authentication login* för att falla tillbaka till *default*.


```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login SSH-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
```

Lokalt AAA – autentiserings exampel

- Configure user accounts:
  - JR-ADMIN account with a type 9 (scrypt) encrypted password Str0ngpa55w0rd
  - ADMIN account with a type 9 encrypted password Str0ng5rPa55w0rd.
- Enable AAA on the router
- Configure the default authentication list with a primary method as loal case-sensitive login with the enable secret as backup.
- Configure a second authentication list named SSH-LOGIN that has only one method, local case-sensitive login.
- Configure accounts to be locked out after a maximum of 3 unsuccessful attempts.
- Apply the SSH-LOGIN list to the virtual terminal lines.
- Use the end command to exit configuration mode.
- Use the show command to view the current AAA sessions on R1.

Lokalt AAA – autentiserings exempel

- *Configure user accounts*:
  - JR-ADMIN account with a type 9 (scrypt) encrypted password Str0ngpa55w0rd
  - ADMIN account with a type 9 encrypted password Str0ng5rPa55w0rd.
- R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ngPa55w0rd
- R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
- *Enable AAA on the router*
- R1(config)# aaa new-model
- *Configure the default authentication list with a primary method as loal case-sensitive login with the enable secret as backup.*
- R1(config)# aaa authentication login default local-case enable
- *Configure a second authentication list named SSH-LOGIN that has only one method, local case-sensitive login.*
- R1(config)# aaa authentication login SSH-LOGIN local-case

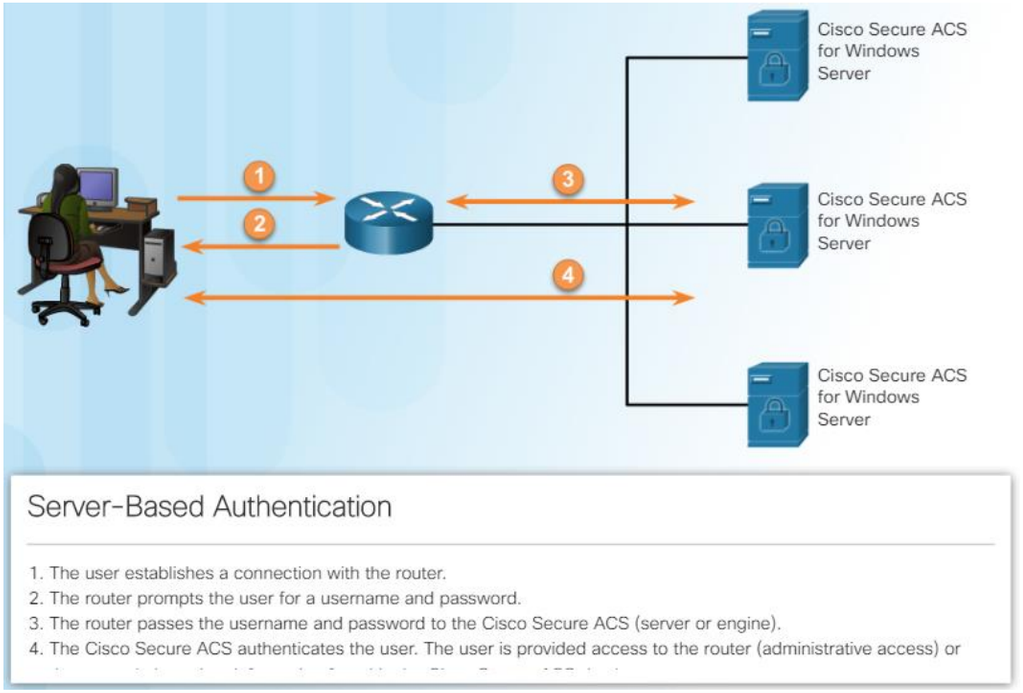
Lokalt AAA – autentiserings exampel

- *Configure accounts to be locked out after a maximum of 3 unsuccessful attempts.*
- R1(config)# aaa local authenticaton attempts max-fail 3
- *Apply the SSH-LOGIN list to the virtual terminal lines.*
- R1(config)# line vty 0 4
- R1(config-line)# login authentication SSH-LOGIN
- *Use the end command to exit configuration mode.*
- R1(config-line)# end
- *Use the show command to view the current AAA sessions on R1.*
- R1# show aaa sessions
- Use the debug command to view AAA authentication messages
- R1# debug aaa authentication

Lokalt och serverbaserade AAA

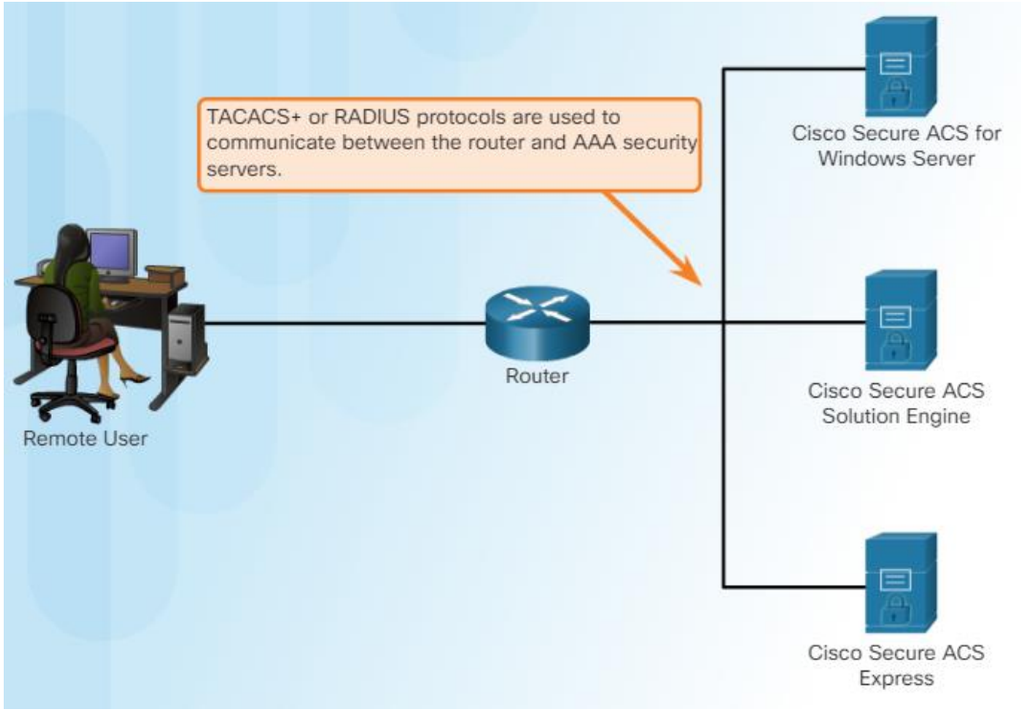
Lokalt vs Serverbaserade AAA autentisering

- Lokala implementeringar av AAA är för små nätverk.
- I stora företagsnätverk kan användas:
  - en eller flera AAA-servrar
  - Cisco Secure ACS
- *Cisco Secure ACS* kan skapa en central databas för användare och administrativ åtkomst som alla enheter i nätverket kan hänvisa till.
- Det kan också fungera med många externa databaser, inklusive Active Directory och LDAP.
- Dessa databaser lagrar användarkontouppgifter och lösenord.
- Det möjliggör central administration.



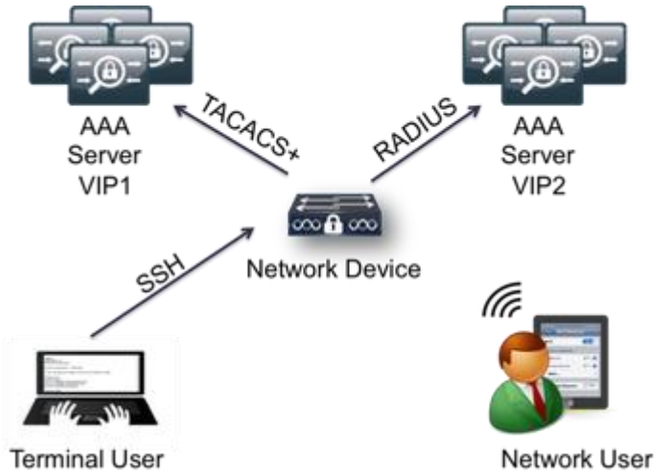
Cisco secure Access Control System

- Cisco Secure Access Control System (ACS) är en central lösning som binder samman företagets nätverks säkerhetspolicy och identitetsstrategi.
- Cisco ACS kan användas för att kontrollera administratörsåtkomst och konfiguration för alla nätverksenheter i ett nätverk som stöder RADIUS, eller TACACS +, eller båda.
- TACACS + och RADIUS är de två dominerande protokollen som används av Cisco säkerhetsapparater, routrar och switchar för att implementera AAA.



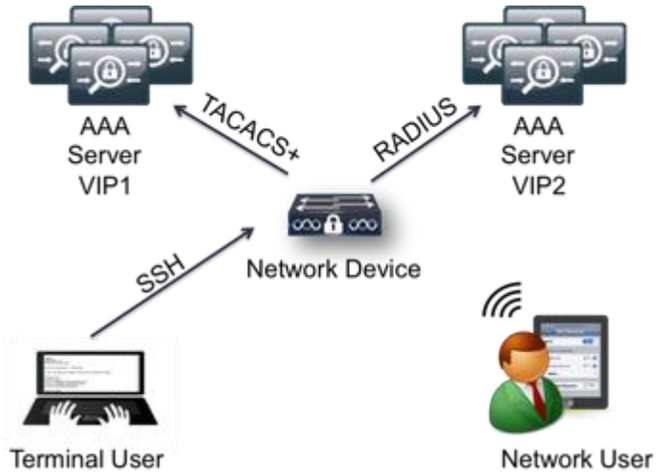
TACACS+ och RADIUS

- TACACS + och RADIUS är båda autentiseringsprotokoll som stöder var och en olika funktioner som används för att kommunicera med AAA-servrar.
- Medan båda protokollen kan användas för att kommunicera mellan en router och AAA-servrar, anses TACACS + vara det säkrare protokollet.
- Detta beror på att alla TACACS + -protokollutbyten är krypterade, medan RADIUS bara krypterar användarens lösenord.
- RADIUS krypterar inte användarnamn, bokföringsinformation eller annan information som tas med i RADIUS-meddelandet



TACACS+ och RADIUS

- Det är viktigt att förstå skillnader mellan TACACS + och RADIUS.
- Dessa är tre viktiga faktorer för TACACS +:
  - Separerar autentisering och auktorisering
  - Krypterar all kommunikation
  - Använder TCP-port 49
- Dessa är fyra kritiska faktorer för RADIUS:
  - Kombinerar RADIUS-autentisering och auktorisering som en process
  - Krypterar bara lösenordet
  - Använder UDP
  - Stöder tekniker för fjärråtkomst, 802.1X och SIP (Session Initiation Protocol)



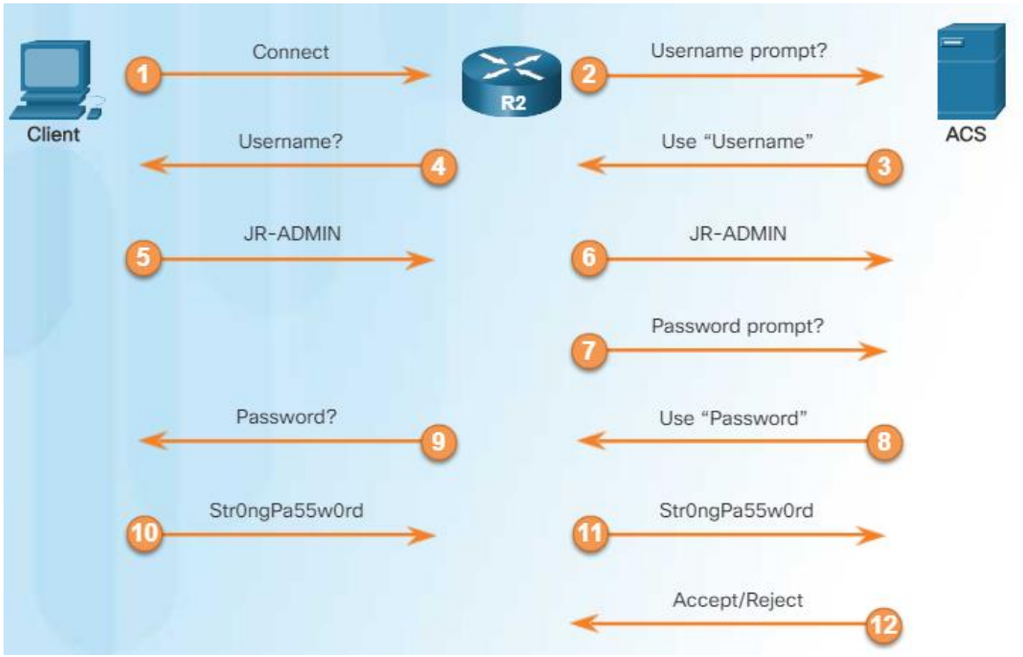
Skillnader mellan TACACS+ och RADIUS

- RADIUS- eller TACACS + protokoll kan tillhandahålla ett centralt autentiseringsprotokoll för användare, routrar, switchar eller servrar.
- De viktigaste skillnaderna mellan RADIUS och TACACS+ är:

RADIUS	TACACS+

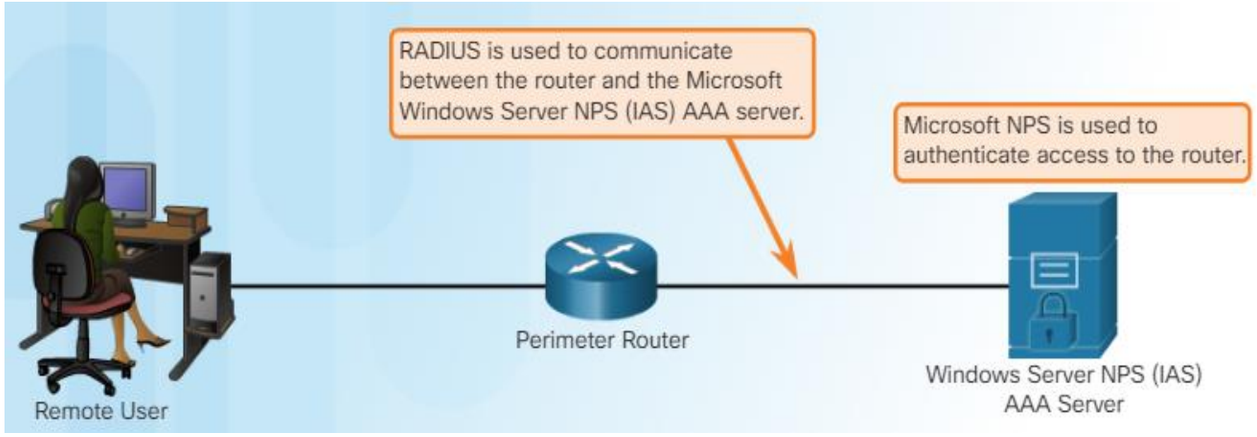
TACACS+ Autentisering

- TACACS+ står för *Terminal Access Control Access Control Server*.
- TACACS+ är en vidareuppdatering av det ursprungliga TACACS-protokollet.
- Trots sitt namn är TACACS+ ett helt nytt protokoll som inte är kompatibel med någon tidigare version av TACACS.
- TACACS + tillhandahåller separata AAA-tjänster.
- TACACS+ kan användas för auktorisering och granskning medan man använder en annan autentiseringsmetod.
- TACACS+ krypterar hela paketet för säkrare kommunikation och använder TCP-port 49.



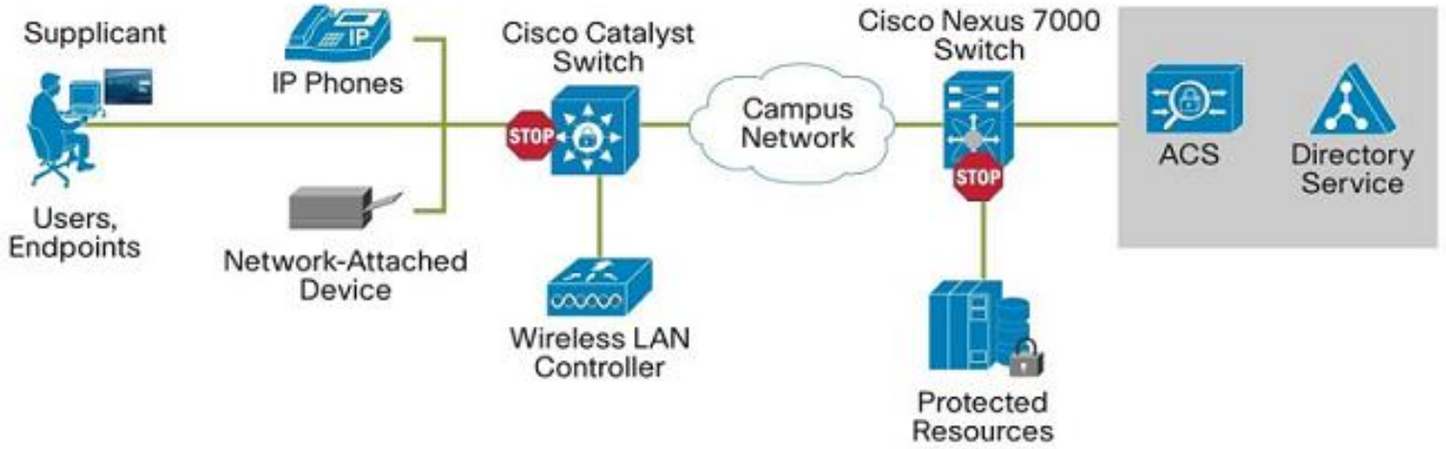
AAA och Active Directory

- Microsoft Active Directory (AD) används för att autentisera och auktorisera användare när de loggar in på Windows-domänen.
- Microsoft AD kan också användas för att hantera autentisering och auktorisering på Cisco IOS-enheter.
- Cisco Secure ACS kan integreras för att använda AD-tjänster
- Microsoft RADIUS är känd som Internet Authentication Service (IAS).
- IAS bytt namn (2008) till Network Policy Server (NPS).
- Konfigurationen för Cisco IOS är densamma som att kommunicera med valfri RADIUS-server.
- Den enda skillnaden är att Microsofts serverns AD-controller används för att utföra autentiserings- och auktoriseringstjänster.



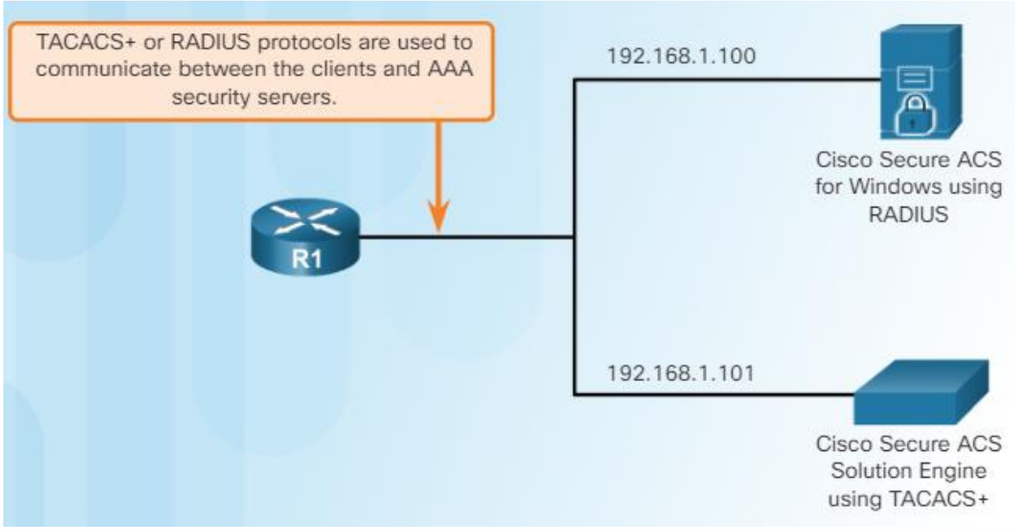
AAA och Identity Service Engine - ISE

- En nätverksadministratör vill logga in på en L3 switch.
- en autentiseringsprocess startas
- Switchen uppmanar användaren till att ange inloggningsuppgifter.
- Efter att ha fått användarnamnet och lösenordet skickar switchen de uppgifterna till AAA-servern och väntar på ett svar.
- ACS-servern tar emot autentiseringsbegäran och kontrollerar autentiseringsuppgifter.
  - Om ACS-servern är konfigurerad att kontakta en domänkontrollant skickar ACS-servern begäran till domänkontrollanten och väntar på svar.
  - Om ACS-servern är konfigurerad att använda den lokala databasen verifierar ACS-server användarnamnet och lösenordet och därefter skickar ett svar till routern.
  - *ACS migreras till Cisco ISE och ISE är en del av NAC*



Konfiguration av serverbaserade AAA autentisering

- Till skillnad från lokal AAA autentisering måste serverbaserad identifiera de olika TACACS+ och RADIUS-servrar AAA-tjänster.
- Steg 1. Aktivera AAA globalt för att tillåta användning av alla AAA-element. Detta steg är en förutsättning för alla andra AAA-kommandon.
- Steg 2. Ange ACS-servern som ska tillhandahålla AAA-tjänster för routern. Detta kan vara en TACACS+ eller RADIUS-server.
- Steg 3. Konfigurera den krypteringsnyckel som behövs för att kryptera dataöverföringen mellan nätverksåtkomstservern och Cisco Secure ACS.
- Steg 4. Konfigurera listan över AAA autentiseringsmetoder så att den hänvisar till TACACS+ eller RADIUS-servern.



TACACS+ server implementation

- *Enable AAA*
- R1(config)# aaa new-model
- *Enter TACACS+ server configuration mode and name the server configuration SERVER-T*
- R1(config)# tacacs server SERVER-T
- *Configure the TACACS+ server address to 192.168.1.100.*
- R1(config-server-tacacs)# address ipv4 192.168.1.100
- *Configure a single persistent TCP connection to the TACACS+ server.*
- R1(config-server-tacacs)# single-connection
- *Configure the shared secret key TACACS-Pa55w0rd.*
- R1(config-server-tacacs)# key TACACS-Pa55w0rd
- *Exit TACACS+ server configuration mode.*
- R1(config-server-tacacs)# exit
- R1(config)#

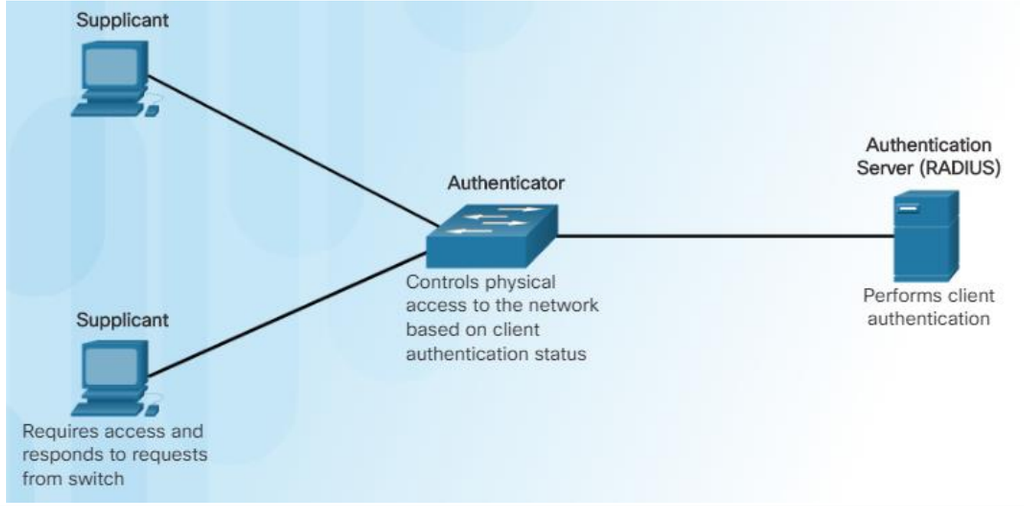
RAIDUS server implementation

- *Enter RADIUS server configuration mode and name the configuration SERVER-R.*
- R1(config)# radius server SERVER-R
- *Configure the RADIUS server address 192.168.1.101 with the authentication port set to 1812 and th accounting port set to 1813.*
- R1(config-radius-server)# addres ipv4 192.168.1.101 auth-port 1812 acct-port 1813
- *Configure the shared key RADIUS-Pa55w0rd.*
- R1(config-radius-server)# key RADISU-Pa55w0rd
- *Exit RADIUS server configuration mode.*
- R1(config-radius-server)# exit
- *Specify a default authentication method list with primary option TACACS+, secondary option RADIUS, and tertiay option local username case-sensitive authentication. After configuration, exit configuration mode.*
- R1(config)# aaa authentication login default group tacacs+ group radius local-case
- R1(config)# exit

IEEE 802.1X Port Control

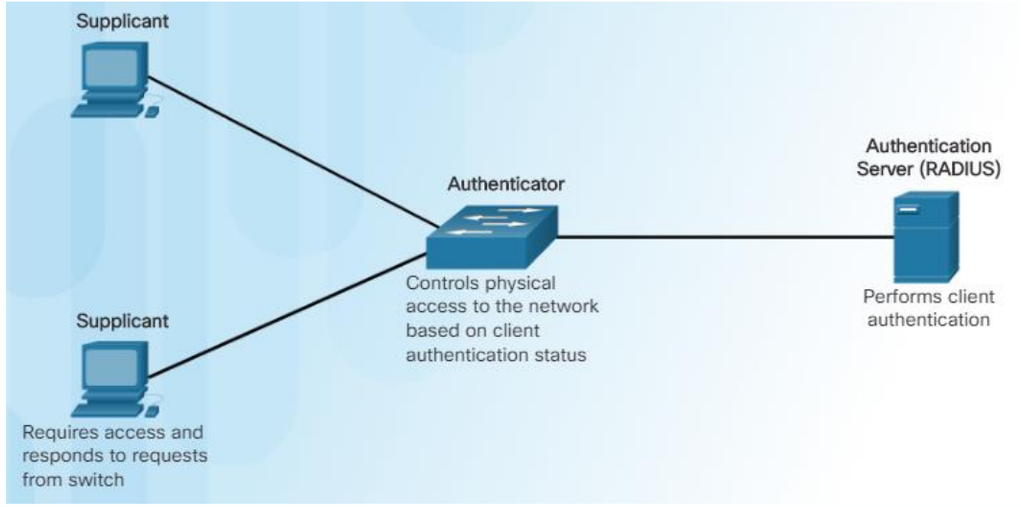
802.1X Portbaserad autentisering

- IEEE 802.1X-standarden definierar ett portbaserat åtkomstkontroll- och autentiseringsprotokoll som begränsar obehöriga arbetsstationer från att ansluta till ett LAN via allmänt tillgängliga switchportar.
- Autentiseringsservern autentiserar varje arbetsstation som är ansluten till en switchport innan alla tjänster som erbjuds av switch eller LAN finns tillgängliga.



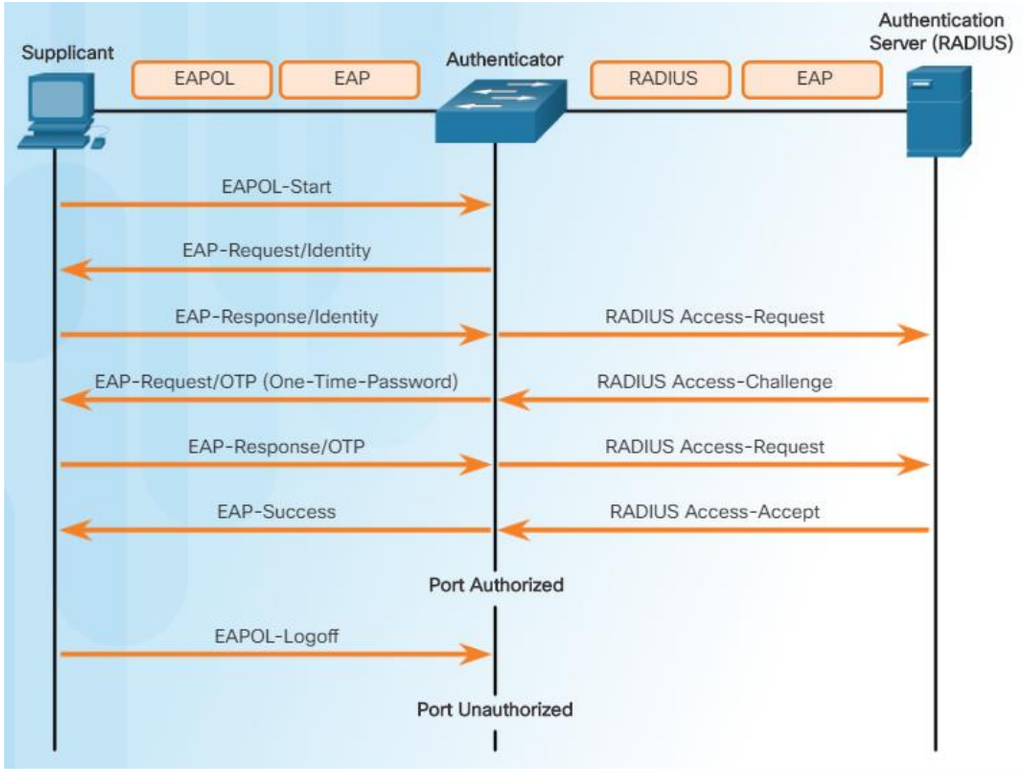
802.1X Portbaserad autentisering

- *Supplicant* (Client) - Nätverksenheten som begär åtkomst till LAN och switchtjänster och sedan svarar på förfrågningar från switch.
- Nätverksenheten måste stödja IEEE 802.1X protokoll
- *Authenticator* - Switchen verifierar supplikantens informationen med autentiseringsservern och vidarebefordrar ett svar till klienten.
- Switchen använder 802.1X för inkapsling och avkapsling av EAP-ramarna (Extensible Authentication Protocol) och interagerar med autentiseringsservern.
- *Autentiseringsserver* - Utför den faktiska autentiseringen av klienten.
- RADIUS-säkerhetssystemet med EAP-tillägg är den enda autentiseringsservern som stöds.



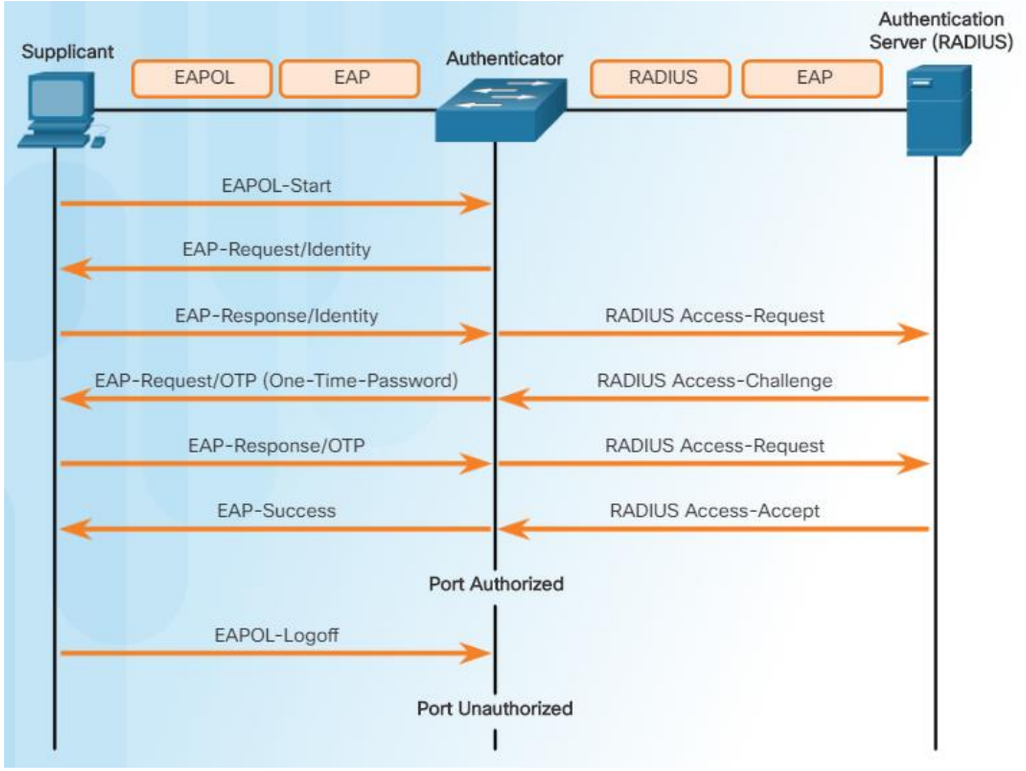
802.1X Portbaserad autentisering

- När switchen är konfigurerad för 802.1X-portbaserad autentisering startarautentiseringsprocessen.
- Tills arbetsstationen är autentiserad möjliggör 802.1X användning av endast Extensible Authentication Protocol via LAN (EAPOL), Cisco Discovery Protocol (CDP) och Spanning Tree Protocol (STP) -trafik genom porten till vilken arbetsstationen är ansluten.
- porten i obehörigt tillstånd.
- I detta tillstånd tillåter inte porten all ingångs- och utgångstrafik förutom 802.1X-protokoll-, STP- och CDP-paket.



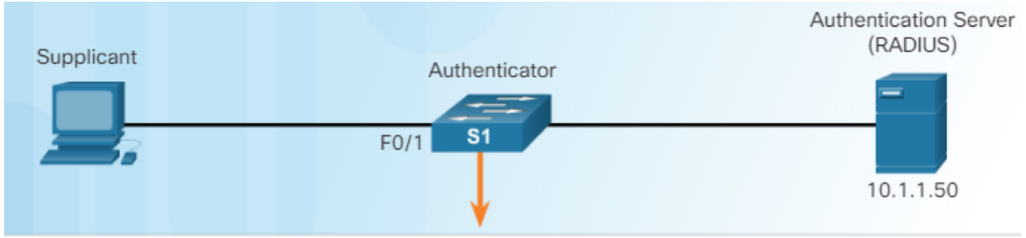
802.1X Portbaserad autentisering

- När en klient har godkänts övergår porten till det auktoriserade tillståndet så att all trafik för klienten kan flöda normalt.
- Om klienten inte stöder 802.1X, förblir porten i obehörigt tillstånd och klienten får inte åtkomst till nätverket.
- Om klienten stöder 802.1X men switchen inte är konfigurerad för autentisering anger sig klienten för godkänd och börjar skicka ramar som om porten är i auktoriserat tillstånd.



802.1X implementation

- Steg 1. Aktivera AAA med kommandot aaa new-model och konfigurera RADIUS-servern.
- Steg 2. Skapa en 802.1X portbaserad autentiseringsmetodlista med aaa-autentisering dot1x-kommandot.
- Steg 3. Aktivera 802.1X portbaserad autentisering globalt med kommandot dot1x system-auth-control.
- Steg 4. Aktivera portbaserad autentisering på gränssnittet med autokommandot för autentiseringsportkontroll.
- Steg 5. Aktivera 802.1X-autentisering på interfacet med kommandot dot1x pae.



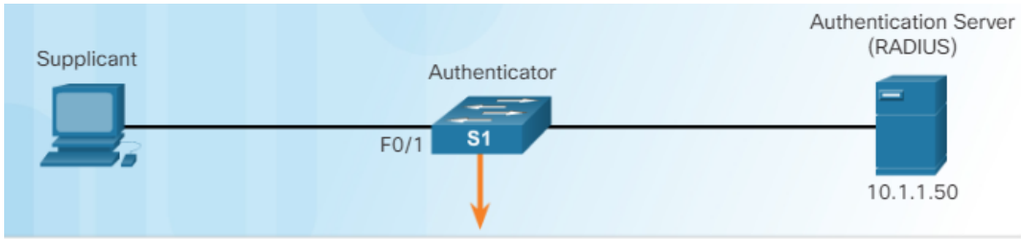

```
S1(config)# aaa new-model
S1(config)# radius server CCNAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```

RADIUS server konfiguration på S1

- *Enable AAA.*
- S1(config)# aaa new-model
- *Enter RADIUS server configuration mode and name the configuration CCNAS.*
- S1(config)# radius server CCNAS
- *Configure the RADIUS server Address to 10.1.1.50 with the authentication port of 1912 and the accounting port of 1813*
- S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
- *Configure the shared secret key RADIUS-Pa55w0rd.*
- S1(config-radius-server)# key RADIUS-Pa55w0rd
- *Exit RADIUS configuration mode.*
- S1(config-radius-server)# exit
- *Specify an 802.1x port-based default authentication method list with the primary option RADIUS.*
- S1(config)# aaa authentication dot1x default group radius
- *Globally enable 802.1x port-based authentication.*
- S1(config)# dot1x system-auth-control

Konfiguration av interface f0/1 för 802.1X

- Configure the interface as an access switchport.
- Enable port-based authentication on the interface.
- Enable 802.1x authentication with the Port Access Entity (PAE) type so the interface acts only as an authenticator.
- Use the end command to exit from configuration mode.
- S1 (config)# interface f0/1
- S1 (config-if)# switchport mode access
- S1 (config-if)# authentication port-control auto
- S1 (config-if)# dot1x pae authenticator
- S1 (config-if)# end
- S1#

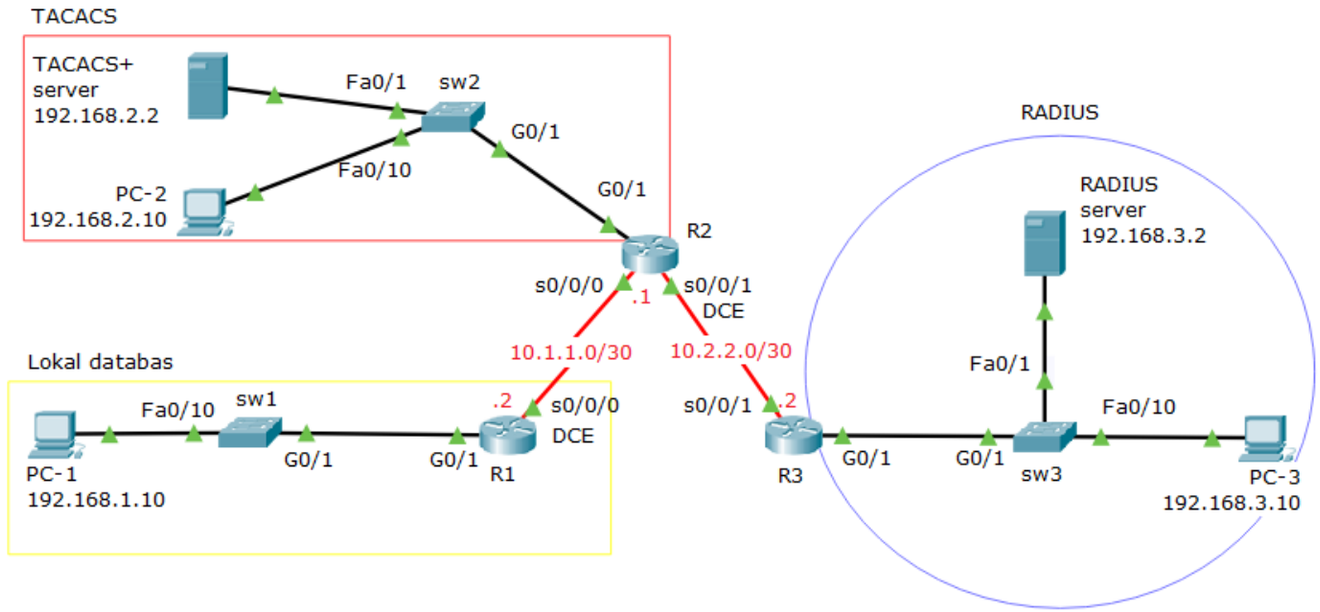



```
S1(config)# aaa new-model
S1(config)# radius server CCNAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```

AAA – Implementation

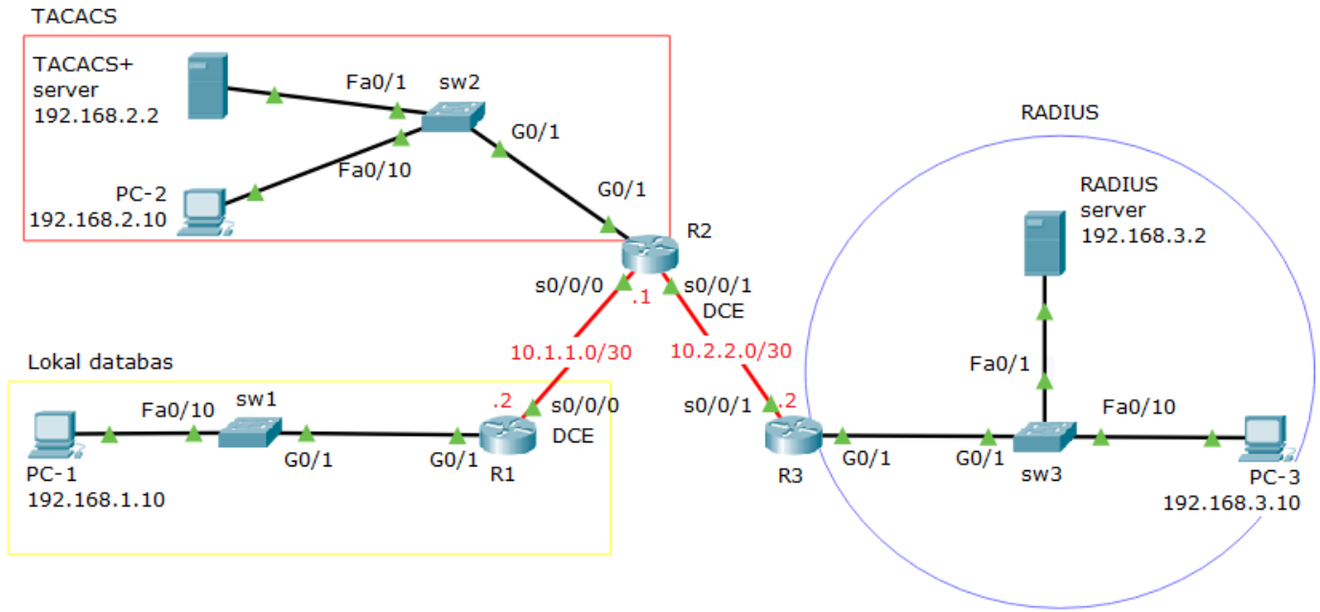
AAA autentiseringssätt

- R1(config)# interface g0/1
- R1(config-if)# ip address 192.168.1.1 255.255.255.0
- R1(config-if)# no shut
- R1(config)# interface s0/0/0
- R1(config-if)# ip address 10.1.1.2 255.255.255.252
- R1(config-if)# clock rate 64000
- R1(config-if)# no shut
- R1(config-if)# end



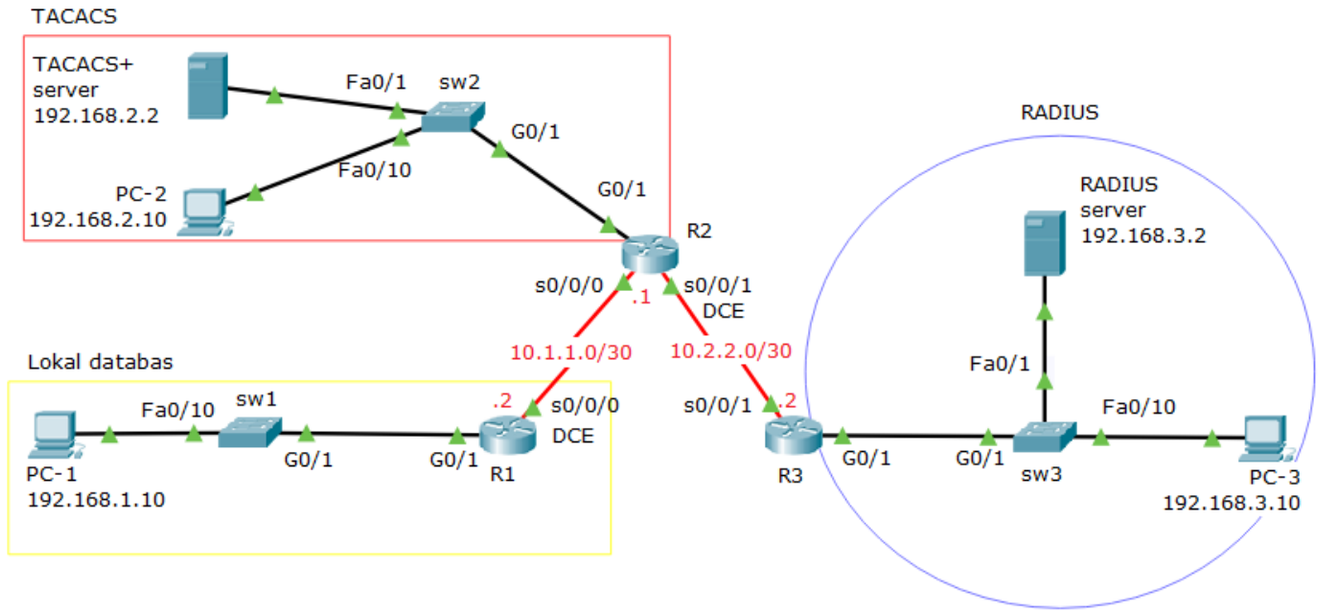
AAA autentiseringssätt

- R2(config)# interface g0/1
- R2(config-if)# ip address 192.168.2.1 255.255.255.0
- R2(config-if)# no shut
- R2(config-if)# interface s0/0/0
- R2(config-if)# ip address 10.1.1.1 255.255.255.252
- R2(config-if)# no shut
- R2(config-if)# interface s0/0/1
- R2(config-if)# ip address 10.2.2.1 255.255.255.252
- R2(config-if)# clock rate 64000
- R2(config-if)# no shut
- R2(config-if)# end



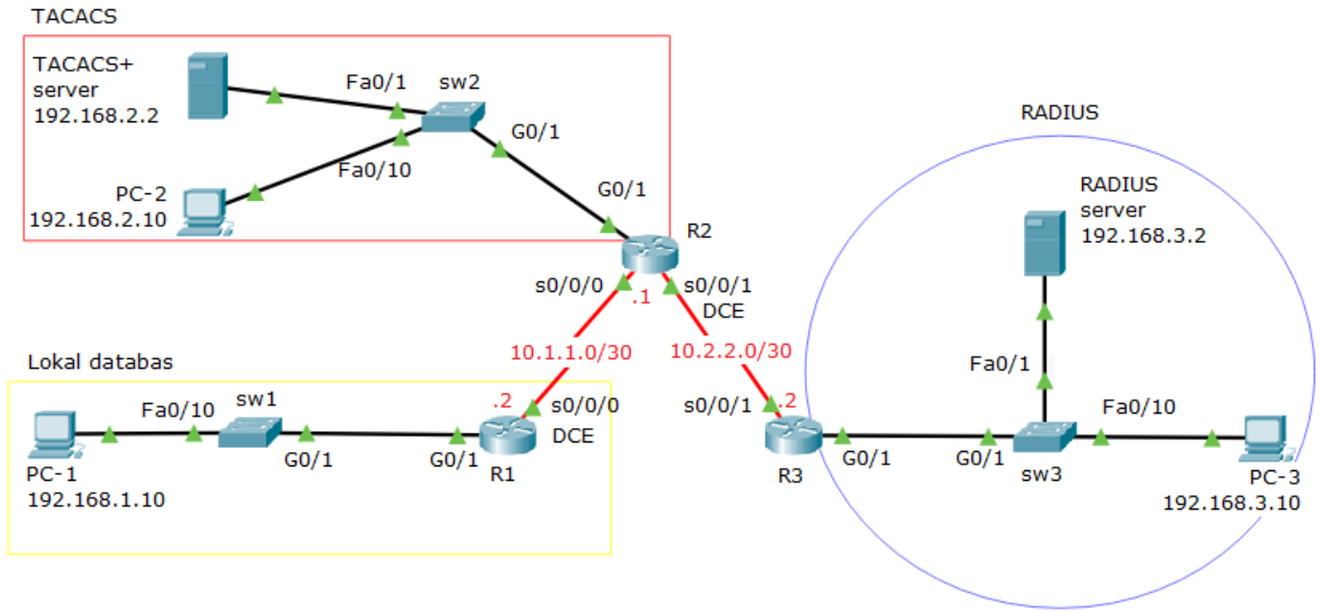
AAA autentiseringssätt

- R3(config)# interface g0/1
- R3(config-if)# ip address 192.168.3.1 255.255.255.0
- R3(config-if)# no shut
- R3(config-if)# exit
- R3(config)# interface s0/0/1
- R3(config-if)# ip address 10.2.2.2 255.255.255.252
- R3(config-if)# no shut
- R3(config-if)# end



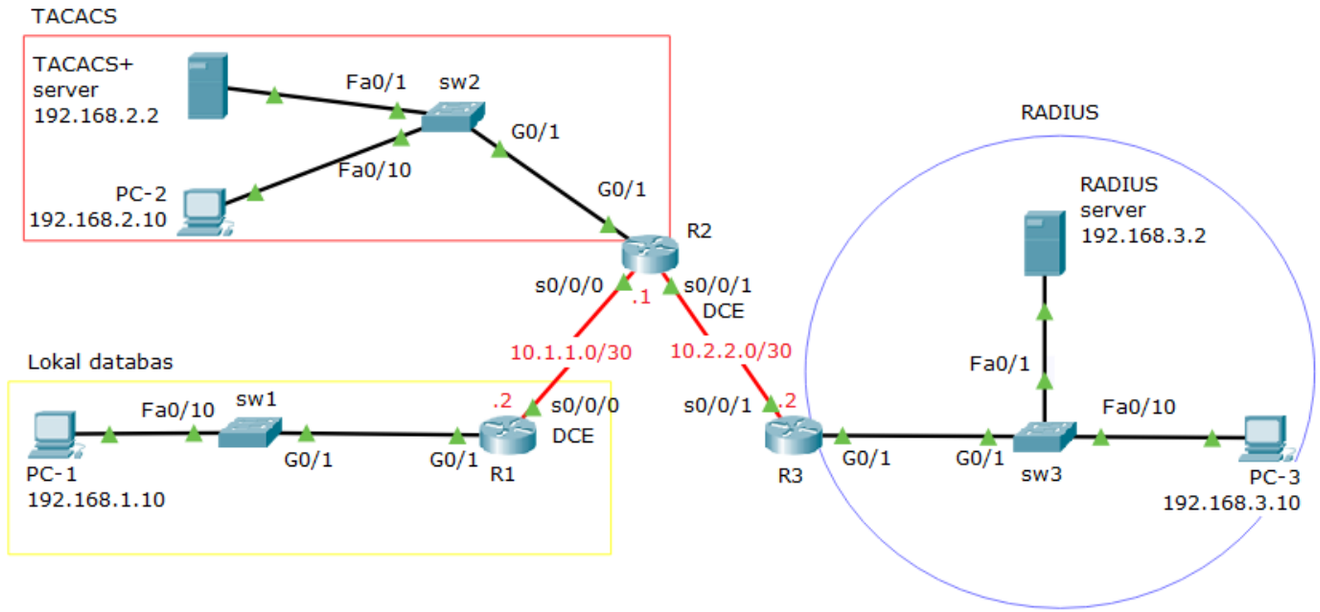
AAA autentiseringssätt

- R1(config)# router eigrp 1
- R1(config-router)# no auto-summary
- R1(config-router)# network 192.168.1.0 0.0.0.255
- R1(config-router)# network 10.1.1.0 0.0.0.3
- R1(config-router)# end



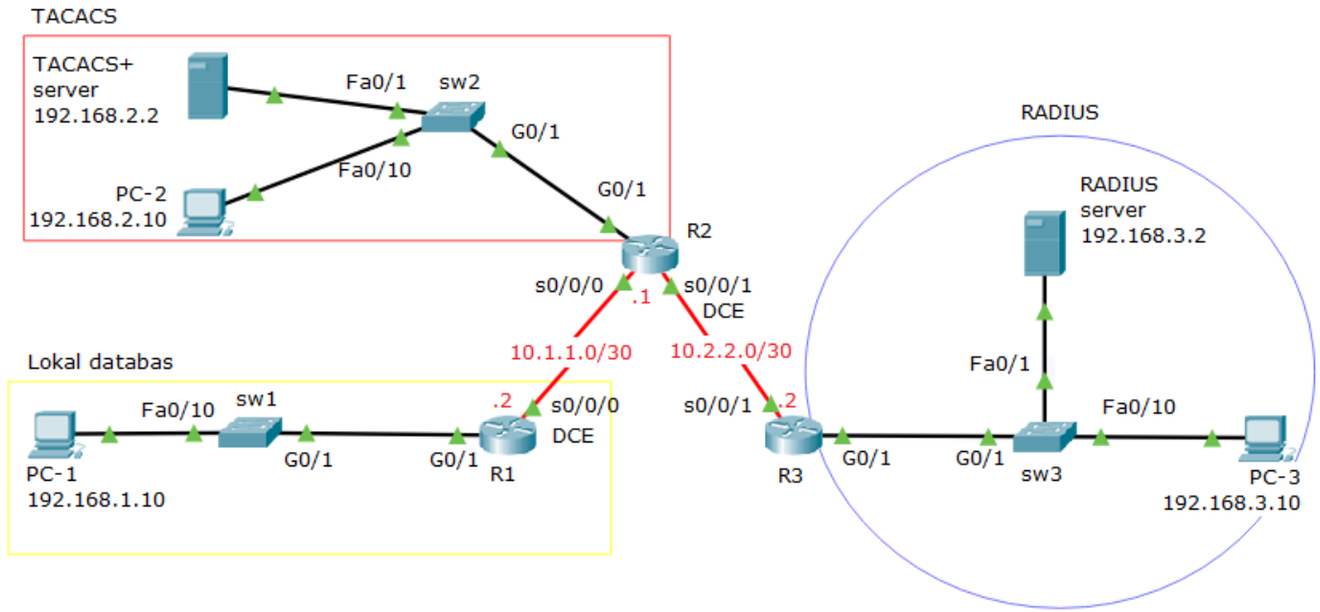
AAA autentiseringssätt

- R2(config)# router eigrp 1
- R2(config-router)# no auto-summary
- R2(config-router)# network 192.168.2.0 0.0.0.255
- R2(config-router)# network 10.1.1.0 0.0.0.3
- R2(config-router)# network 10.2.2.0 0.0.0.3
- R2(config-router)# end



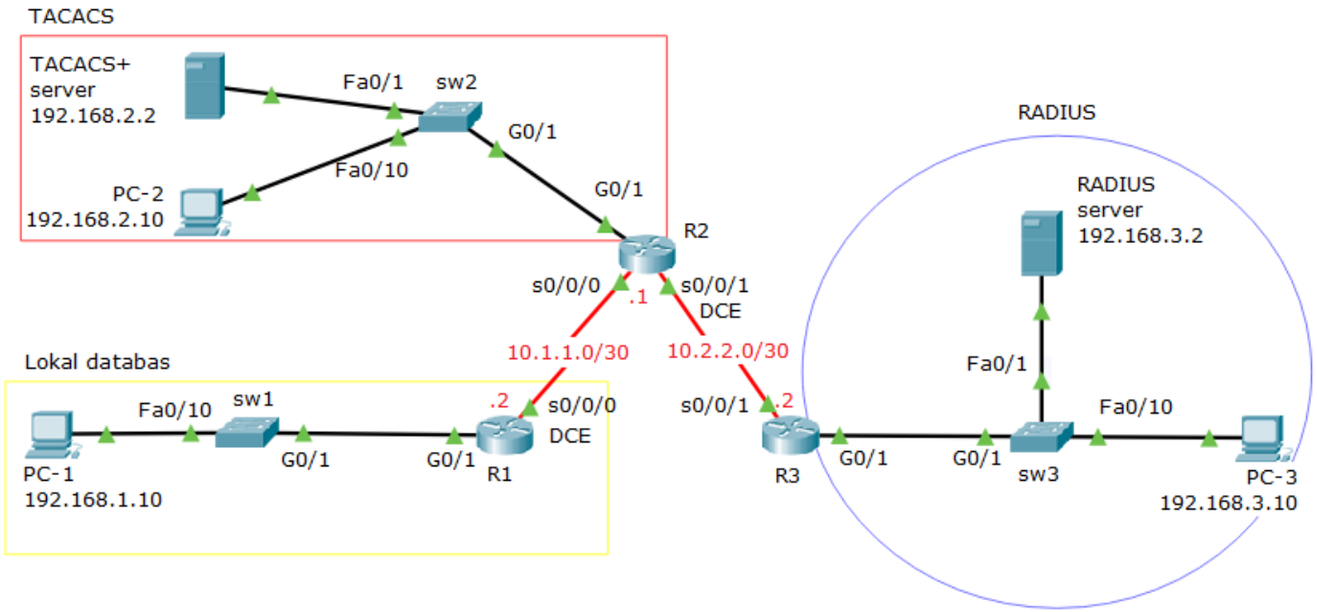
AAA autentiseringssätt

- R3(config)# router eigrp 1
- R3(config-router)# no auto-summary
- R3(config-router)# network 192.168.3.0 0.0.0.255
- R3(config-router)# network 10.2.2.0 0.0.0.3
- R3(config-router)# end



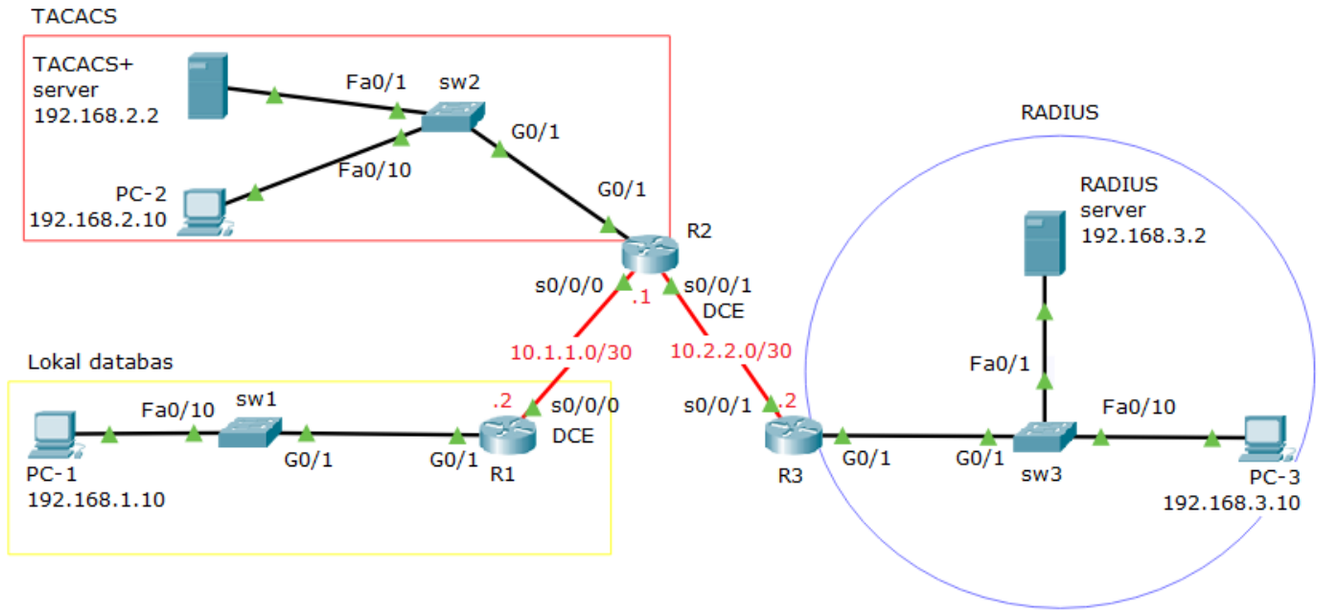
AAA autentiseringssätt - lokalt

- R1(config)# enable secret enpass
- R1(config)# username Admin1 secret admin1pass
- R1(config)# aaa new-model
- R1(config)# aaa authentication login default local
- R1(config)# line console 0
- R1(config-line)# login authentication default
- R1(config-line)# end
- Testa konsolåtkomst
- R1# exit
- Username: Admin1
- Password: admin1pass
- R1>



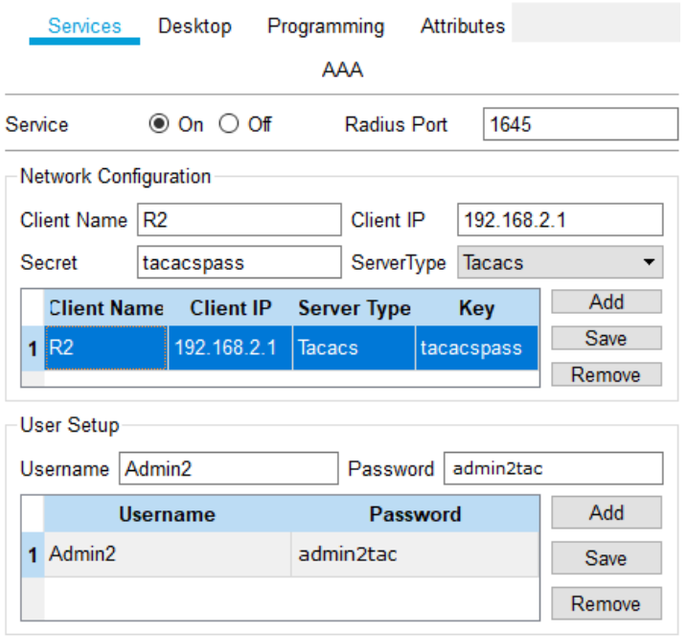
AAA autentiseringssätt – Lokalt VTY via SSH

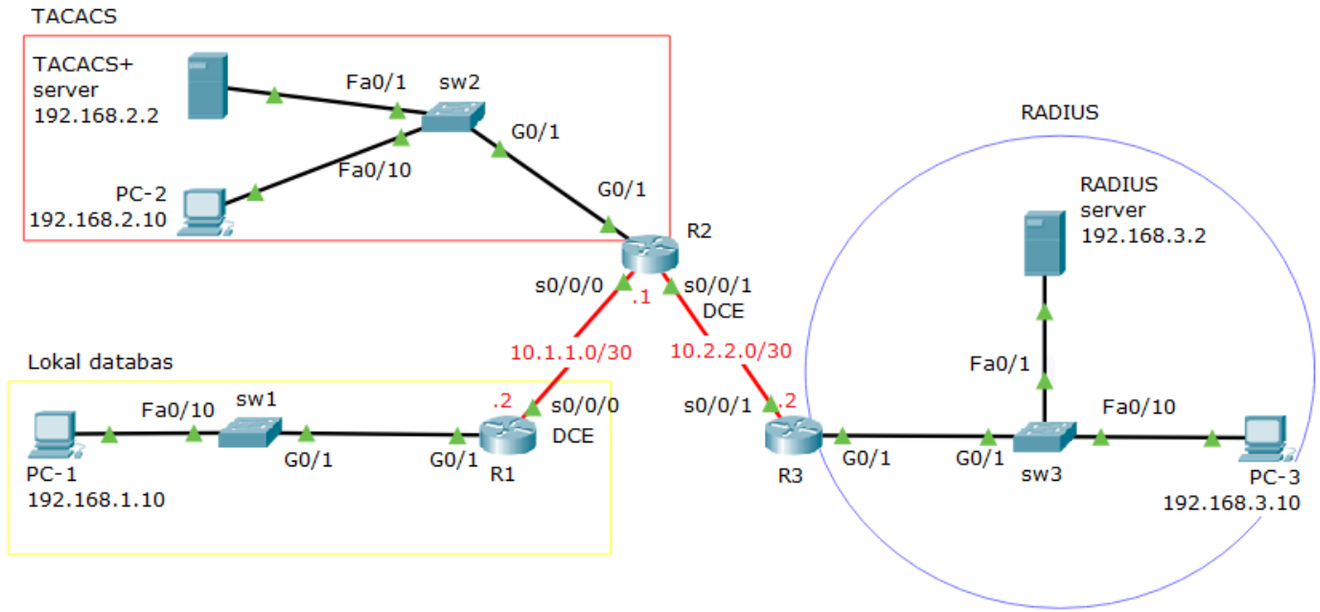
- R1(config)# ip domain-name diginto.se
- R1(config)# crypto key generate rsa
  How many bits in the modulus [512]: 1024
- R1(config)# aaa authentication login SSH-LOGIN local
- R1(config)# line vty 0 4
- R1(config-line)# login authentication SSH-LOGIN
- R1(config-line)# transport input ssh
- R1(config-line)# end
- R1#



AAA autentiseringssätt – TACACS+ och lokalt

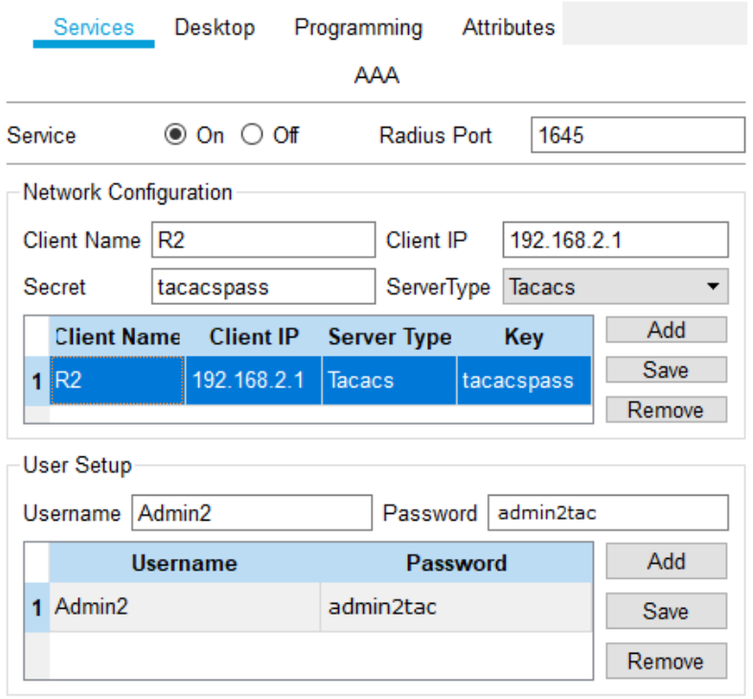
- R2(config)# username Admin2 secret admin2pass
- R2(config)# tacacs-server host 192.168.2.2 key tacacspass
- R2(config)# aaa new-model
- R2(config)# aaa authentication login default group tacacs+ local
- R2(config)# line console 0
- R2(config-line)# login authentication default
- R2(config-line)# end

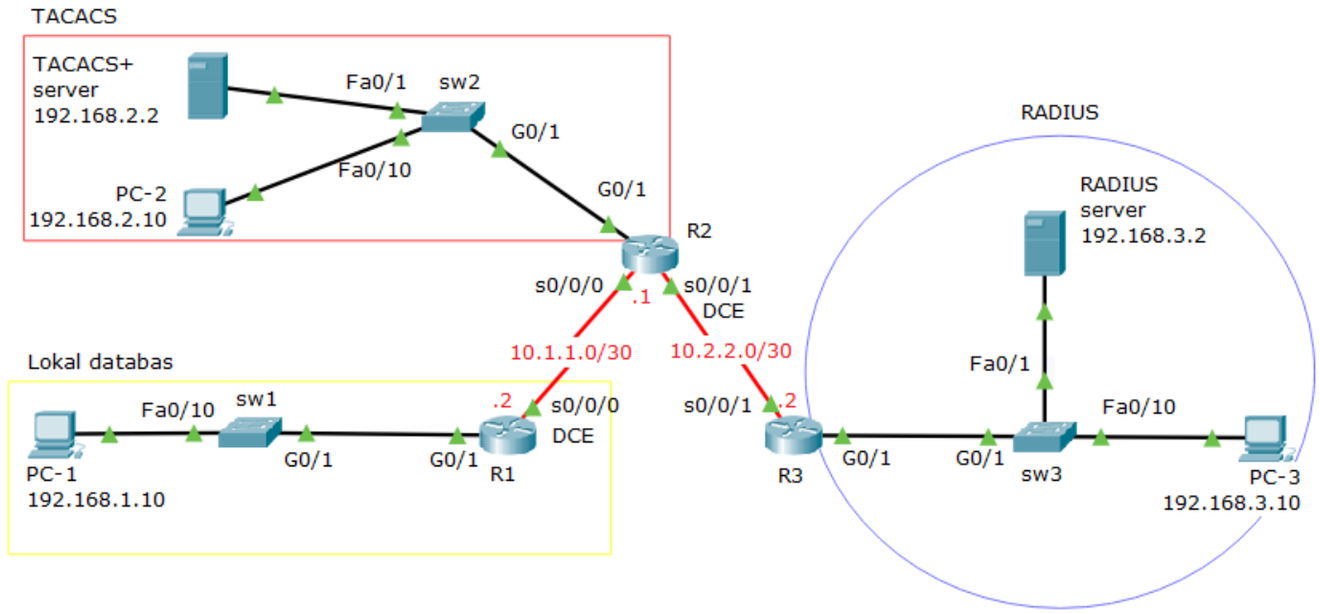




AAA autentiseringssätt – VTY via SSH

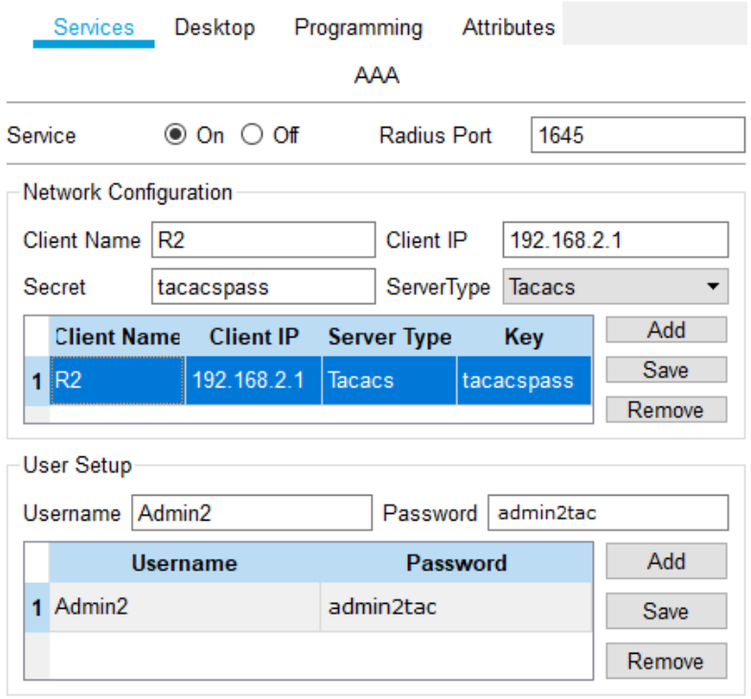
- R2(config)# ip domain-name diginto.se
- R2(config)# crypto key generate rsa
  How many bits in the modulus [512]: 1024
- R2(config)# line vty 0 4
- R2(config-line)# login authentication default
- R2(config-line)# transport input ssh
- R2(config-line)# end

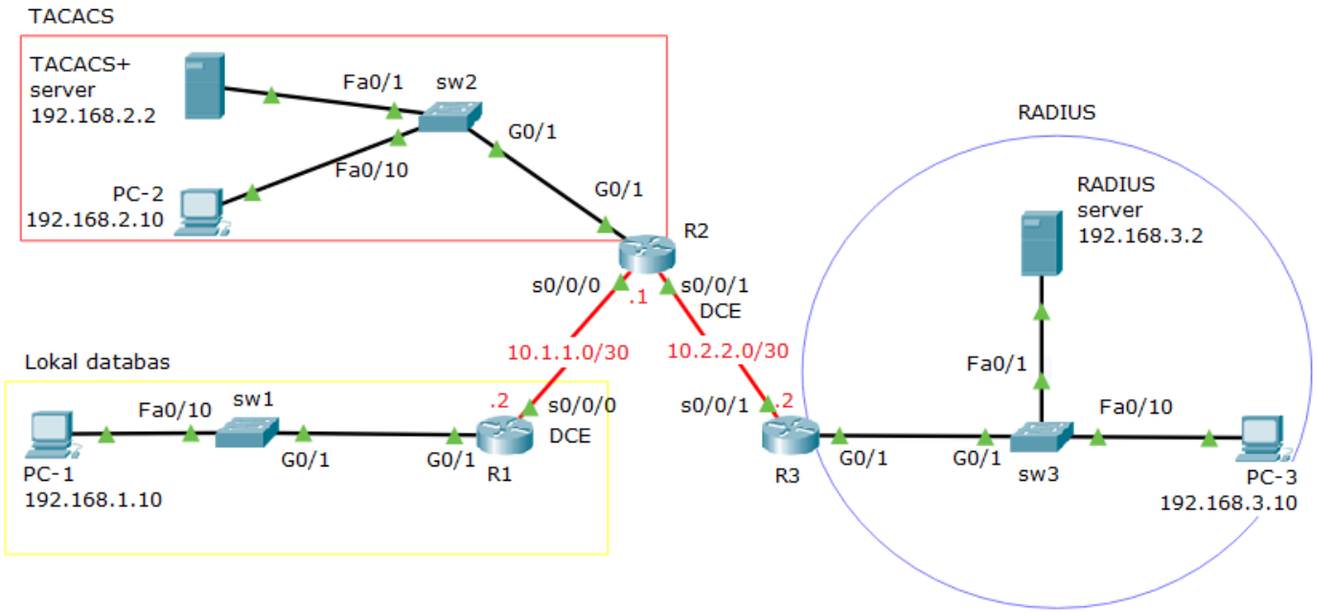




AAA autentiseringssätt - VTY via SSH

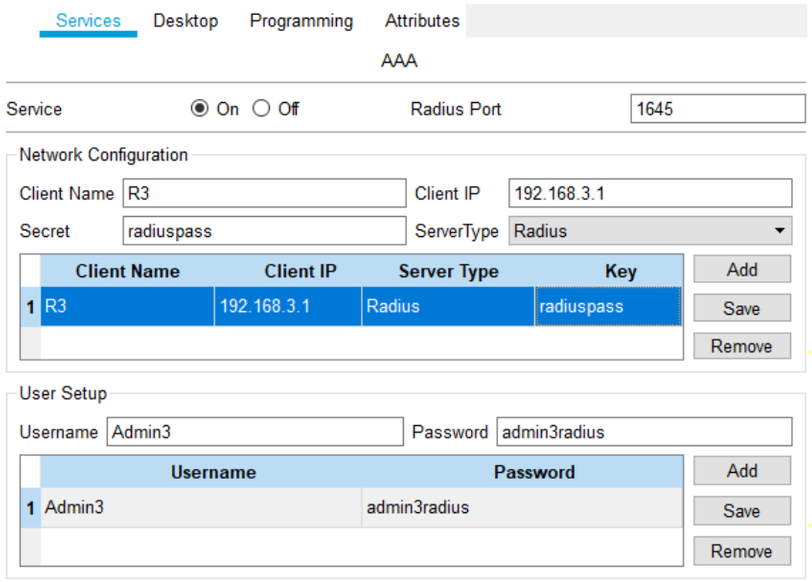
- **Verifiera SSH anslutning från PC2**
- PC> ssh -l Admin1 192.168.2.1; Password: admin2pass
- Konfigurera TACACS-servern
  Client Name: R2 - Client IP 192.168.2.1
  Secret: tacacspass - ServerType: Tacacs
  Username: Admin2 - Password: admin2pass (fel på bilden)
- **Verifiera konsolåtkomsten**
  Username: Admin2; Password: admin2pass

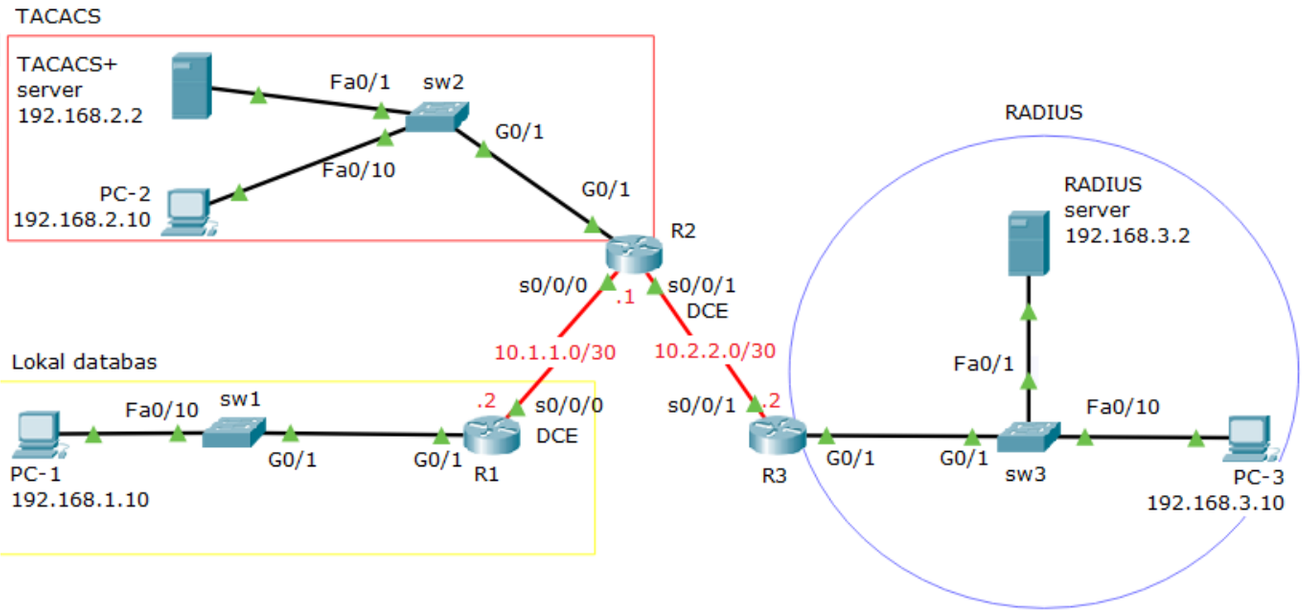




AAA autentiseringssätt - RADIUS

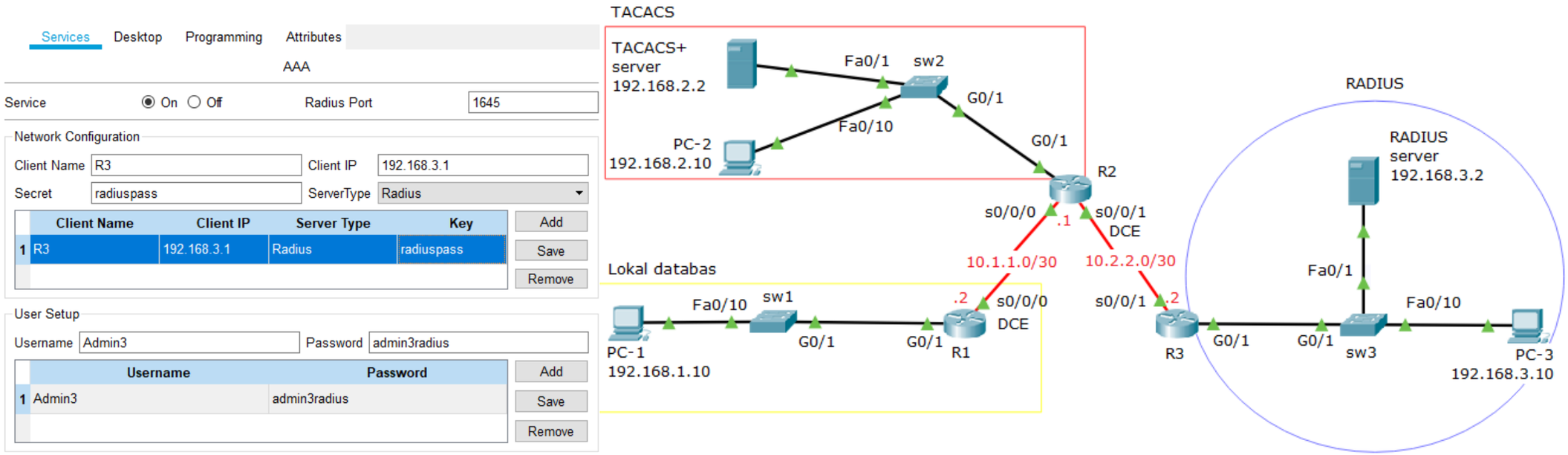
- R3(config)# username Admin3 secret admin3pass
- R3(config)# radius-server host 192.168.3.2
- R3(config)# radius-server key radiuspass
- R3(config)# aaa new-model
- R3(config)# aaa authentication login default group radius local
- R3(config)# line console 0
- R3(config-line)# login authentication default
- R3(config-line)# exit





AAA autentiseringssätt – VTY via SSH

- R3(config)# ip domain-name diginto.se
- R3(config)# crypto key generate rsa
  How many bits in the modulus [512]: 1024
- R3(config)# line vty 0 4
- R3(config-line)# login authentication default
- R3(config-line)# transport input ssh
- R3(config-line)# end



AAA autentiseringssätt – VTY via SSH

- **Verifiera SSH anslutning från PC-A**
  PC3>ssh -l Admin1 192.168.2.1
  Password: admin3pass
- Konfigurera RADIUS-servern
  Client Name: R3 - Client IP 192.168.3.1
  Secret: radiuspass- ServerType: radius
  Username: Admin3 - Password: admin3pass (fel på bilden)
- **Verifiera konsolåtkomsten**
  Username: Admin3
  Password: admin3pass
  R3>
- Verifiera att användare exekveringsläge använder AAA RADIUS servern
- R3# exit
  Username: Admin3
  Password: admin3pass
  R3>


DIGINTO
Nätverkssäkerhet