Tampereen ammattikorkeakoulu

RADIUS autentikointi Ciscon verkkolaitteille

Ville Koivisto

OPINNÄYTETYÖ
Toukokuu 2021

Tieto- ja viestintätekniikka
Tietoverkot ja tietoliikennetekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoverkot ja tietoliikennetekniikka

KOIVISTO, VILLE:
RADIUS-autentikointi Ciscon verkkolaitteille

Opinnäytetyö 22 sivua, joista liitteitä 24 sivua
Toukokuu 2021

Opinnäytetyö tehtiin Triuvare Oy:lle tarkoituksena kehittää ratkaisu, jolla voidaan keskittää käyttäjien hallinta. Keskitetty käyttäjien hallinta parantaa tietoturvaa, sillä kaikkia tunnuksia pystytään hallinnoimaan yhdestä paikasta. Keskitettyjä käyttäjätunnuksia voidaan tämän opinnäytetyön mukaisesti käyttää esimerkiksi verkkolaitteille kirjautumiseen. Tässä työssä käyttäjien hallinta toteutetaan RADIUS-protokollan avulla Cisco-verkkolaitteille.

Opinnäytetyössä muutokset tehtiin valmiiseen testiympäristöön, jossa oli yksi Cisco-kytkin, Cisco-palomuuri ja Windows-palvelin. Testiympäristöllä oli tarkoitus simuloida tilannetta, jossa verkkolaitteet ovat asiakkaan tiloissa ja palvelin Triuvaren toimistolla. Palvelimelle asennettiin Network Policy Server, joka toimi RADIUS-palvelimena ja jonka pääsyoikeuksia voidaan hallita Windowsin käyttäjäryhmillä.

RADIUS-autentikointi toimii verkkolaitteilla hyvin, ja vikatilanteiden varalta verkkolaitteilla on paikalliset hallintatunnukset, joilla pääsee kirjautumaan, mikäli RADIUS-palvelin ei syystä tai toisesta ole saatavilla. Jatkossa RADIUS-autentikointiin voidaan lisätä vielä kaksivaiheinen tunnistautuminen parantamaan tietoturvaa entisestään.

Asiasanat: RADIUS, autentikointi, Cisco

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecomminications and Networks

KOIVISTO, VILLE:
RADIUS Authentication for Cisco Network Devices

Bachelor's thesis 22 pages, appendices 24 pages
May 2021

This thesis study was carried out for Triuvare Oy to find a solution for centralized user management. Centralized user management increases data security because every user account can be managed from one place. Centralized user management can be used for example on network devices explored in this study. In this thesis user management was created for Cisco network devices using the RADIUS protocol.

In this thesis changes were made in the already configured test environment, which includes one Cisco switch, one Cisco firewall and a Windows server. The purpose of the test environment was to simulate the real environment, where the network devices are located at the customer’s premises and the server is located at Triuvare’s office. The Network Policy Server was installed on the Windows server, which worked as a RADIUS server and access rights could be managed with Windows user groups.

RADIUS authentication on network devices works well and there is a local account for logging in if RADIUS authentication could not be used for one reason or another. In the future two-factor authentication can be added to RADIUS authentication.

Key words: RADIUS, authentication, Cisco

SISÄLLYS

TERMIT

AAA	Lyhenne sanoista Authentication, Authorization ja Accounting
EAP	Extensible Authentication Protocol, yleisesti RADIUS-autentikoinnissa käytössä oleva autentikointi- protokolla.
LDAP	Lightwight Directory Access Protocol, verkkoprotokolla, joka on tarkoitettu hakemistopalveluihin.
NAS	Network Access Server, välittää RADIUS-viestit käyttäjän laitteelta palvelimelle.
NPS	Network Policy Server, Windows ohjelma, jota voidaan käyttää RADIUS-palvelimena.
PAP	Password Authentication Protocol, salasanapohjainen autentikointi- protokolla.
PEAP	Protected Extensible Authentication Protocol, autentikointiprotokolla, joka kuljettaa tunnistetiedot TLS salattuna.
RADIUS	Remote Authentication Dial In User Service, autentikointi- protokolla.
SPAP	Shiva Password Authentication Protocol, Shiva nimisen yrityksen luoma parannettu versio PAP- protokollasta
SQL	Structured Query Language, IBM:n kehittämä kyselykieli, jota käytetään tietokannoissa.

1 JOHDANTO

Tämä työ käsittelee RADIUS autentikoinnin käyttöönottoa komentoriviltä hallittaville Ciscon verkkolaitteille. Työ toteutettiin toimeksiantona Tamperelaiselle Triuvare Oy:lle, joka tuottaa IT- asiantuntijapalveluita pääasiassa yrityksille. Työ tehtiin valmiiseen testiympäristöön, joka vastaa lopullista käyttöönotto ympäristöä. Ympäristö koostuu Cisco ASA-palomuureista, sekä Cisco SG-sarjan kytkimistä.

Työn tavoitteena on kehittää ratkaisu, jolla saadaan käyttöön keskitetty käyttäjien hallinta. Keskitetty käyttäjänhallinta poistaa tarpeen mahdollisille yleisesti tiedossa oleville käyttäjätunnuksille ja siten parantaa järjestelmien tietoturvaa. Käyttäjätunnusten hallinta on tarkoitus toteuttaa RADIUS-protokollan avulla, jolloin Windows Server Palvelimelle määritetty Network Policy Server toimii RADIUS-palvelimena. Vikatilanteissa voitaisiin käyttää paikallisia käyttäjätunnuksia, jotta pääsy laitteille ei estyisi.

Työ toteutettiin valmiiseen testiympäristöön, jossa Windows palvelin ja verkkolaitteet olivat määritetty toimintavalmiiksi. Windows palvelimelle asennettiin Network Policy server, sekä määritettiin RADIUS-protokollaa varten tarvittavat asetukset. Myös verkkolaitteille tehtiin oikeanlaiset määritykset RADIUS-autentikointia varten ja varmistettiin, että kirjautuminen palvelimella olevilla tunnuksilla on mahdollista ja, että kirjautuminen on mahdollista myös, jos RADIUS-palvelimeen ei saada yhteyttä.

2 YLEISTÄ TIETOVERKOISTA

Tänä päivänä tietoverkkojen merkitys liiketoiminnassa on hyvin merkittävä, sillä suurin osa työstä tehdään verkon kautta ja internet on yritysmaailmassa käytännössä välttämätön. Epävakaa tai vikaherkkä tietoverkko voi helposti rajoittaa liiketoimintaa tai pahimmassa tapauksessa jopa keskeyttää sen. Myös hidas verkkoyhteys suuressa yrityksessä aiheuttaa työn keskeytymistä, sekä pahimmassa tapauksessa vie työtunteja pois.

2.1 Verkkojen tietoturva

Tietoverkkojen täytyy olla tietoturvallisia, koska yritystoiminnassa verkon ylitse siirretty data pitää pysyä muuttumattomana, sekä koskemattomana. Tällä taataan, että esimerkiksi liikesalaisuuksia tai asiakastietoja ei päädy vääriin käsiin. Verkko on luotettavampi ja vakaampi, kun tietoturva on kunnossa, eikä ulkopuoliset hyökkäykset vaikuta siihen niin suurella todennäköisyydellä, kuin tietoturvaltaan heikkoon verkkoon. Verkon tietoturva sisältää paljon muutakin, kuin laitteita ja salasanoja. Myös käyttäjillä on vastuuta, jotta tietoturva pysyy halutulla tasolla.

2.1.1 Fyysinen tietoturva

Verkkojen tietototurvaan liittyy myös fyysinen tietoturva. Fyysisiä verkon suojaamistoimenpiteitä voi olla esimerkiksi ulkopuolisten laitteiden kytkemisen estäminen verkkoon tai palvelintiloihin pääsyn rajaaminen. Myös varkauksien ja tulipalojen ehkäisy kuuluu fyysiseen tietoturvaan. Nykyaikaisilla etähallittavilla sähkölukoilla voidaan parantaa fyysistä tietoturvaa, sillä kadonneet avaimet voi tehdä helposti käyttökelvottomiksi. (Halonen 2021).

2.1.2 Järjestelmien tietoturva

Järjestelmien tietoturva on myös tärkeä osa tietoturvallista tietoverkkoa. Varsinkin järjestelmät ja laitteet, jolla pääsee hallinnoimaan verkon toimintaa ja siellä kulkeva data, täytyisi olla hyvin suojattu, esimerkiksi vahvoin salasanoin, sekä järjestelmät tulisi pitää ajan tasalla. Myös oikeanlaisella konfiguraatiolla on suuri merkitys, jotta laitteisiin ei jää aukinaisia reittejä päästä tietoihin käsiksi. Verkkolaitteilla kannattaa olla myös valvontaa, koska silloin pystytään reagoimaan epätavallisiin tapahtumiin pienemmällä viiveellä, mikäli hyökkäykset tai muut tunkeutumiset havaitaan ajoissa, voidaan pahin mahdollisesti estää tapahtumasta. Lisäksi toimintavarmuus säilyy, kun viat saadaan heti selville.

2.1.3 Hallinnollinen tietoturva

Hallinnollinen tietoturva parantaa tietoturvaa siten, että tietoturva osataan kohdentaa oikeisiin asioihin. Organisaatioissa saattaa olla erilaisia sääntöjä tietoturvan osalta, joilla voidaan sitouttaa työntekijöitä toimimaan tietoturvallisesti. Myös ennalta määritetyt toimintatavat ja prosessit parantavat tietoturvaa, sillä ne vähentävät inhimillisiä virheitä. Ennalta määritettyjä prosesseja ja toimintatapoja voidaan parantaa koulutuksilla ja yhteisillä pelisäännöillä. Yrityksen henkilöstö voi omalla toiminnallaan estää mahdollisia tietoturvauhkia, esimerkiksi siten, että ei päästä tuntemattomia henkilöitä lukituista ovista. Monissa yrityksissä myös testataan henkilöstön toimintaa tietoturvaan liittyen, kuten lähettämällä sähköpostia, joka voisi olla todellisessa tilanteessa olla harmillinen. Tai vaihtoehtoisesti kokeillaan päästä sisään tiloihin, ilman kulkuoikeuksia mahdollisesti tikkaiden tai muiden välineiden kanssa naamioituneena. (Hallinnollinen tietoturva – Mitä se on? n.d.).

3 RADIUS

RADIUS on lyhenne sanoista Remote Authentication Dial In User Service. RADIUS-autentikointi on nykyisin käytössä lähes jokaisessa suuremmassa ympäristössä, jossa on käytössä työasemien keskitetty käyttäjänhallinta. Tämä mahdollistaa uusien käyttäjien luomisen joustavammin, sekä antaa järjestelmänvalvojille mahdollisuuden vaihtaa käyttäjien salasanan tai hallita oikeuksia.

3.1 Yleistä RADIUS-protokollasta

RADIUS on vuodesta 1987 lähtien kehitetty yleisimmin sisäänsoittopalveluissa käytetty protokolla, joka mahdollistaa keskitetyn käyttäjänhallinnan ja käytön tilastoinnin. (Lujan 2018).

3.2 AAA

Vaikka RADIUS luotiin ennen AAA protokollaa, niin sen toiminta on hyvin samankaltaista. Lyhenne AAA tulee sanoista authentication, authorization ja accounting, jotka ovat suomeksi samassa järjestyksessä todennus, valtuutus ja tilastointi. (Hassell 2003).

3.2.1 Authentication

Autentikointi eli todennus on vaihe, jossa käyttäjän tai laitteen identiteetti todennetaan. Yleisemmin käytössä on käyttäjätunnus ja salasana yhdistelmä, jotka käyttäjä syöttää kirjautuessaan palveluihin. Nykyisin salasanojen leviäminen aiheuttaa tavallisen salasana todennuksen heikentymisen, mutta salasanan ja digitaalisen sertifikaatin avulla voidaan lisätä todennuksen varmuutta. (Hassell 2003).

3.2.2 Authorization

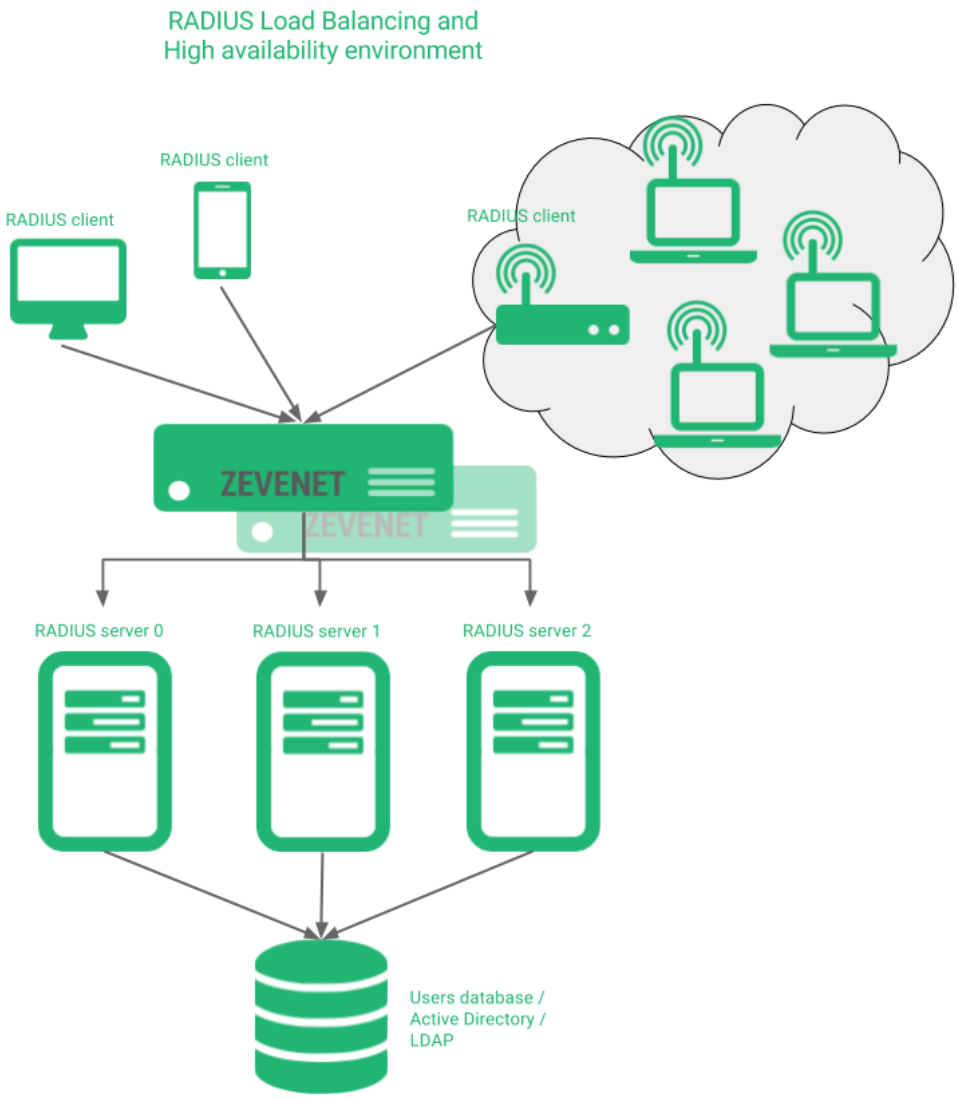
Authorization eli valtuutus vaiheessa määritellään, että mihin todennetulla käyttäjällä on oikeus. Oikeudet määrittää järjestelmänvalvoja. Määritettyjä oikeuksia voi olla esimerkiksi verkkoon pääsyn rajaaminen tai käytettävissä olevien resurssien määritys. (Hassell 2003).

3.2.3 Accounting

Accounting eli tilastointi kerää tietoa käyttäjästä ja sen käyttämistä resursseista. Tässä vaiheessa kerätään käyttäjästä ainakin aika, jolloin palveluun kirjauduttiin ja milloin yhteys katkaistiin. Lisäksi istunnosta jää tietoa datan määrästä ja jälki, että mitä dataa on lähetetty tai vastaanotettu. Näillä tiedoilla palveluntarjoaja pystyy tarvittaessa laskuttamaan käyttäjää käytetyn ajan mukaan tai tarkastelemaan palvelun käyttöastetta. (Hassell 2003).

3.3 RADIUS komponentit

Radius koostuu tyypillisesti neljästä eri komponentista, jotka ovat käyttäjä tai laite, Network Access Server (NAS), Radius-palvelin ja tietokanta. Kuvassa 1 nähdään, että miten eri komponentin sijoittuvat tyypillisessä RADIUS-ympäristössä. Suuremmissa ympäristöissä kuormaa voidaan jakaa useammalle laitteelle, joka varmistaa oikean toiminnan myös vikatilanteessa, jos jokin yksittäinen laite lakkaa toimimasta.



KUVA 1. Esimerkki RADIUS-ympäristöstä, jossa on kolme RADIUS-palvelinta jakamassa kuormaa. (Zevenet 2017).

3.3.1 Käyttäjä / Laite

Tunnistautumista pyytävä laite tai käyttäjä. Kun käyttäjää pyydetään syöttämään käyttäjätunnus ja salasana, niin se lähetetään NAS-liityntäpisteelle. (FreeRADIUS Documentation n.d.).

3.3.2 Network Access Server

Network Access Server on yleisesti laite, joka vastaanottaa tunnistautumispyynnöt ja välittää ne eteenpäin RADIUS-palvelimelle. NAS-liityntäpiste voi olla esimerkiksi kytkin tai langattoman verkon tukiasema. (FreeRADIUS Documentation n.d.).

3.3.3 RADIUS-palvelin

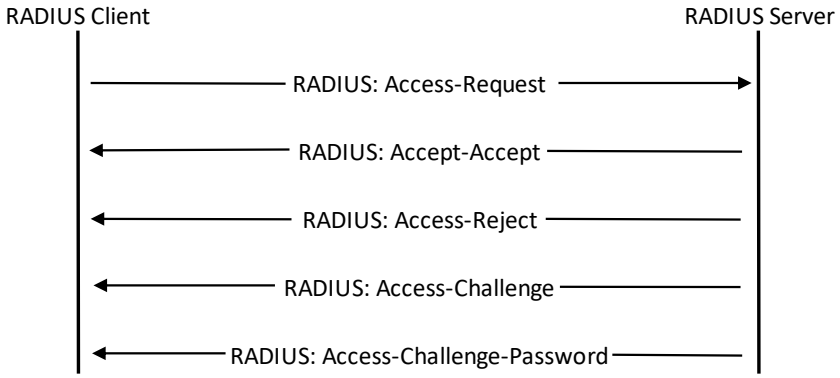
Radius-palvelin on yleensä ohjelma, joka vastaanottaa NAS-liityntäpisteen lähettämät tunnistautumispyynnöt ja vastaa valtuutustiedot NAS-liityntäpisteelle. RADIUS-palvelin saa myös tilastointidataa NAS-liityntäpisteeltä. RADIUS-palvelin on usein Windows-ympäristössä Microsoftin Network Policy Server, joka on Windows Server-ympäristössä valmiina. RADIUS-palvelimelle on myös paljon avoimen lähdekoodin vaihtoehtoja. (FreeRADIUS Documentation n.d.).

3.3.4 Tietokanta

Tietokanta on järjestelmä, jossa käyttäjätiedot säilötään. RADIUS-palvelin pyytää käyttäjätietoja tietokannalta, sekä tallentaa sinne tilastodataa. Tietokanta voi olla esimerkiksi SQL-tietokanta tai LDAP-hakemisto. (FreeRADIUS Documentation n.d.).

3.4 RADIUS-autentikoinnin vaiheet

Kun käyttäjä kirjautuu palveluun, jossa RADIUS autentikointi on käytössä, niin käyttäjältä pyydetään käyttäjätunnus ja salasana. Tunnistetiedot lähetetään verkon ylitse RADIUS-palvelimelle, joka vertaa tunnistetietoja käyttäjähakemiston tietoihin. Palvelin vastaa pyyntöön yhdellä neljästä vaihtoehdosta (kuvio 1), jotka ovat ACCEPT, REJECT, CHALLENGE tai CHALLENGE PASSWORD. (Cisco 2019).



KUVIO 1. RADIUS-autentikoinnin vaiheet käyttäjän ja palvelimen välillä. (Itse tehty)

3.4.1 RADIUS Access-Accept

Accept-vastaus tarkoittaa, että käyttäjä löytyi hakemistosta ja käyttöoikeuksien pyytäminen onnistui ja oikeudet voidaan antaa. Useampi käyttäjä voi kirjautua käyttäen RADIUS tunnistautumista samanaikaisesti vaikuttamatta toisiin käyttäjiin. (How Does RADIUS Authentication Work? 2019).

3.4.2 RADIUS Access-Reject

Reject-vastaus kertoo, että käyttöoikeuksia ei voida myöntää. Tässä vaiheessa käyttäjää saatetaan pyytää syöttämään salasana uudelleen, mikäli ensimmäisellä yrityksellä syötettiin virheellinen salasana. Vaihtoehtoisesti käyttäjän pääsy kyseiseen resurssiin on estetty järjestelmänvalvojan toimesta. (How Does RADIUS Authentication Work? 2019).

3.4.3 RADIUS Access-Challenge

Kun RADIUS-palvelimen vastaus on challenge, niin kirjautuvalta käyttäjältä pyydetään lisää tietoa. Challenge-vastausta voidaan käyttää, jos käytössä on monivaiheinen tunnistautuminen ja käyttäjältä pyydetään esimerkiksi tekstiviestillä lähetettyä koodia. (How Does RADIUS Authentication Work? 2019).

3.4.4 RADIUS Access-Challenge Password

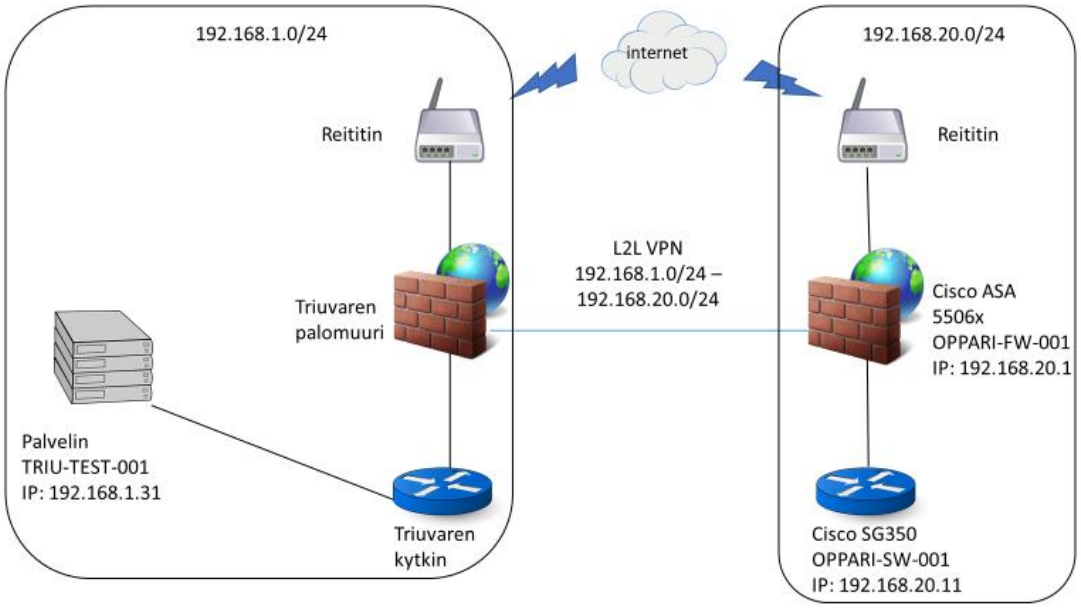
Challenge password vaiheessa käyttäjää pyydetään syöttämään uusi salasana. Vanha salasana voi olla vanhentunut tai käyttäjä on pyytänyt salasanan vaihtoa aiemmin. (Cisco 2019).

4 KÄYTÄNNÖN TOTETUTUS

Työ tehtiin valmiiseen testiympäristöön, jotta oikean ympäristön toiminta saatiin pidettyä turvallisena ja varmistettua sen toiminta.

4.1 Testiympäristö

Testiympäristöön kuuluu Cisco ASA 5506x palomuuri ja Cisco SG350 kytkin, kuvan 2. palomuuri on yhteydessä mobiiliverkkoon, jolla saadaan simuloitua mahdollinen asiakasverkko erilleen Triuvaren omasta verkosta. Palomuurien välillä on L2L VPN tunneli verkkojen 192.168.1.0/24–192.168.20.0/24 välille. Testiympäristössä on valmiina perusmääritykset, joilla verkko toimii. RADIUS-palvelimena toimiva Windows Server asennettiin alustapalvelimelle, sekä verkkolaitteisiin määritettiin RADIUS-toiminto käyttöön.



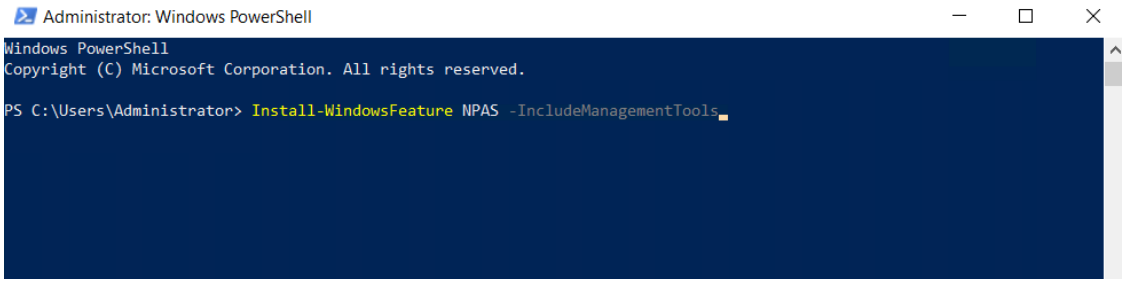
KUVA 2. Työhön käytetty testiympäristö. Vasemman puolen palomuuri ja kytkin kuvaavat Triuvaren ympäristöä ja oikean puolen laitteet kuvaavat asiakkaan ympäristöä.

4.2 Windows Server asennus ja määritys

RADIUS-palvelimena toimiva Windows Server toimii virtuaalipalvelimella. Palvelimelle on asennettu Windows Server 2019 käyttöjärjestelmä, mutta muut määritykset tehtiin sen mukaiseksi, että palvelin toimii RADIUS-palvelimena. Palvelimen IP-osoite on määritetty valmiiksi olemaan 192.168.1.31.

4.2.1 Network Policy Serverin asennus

Network Policy Server voidaan asentaa kahdella eri tavalla. Toinen tavoista on asentaa se Windows Server käyttöjärjestelmässä olevasta Server Manager ohjelmasta tai sitten Powershell-komentoikkunassa. Tässä työssä Network Policy Server asennettiin Powershell-komentoikkunan avulla, kuvassa 3 näkyvällä komennolla.



KUVA 3. Network Policy Serverin asennus Powershell-komentoikkunassa.

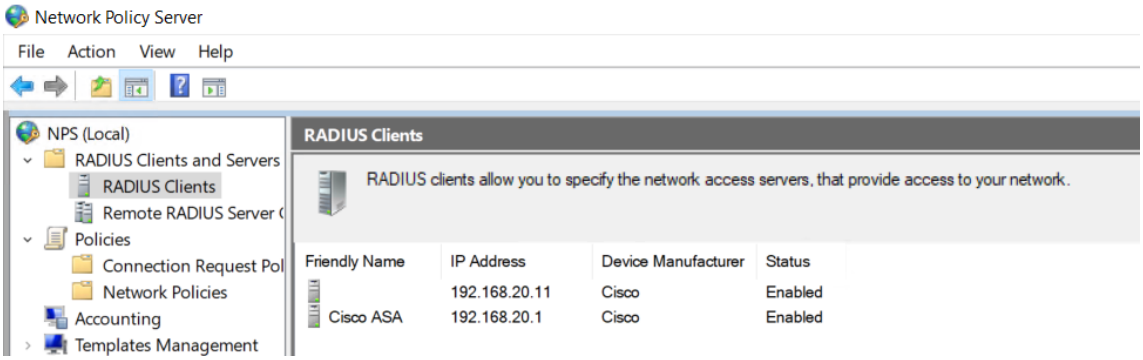
4.3 RADIUS-palvelimen määritys

RADIUS-palvelimena toimii Network Policy Server, joka on saatavilla Windows palvelimiin. Kun Network Policy Server on saatu asennettua, täytyy siihen tehdä tarvittavat määritykset, jotta se toimii halutulla tavalla.

4.3.1 RADIUS Clients

Network Policy Serverin näkymässä vasemmassa reunassa on valikko RADIUS Clients (kuva 4), johon syötetään tiedot laitteista, jotka tunnistautuvat Network

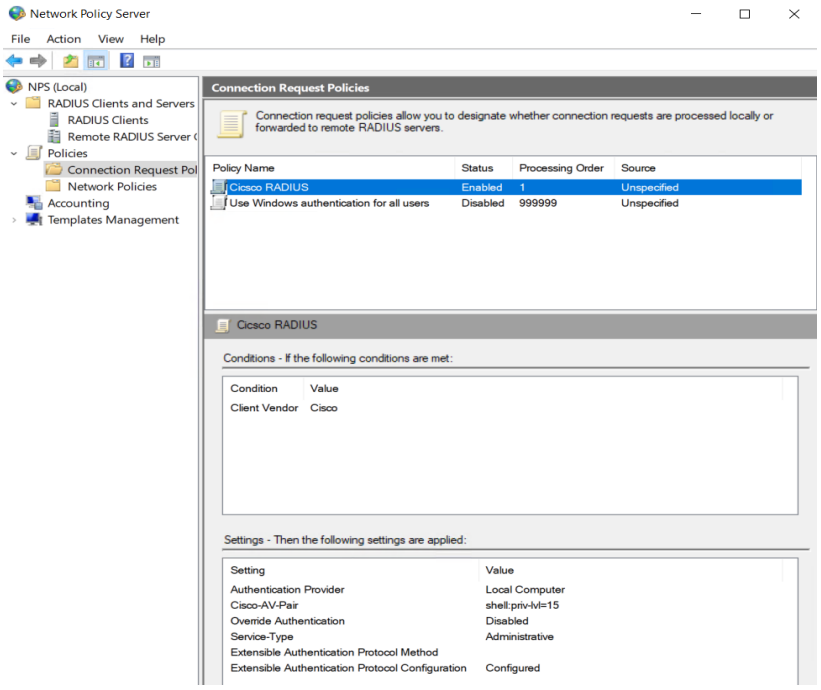
Policy Serverin avulla. Tässä työssä kytkin nimettiin Cisco SG350:ksi ja palomuuri Cisco ASA:ksi. Molemmille laitteille määritettiin IP-osoitteet, jaettu avain sekä laitteen valmistaja.



KUVA 4. Network Policy Serverin RADIUS Clients näkymä

4.3.2 Connection Request Policies

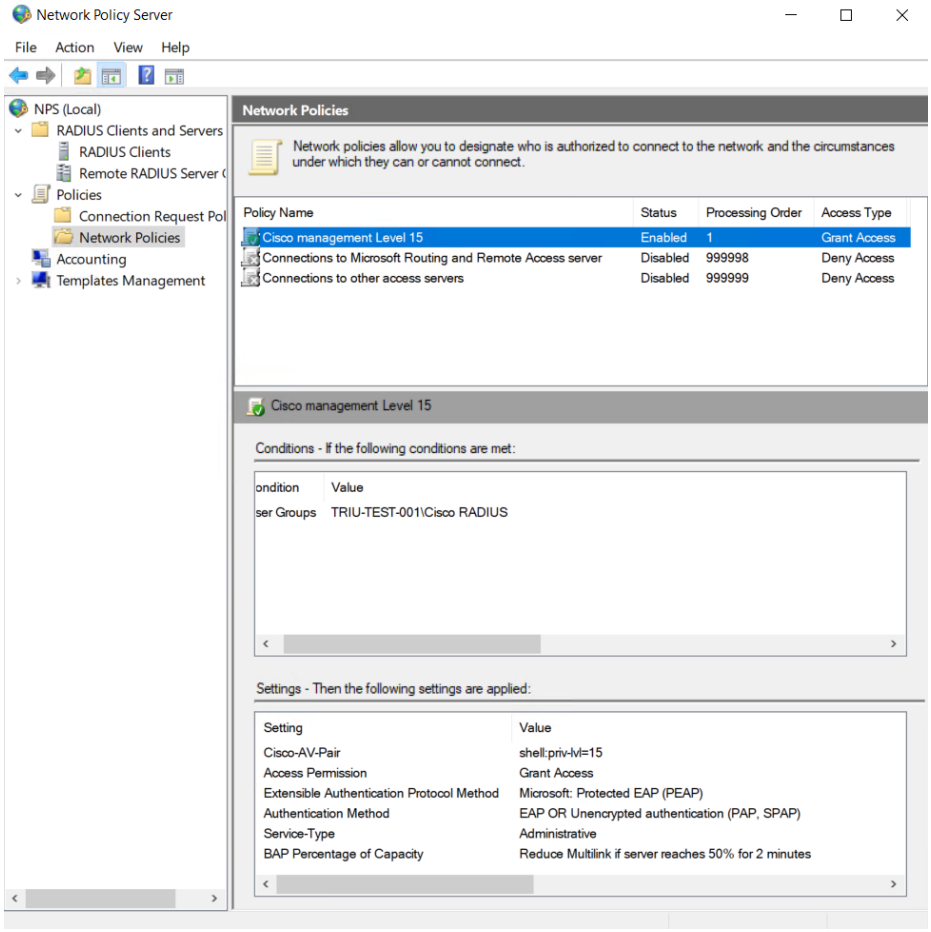
RADIUS laitteiden määrityksen lisäksi täytyy luoda sääntö, jonka mukaan oikeudet annetaan niitä pyytäville laitteille. Kuvassa 5 nähdään luotu sääntö nimellä ”Cisco RADIUS”. Sääntö määrittää, että laitteet, joiden valmistaja on Cisco, voivat ottaa yhteyttä RADIUS palvelimeen. Lisäksi sääntöön on määritetty, että RADIUS tunnuksilla saa tason 15 käyttöoikeuden Ciscon laitteille, joka tarkoittaa Ciscon laitteilla korkeimpia hallintaoikeuksia.



KUVA 5. Connection Reguest Policies-näkymä

4.3.3 Network Policies

Network Policies asetukset määrittävät, että millä perusteella käyttöoikeudet annetaan. Kuvassa 6 näkyvä sääntö Cisco management Level 15, antaa oikeudet palvelimella olevalle käyttäjäryhmälle Cisco RADIUS. Tunnistautumiseen käytetään SPAP- tai PAP-protokollaa.



KUVA 6. Network Policies-näkymä

4.4 Verkkolaitteiden määritys

Verkkolaitteilla oli valmiina niin sanotut perusmääritykset, jotta testiympäristö toimii. Tässä työssä on tarkoitus määrittää RADIUS tunnistautuminen käyttöön laitteille, jolloin kirjautuessa tunnukset ovat ensisijaisesti palvelimella olevat tunnukset, mutta vikatilanteen varalta myös paikallisilla tunnuksilla olisi mahdollista kirjautua.

4.4.1 Cisco SG350 kytkin

Kytkimenä testiympäristössä toimi kuvan 7 mukainen Ciscon valmistama SG350 10-porttinen hallittava kytkin.

KUVA 7. Cisco SG350 10-porttinen kytkin (Cisco 2016).

Kytkimen hallinta tapahtui SSH-yhteydellä palvelimelta, jossa RADIUS-palvelin toimi. Ciscon laitteissa on valmiiksi olemassa RADIUS-tuki, joten sen määritys vaatii vain oikeat asetukset.

4.4.2 Cisco SG350 määritykset

Jotta RADIUS saataisiin toimimaan, tarvittiin palvelimen osoite, sekä radius avain, joka määritettiin palvelimelle aiemmin. Kuvassa 8 nähdään kytkimelle tehtyjä määrityksiä. Ensimmäisenä oleva ”radius-server key”, on palvelimelle ja kytkimelle määritetty jaettu avain, joka toimii salasanan tavoin laitteiden välisessä yhteydessä. Kuvassa jaettu avain on kuitenkin salattu. RADIUS-palvelin on määritetty IP-osoitteella ja sen prioriteetti on 1, joka tarkoittaa sitä, että kyseistä palvelinta kutsutaan ensimmäisenä, mikäli niitä olisi useita.

Palvelimen määritysten lisäksi täytyy määrittää, että miten RADIUS:ta käytetään. Kuvassa näkyvillä ”aaa authentication login” komennoilla määritetään, että mitä yhteyksiä käyttäen pystytään kirjautumaan, ja komennon lopussa oleva ”radius local” määrittää, että kirjautuminen on mahdollista sekä RADIUS-protokollan avulla, että paikallisilla tunnuksilla. ”Aaa authentication enable” komennot kytkevät sekä RADIUS-autentikoinnin, että paikallisen kirjautumisen käyttöön.

Kuvassa 8 näkyvät viimeiset kaksi komentoa, liittyvät tilastointiin. Kun tilastoinniksi on määritetty ”start-stop”, niin käyttäjän istunnosta kerätään aloitusaika, sekä lopetusaika.

```
encrypted radius-server key Ao64yefH80992SjL0Yzpfp4zqC4YzmAmGw+iRYvUStcDMtGSVFgD
LUTKpinS0GDz6UcTAJqzHPg2xV2k4bGrF7g5gxHbLnfAK+stqUBEpgJjachubsn92ULQ2yHgK4uF
radius-server host 192.168.1.31
aaa authentication login ssh radius local
aaa authentication enable shh radius enable
aaa authentication login console radius local
aaa authentication enable console radius enable
aaa authentication login default radius local
aaa accounting dot1x start-stop group radius
aaa accounting login start-stop group radius
```

KUVA 8. Kytkimen RADIUS-määritykset

4.4.3 Cisco ASA 5506x palomuuri

Palomuurina testiympäristössä toimi Ciscon valmistama ASA 5506x. Kyseisessä palomuurissa on kahdeksan Gigabit Ethernet porttia

Kuva 9. Cisco ASA 5506x palomuuri (Cisco 2015).

Palomuurin hallinta tapahtui Triuvaren toimistolla olevan Perle serial-ethernet sovittimen kautta. Palomuurin hallinta onnistui Triuvaren toimistovekosta käsin SSH-yhteydellä.

4.4.4 Cisco ASA 5506x määritykset

Palomuurille täytyi kytkimen tapaan syöttää radiusta varten vaadittavat tiedot, kuten palvelimen osoite, jaettu avain, sekä sallia RADIUS-autentikointi. Palomuurin konfigurointi tapahtui hieman eri taivoin, kuin kytkimen. Palomuurissa täytyi luoda ensin ryhmä RADIUS-määrityksille, joka nimettiin RADIUS_SRV:ksi (kuva 10), jonka jälkeen pystyi määrittämään palvelimen osoitteen, joka oli porttikohtainen. Tässä tapauksessa portti oli nimeltään ”mgt”.

Palvelimen tietojen lisäksi täytyy sallia RADIUS tunnistautuminen eri yhteystyypeille komennolla, kuten kuvassa 10 näkyvä komento ”aaa authentication ssh console RADIUS_SRV LOCAL”, joka sallii SSH yhteydellä kirjautumisen RADIUS-protokollaa käyttäen, tai paikallisilla tunnuksilla, mikäli radius ei ole käytettävissä. Kun tarvittavat yhteystyypit oli sallittu, täytyi määrittää vielä tilastointi, joka on käytössä SSH-, sekä sarjaliikenne yhteyksillä.

```
aaa-server radius_auth protocol radius
aaa-server RADIUS_SRV protocol radius
aaa-server RADIUS_SRV (mgt) host 192.168.1.31
user-identity default-domain LOCAL
aaa authentication ssh console RADIUS_SRV LOCAL
aaa authentication http console RADIUS_SRV LOCAL
aaa authentication serial console RADIUS_SRV LOCAL
aaa accounting ssh console RADIUS_SRV
aaa accounting serial console RADIUS_SRV
aaa authentication login-history
```

KUVA 10. Cisco ASA 5506x palomuurin määritykset.

5 POHDINTA

Tässä opinnäytetyössä oli tarkoitus luoda ratkaisu käyttäjätunnusten hallinnan keskittämiseen RADIUS-protokollalla. Keskittämisellä voidaan parantaa tietoturvaa, koska jokaisella käyttäjällä olisi omat tunnukset, sekä niitä pystyttäisiin hallinnoimaan yhdestä paikasta. RADIUS-protokolla valittiin, koska se oli jo ennestään käytössä Triuvaren ympäristössä ja tällöin keskitetty käyttäjienhallinta olisi helppo toteuttaa.

RADIUS-autentikointi oli aiheena melko vieras, sillä sen toiminnasta ei ollut tietämystä ennestään juurikaan ja siihen perehtyminen vaati melko paljon työtä. RADIUS on kuitenkin melko vanha protokolla, joten siitä löytyi paljon tietoa eri lähteistä. Vaikka testiympäristö oli valmiiksi määritetty, sen toiminta täytyi silti tietää, jotta laitteet voi konfiguroida oikein RADIUS-autentikointia varten.

Ciscon verkkolaitteiden määritys oli melko helppoa, sillä siitä oli hieman aikaisempaa kokemusta. Kuitenkin kytkin ja palomuuri olivat keskenään hyvin erilaisia, joten niihin tutustuminen vei kuitenkin aikaa, jotta sai oikeanlaiset konfiguraatiot tehtyä.

Tässä työssä RADIUS-autentikointi määritettiin toimimaan ilman erikoisempia asetuksia, mutta jatkossa sen rinnalle voidaan vielä lisätä esimerkiksi kaksivaiheinen todennus joko tekstiviestillä tai Authenticator-applikaatiolla. Lisäksi ympäristöä voidaan kehittää, lisäämällä siihen Active Directory integrointi, jolloin käyttäjäryhmiä voitaisiin hallita Active Directorysta.

Työn lopputulos oli se mitä alun perin lähdettiin hakemaan, RADIUS-autentikointi toimii Ciscon laitteilla halutulla tavalla, sekä yhteyden katketessa laitteille pääsee kirjautumaan laitteille säilötyillä paikallisilla käyttäjätunnuksilla. Monissa kohdissa asetukset ja määritykset voisivat olla monella tapaa erilaiset, mutta niihin vaikuttavat ympäristön vaatimukset, sekä käytössä olevat laitteet.

LÄHTEET

Cisco. 2015. Cisco ASA 5506-X with FirePOWER Services. Kuva: Cisco ASA 5506x palomuuri. Katsottu 22.4.2021. https://www.cisco.com/c/en/us/support/security/asa-5506-x-firepower-services/model.html?dtid=osscdc000283

Cisco. 2019. RADIUS Configuration Guide. Cisco IOS Release 15M&T. Luettu 17.03.2021. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/15-mt/sec-usr-rad-15-mt-book/sec-cfg-radius.html

Cisco. 2016. Cisco SG350-10 10-Port Gigabit Managed Switch. Kuva: Cisco SG350 10-porttinen kytkin. Katsottu 22.4.2021. https://www.cisco.com/c/en/us/support/switches/sg350-10-10-port-gigabit-managed-switch/model.html

FreeRADIUS. n.d. FreeRADIUS Documentation. Luettu 28.02.2021. https://networkradius.com/doc/3.0.10/concepts/introduction/components.html

Second Nature Security. n.d. Hallinnollinen tietoturva – Mitä se on? Luettu 16.03.2021. https://www.2ns.fi/hallinnollinen-tietoturva-mita-se-on/

Halonen, P. 2021. Mitä on fyysinen tietoturvallisuus? Luettu 16.03.2021. https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus

Hassel, J. 2002. RADIUS. 2003. Sebastopol: O'Reilly & Associates, Inc.

NetworkRADIUS. 2019. How Does RADIUS Authentication Work? Luettu 10.03.2021. https://networkradius.com/articles/2019/05/08/how-does-radius-authentication-work.html

Lujan, J. 2018. The History and Evolution of the RADIUS Protocol. Luettu 11.02.2021. https://jumpcloud.com/blog/radius-history-evolution

Zevenet. 2017. Remote Authentication Dial-In User Service (RADIUS) reliability and scalability. Kuva: RADIUS ympäristö. Katsottu 24.3.2021. https://www.zevenet.com/knowledge-base/howtos/remote-authentication-dial-in-user-service-radius-reliability-and-scalability/

LIITTEET

Liite 1. RADIUS Configuration Guide

Configuring RADIUS

The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS

To configure RADIUS on your Cisco device or access server, you must perform these tasks:

- Use the **aaa new-model** global configuration command to enable Authentication, Authorization, and Accounting (AAA). AAA must be configured if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use **line** and **interface** commands to enable the defined method lists to be used.

(jatkuu)

Restrictions for RadSec (RADIUS Security)

RadSec is not supported on any of the Cisco enterprise routing platforms.

Information About RADIUS

RADIUS Network Environments

Cisco supports RADIUS under its authentication, authorization, and accounting (AAA) security paradigm. RADIUS can be used with other AAA security protocols such as TACACS+, Kerberos, and local username lookup. RADIUS is supported on all Cisco platforms, but some RADIUS-supported features run only on specified platforms.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and grant access to network resources.
- Networks already using RADIUS. You can add a Cisco device with RADIUS to the network. This might be the first step when you make a transition to a TACACS+ server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as PPP. For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using the IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, and bytes) used during the session. An ISP might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.
- Networks that support preauthentication. Using the RADIUS server in your network, you can configure AAA preauthentication and set up the preauthentication profiles. Preauthentication enables service providers to better manage ports using their existing RADIUS solutions, and to efficiently manage the use of shared resources to offer differing service-level agreements.

RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:
  - AppleTalk Remote Access (ARA)

- NetBIOS Frame Control Protocol (NBFCP)
- NetWare Asynchronous Services Interface (NASI)
- X.25 Packet Assemblers/Disassemblers (PAD) connections

- Device-to-device situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

1. The user is prompted to enter the username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
    1. ACCEPT—The user is authenticated.
    2. CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
    3. CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.
    4. REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including connections such as Telnet, rlogin, or local-area transport (LAT), and services such as PPP, Serial Line Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IP address, access list, and user timeouts.

RADIUS Attributes

The network access server monitors the RADIUS authorization and accounting functions defined by RADIUS attributes in each user profile:

Vendor-Proprietary RADIUS Attributes

An Internet Engineering Task Force (IETF) standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. Some vendors, nevertheless, have extended the RADIUS attribute set in a unique way. Cisco software supports a subset of vendor-proprietary RADIUS attributes.

RADIUS Tunnel Attributes

RADIUS is a security server AAA protocol originally developed by Livingston, Inc. RADIUS uses attribute value (AV) pairs to communicate information between the security server and the network access server.

RFC 2138 and RFC 2139 describe the basic functionality of RADIUS and the original set of IETF-standard AV pairs used to send AAA information. Two IETF standards, "RADIUS Attributes for Tunnel Protocol Support" and "RADIUS Accounting Modifications for Tunnel Protocol Support," extend the IETF-defined set of AV pairs to include attributes specific to VPNs. These attributes are used to carry the tunneling information between the RADIUS server and the tunnel initiator.

RFC 2865 and RFC 2868 extend the IETF-defined set of AV pairs to include attributes specific to compulsory tunneling in VPNs by allowing the user to specify authentication names for the network access server and the RADIUS server.

Cisco devices and access servers support new RADIUS IETF-standard virtual private dialup network (VPDN) tunnel attributes.

Preauthentication on a RADIUS Server

RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. In addition to configuring preauthentication on your Cisco device, you must set up the preauthentication profiles on the RADIUS server.

RADIUS Profile for DNIS or CLID Preauthentication

To configure the RADIUS preauthentication profile, use the Dialed Number Identification Service (DNIS) or Calling Line Identification (CLID) number as the username, and use the password defined in the **dnis** or **clid** command as the password.

Note The preauthentication profile must have "outbound" as the service type because the password is predefined on the network access server (NAS). Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The "outbound" service type is also included in the Access-Request packet sent to the RADIUS server.

RADIUS Profile for Call Type Preauthentication

To set up the RADIUS preauthentication profile, use the call type string as the username, and use the password defined in the **ctype** command as the password. The table below lists the call type strings that can be used in the preauthentication profile.

Table 1: Call Type Strings Used in Preauthentication

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.

Call Type String	ISDN Bearer Capabilities
speech	Speech, 3.1 kHz audio, 7 kHz audio. **Note** This is the only call type available for channel-associated signaling (CAS) .
v.110	Anything with the V.110 user information layer.
v.120	Anything with the V.120 user information layer.

Note The preauthentication profile must have “outbound” as the service type because the password is predefined on the NAS. Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The “outbound” service type is also included in the Access-Request packet sent to the RADIUS server and should be a checkin item if the RADIUS server supports checkin items.

RADIUS Profile for Preauthentication Enhancements for Callback

Callback allows remote network users such as telecommuters to dial in to the NAS without being charged. When callback is required, the NAS hangs up the current call and dials the caller back. When the NAS performs the callback, only information for the outgoing connection is applied. The rest of the attributes from the preauthentication access-accept message are discarded.

Note The destination IP address is not required to be returned from the RADIUS server.

The following example shows a RADIUS profile configuration with a callback number of 555-0101 and the service type set to outbound. The cisco-avpair = “preauth:send-name=<string>” uses the string “user1” and the cisco-avpair = “preauth:send-secret=<string>” uses the password “cisco.”

```
5550101 password = “cisco”, Service-Type = Outbound
Service-Type = Callback-Framed
Framed-Protocol = PPP,
Dialback-No = “5550119”
Class = “ISP12”
cisco-avpair = “preauth:send-name=user1”
cisco-avpair = “preauth:send-secret=cisco”
```

RADIUS Profile for a Remote Hostname Used for Large-Scale Dial-Out

The following example protects against accidentally calling a valid telephone number but accessing the wrong device by providing the name of the remote device, for use in large-scale dial-out:

```
5550101 password = "PASSWORD1", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5550190"
       Class = "ISP12"
       cisco-avpair = "preauth:send-name=user1"
```

```
cisco-avpair = "preauth:send-secret=PASSWORD1"
cisco-avpair = "preauth:remote-name=Device2"
```

RADIUS Profile for Modem Management

When DNIS, CLID, or call type preauthentication is used, the affirmative response from the RADIUS server might include a modem string for modem management in the NAS through vendor-specific attribute (VSA) 26. The modem management VSA has this syntax:

```
cisco-avpair = "preauth:modem-service=modem min-speed <
x
> max-speed <
y
>
modulation <
z
> error-correction <
a
> compression <
b
>"
```

The table below lists the modem management string elements within the VSA.

Table 2: Modem Management String

Command	Argument
min-speed	300 to 56000, any
max-speed	300 to 56000, any
modulation	K56Flex, v22bis, v32bis, v34, v90, any
error-correction	lapm, mnp4
compression	mnp5, v42bis

When the modem management string is received from the RADIUS server in the form of a VSA, the information is passed to the Cisco software and applied on a per-call basis. Modem ISDN channel aggregation (MICA) modems provide a control channel through which messages can be sent during the call setup time. Hence, this modem management feature is supported only with MICA modems. This feature is not supported with Microcom modems.

RADIUS Profile for Subsequent Authentication

If preauthentication passes, you can use vendor-proprietary RADIUS attribute 201 (Require-Auth) in the preauthentication profile to determine whether subsequent authentication is performed. If attribute 201, returned in the access-accept message, has a value of 0, subsequent authentication is not performed. If attribute 201 has a value of 1, subsequent authentication is performed as usual.

Attribute 201 has this syntax:

```
cisco-avpair = "preauth:auth-required=<
n
>"
```

where <*n*> has the same value range as attribute 201 (that is, 0 or 1).

If attribute 201 is missing in the preauthentication profile, a value of 1 is assumed, and subsequent authentication is performed.

Note Before you can perform subsequent authentication, you must set up a regular user profile in addition to a preauthentication profile.

RADIUS Profile for Subsequent Authentication Types

If you specified subsequent authentication in the preauthentication profile, you must also specify the authentication types to be used for subsequent authentication. To specify the authentication types allowed in subsequent authentication, use this VSA:

```
cisco-avpair = "preauth:auth-type=<
string
>"
```

The table below lists the allowed values for the <*string*> element.

Table 3: <string> Element Values

String	Description
chap	Requires the username and password for the Challenge-Handshake Authentication Protocol (CHAP) for PPP authentication.
ms-chap	Requires the username and password for the MS-CHAP for PPP authentication.
pap	Requires the username and password for the Password Authentication Protocol (PAP) for PPP authentication.

To specify that multiple authentication types are allowed, you can configure more than one instance of this VSA in the preauthentication profile. The sequence of the authentication type VSAs in the preauthentication profile is significant because it specifies the order of authentication types to be used in the PPP negotiation.

This VSA is a per-user attribute and replaces the authentication type list in the **ppp authentication** interface configuration command.

Note You should use this VSA only if subsequent authentication is required because it specifies the authentication type for subsequent authentication.

RADIUS Profile to Include the Username

If only preauthentication is used to authenticate a call, the NAS could be missing a username when it brings up the call. RADIUS can provide a username for the NAS to use through RADIUS attribute 1 (User-Name) or through a VSA returned in the Access-Accept packet. The VSA for specifying the username has this syntax:

```
cisco-avpair = "preauth:username=<
```

```
string
>"
```

If no username is specified, the DNIS number, CLID number, or call type is used, depending on the last preauthentication command configured (for example, if **clid** was the last preauthentication command configured, the CLID number is used as the username).

If subsequent authentication is used to authenticate a call, there might be two usernames: one provided by RADIUS and one provided by the user. In this case, the username provided by the user overrides the one contained in the RADIUS preauthentication profile. The username provided by the user is used for both authentication and accounting.

RADIUS Profile for Two-Way Authentication

In the case of two-way authentication, the calling networking device must authenticate the NAS. The PAP username and password or CHAP username and password need not be configured locally on the NAS. Instead, the username and password can be included in the Access-Accept messages for preauthentication.

Note Do not configure the **ppp authentication** command with the **radius** command.

To set up PAP, do not configure the **ppp pap sent-name password** command on the interface. The VSAs "preauth:send-name" and "preauth:send-secret" are used as the PAP username and PAP password for outbound authentication.

For CHAP, "preauth:send-name" is used not only for outbound authentication but also for inbound authentication. For a CHAP inbound case, the NAS uses the name defined in "preauth:send-name" in the challenge packet to the caller networking device. For a CHAP outbound case, both "preauth:send-name" and "preauth:send-secret" are used in the response packet.

The following example shows a configuration that specifies two-way authentication:

```
5550101 password = "PASSWORD2", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=user1"
cisco-avpair = "preauth:send-secret=PASSWORD2"
class = "<some class>"
```

Note Two-way authentication does not work when resource pooling is enabled.

RADIUS Profile to Support Authorization

If only preauthentication is configured, subsequent authentication is bypassed. Note that because the username and password are not available, authorization is also bypassed. However, you can include authorization attributes in the preauthentication profile to apply per-user attributes and avoid having to return subsequently to RADIUS for authorization. To initiate the authorization process, you must also configure the **aaa authorization network** command on the NAS.

You can configure authorization attributes in the preauthentication profile with one exception: the service-type attribute (attribute 6). The service-type attribute must be converted to a VSA in the preauthentication profile. This VSA has this syntax:

```
cisco-avpair = "preauth:service-type=<
n
>"
```

where <*n*> is one of the standard RFC 2865 values for attribute 6.

Note If subsequent authentication is required, the authorization attributes in the preauthentication profile are not applied.

RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the **aaa authentication** command, specifying RADIUS as the authentication method.

RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, AppleTalk Remote Access (ARA), and Telnet. Because RADIUS authorization is facilitated through AAA, you must enter the **aaa authorization** command, specifying RADIUS as the authorization method.

RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing and the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must enter the **aaa accounting** command, specifying RADIUS as the accounting method.

RADIUS Login-IP-Host

To enable the network access server (NAS) to attempt more than one login host when trying to connect a dial-in user, you can enter as many as three Login-IP-Host entries in the user's profile on the RADIUS server. The following example shows that three Login-IP-Host instances are configured for the user *user1*, and that TCP-Clear is used for the connection:

```
user1 Password = xyz
        Service-Type = Login,
        Login-Service = TCP-Clear,
        Login-IP-Host = 10.0.0.0,
        Login-IP-Host = 10.2.2.2,
        Login-IP-Host = 10.255.255.255,
        Login-TCP-Port = 23
```

The order in which the hosts are entered is the order in which they are attempted. Use the **ip tcp synwait-time** command to set the number of seconds that the NAS waits before trying to connect to the next host on the list; the default is 30 seconds.

Your RADIUS server might permit more than three Login-IP-Host entries; however, the NAS supports only three hosts in Access-Accept packets.

RADIUS Prompt

To control whether user responses to Access-Challenge packets are echoed to the screen, you can configure the Prompt attribute in the user profile on the RADIUS server. This attribute is included only in Access-Challenge packets. The following example shows the Prompt attribute set to No-Echo, which prevents the user's responses from echoing:

```
user1 Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

To allow user responses to echo, set the attribute to Echo. If the Prompt attribute is not included in the user profile, responses are echoed by default.

This attribute overrides the behavior of the **radius-server challenge-noecho** command configured on the access server. For example, if the access server is configured to suppress echoing, but the individual user profile allows echoing, the user responses are echoed.

Note If you want to use the Prompt attribute, your RADIUS server must be configured to support Access-Challenge packets.

Vendor-Specific RADIUS Attributes

The IETF standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, which is named "cisco-avpair." The value is a string with this format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; protocols that can be used include IP, Internetwork Packet Exchange (IPX), VPDN, VoIP, Secure Shell (SSH), Resource Reservation Protocol (RSVP), Serial Interface Processor (SIP), AirNet, and Outbound. "Attribute" and "value" are an appropriate AV pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes, allowing the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an "*", the AV pair "ip:addr-pool=first" becomes optional. Note that any AV pair can be made optional:

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs.

Static Routes and IP Addresses on the RADIUS Server

Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. Each network access server then queries the RADIUS server for static route and IP pool information.

To have the Cisco device or access server query the RADIUS server for static routes and IP pool definitions when the device starts up, use the **radius-server configure-nas** command.

Because the **radius-server configure-nas** command is performed when the Cisco devcie starts up, it does not take effect until you enter a **copy system:running-config nvram:startup-config** command.

How to Configure RADIUS

Configuring a Device for Vendor-Proprietary RADIUS Server Communication

Although an IETF standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco software supports a subset of vendor-proprietary RADIUS attributes.

To configure RADIUS (whether vendor-proprietary or IETF compliant), you must use the **radius-server** commands to specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. To identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command. Vendor-proprietary attributes are not supported unless you use the **radius-server host non-standard** command.

Note The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **radius-server vsa send** [**accounting** | **authentication**]
4. **radius server** *server-name*
5. **address ipv4** *ip-address*
6. **non-standard**
7. **key** {**0** *string* | **7** *string* | *string*}
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting**	**authentication**] **Example:** `Device(config)# radius-server vsa send`	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.
Step 4	**radius server** *server-name* **Example:** `Device(config)# radius server rad1`	Specifies the name for the RADIUS server. **Note** The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.
Step 5	**address ipv4** *ip-address* **Example:** `Device(config-radius-server)# address ipv4 10.45.1.2`	Assigns an IP address to the RADIUS server.
Step 6	**non-standard** **Example:** `Device(config-radius-server)# non-standard`	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.
Step 7	**key** {**0** *string*	**7** *string*	*string*} **Example:**	Specifies the shared secret text string used between the device and the vendor-proprietary RADIUS server.

	Command or Action	Purpose
	`Device(config-radius-server)# key myRaDIUSpassword`	• The device and the RADIUS server use this text string to encrypt passwords and exchange responses.
Step 8	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring a Device to Expand Network Access Server Port Information

Sometimes PPP or login authentication occurs on an interface that is different from the interface on which the call itself comes in. For example, in a V.120 ISDN call, login or PPP authentication occurs on a virtual asynchronous interface "ttt", but the call itself occurs on one of the channels of the ISDN interface.

The **radius-server attribute nas-port extended** command configures RADIUS to expand the size of the NAS-Port attribute (RADIUS IETF attribute 5) field to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface undergoing authentication.

Note The **radius-server attribute nas-port format** command replaces the **radius-server extended-portnames** command and the **radius-server attribute nas-port extended** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server configure-nas**
4. **radius-server attribute nas-port format**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius-server configure-nas** **Example:** `Device(config)# radius-server configure-nas`	(Optional) Tells the Cisco device or access server to query the RADIUS server for the static routes and IP pool definitions used throughout its domain. **Note** Because the **radius-server configure-nas** command is used when the Cisco device starts up, it does not take effect until you issue a **copy system:running-config nvram:startup-config** command.
Step 4	**radius-server attribute nas-port format** **Example:** `Device(config)# radius-server attribute nas-port format`	Expands the size of the NAS-Port attribute from 16 to 32 bits to display extended interface information.
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Replacing the NAS-Port Attribute with the RADIUS Attribute

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation does not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 appear as NAS-Port = 20101 because of the 16-bit field size limitation associated with the RADIUS IETF NAS-Port attribute. In this case, you can replace the NAS-Port attribute with a VSA (RADIUS IETF attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. VSAs can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) is sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. After this command is configured, the standard NAS-Port attribute is no longer sent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **aaa nas port extended**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Device(config)# radius-server vsa send`	Enables the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF attribute 26.
Step 4	**aaa nas port extended** **Example:** `Device(config)# aaa nas port extended`	Expands the size of the VSA NAS-Port field from 16 to 32 bits to display extended interface information.
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring the Suffix and Password in RADIUS Access Requests

Large-scale dial-out eliminates the need to configure dialer maps on every NAS for every destination. Instead, you can create remote site profiles that contain outgoing call attributes on the AAA server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site.

You can configure the username in the Access-Request message to RADIUS. The default suffix of the username, "-out," is appended to the username. The format for composing the username attribute is the IP address plus the configured suffix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa route download** *time*
5. **aaa authorization configuration default**
6. **interface dialer** *number*
7. **dialer aaa**
8. **dialer aaa suffix** *suffix* **password** *password*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa route download** *time* **Example:** `Device(config)# aaa route download 450`	Enables the download static route feature and sets the amount of time in minutes between downloads.
Step 5	**aaa authorization configuration default** **Example:** `Device(config)# aaa authorization configuration default`	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
Step 6	**interface dialer** *number* **Example:** `Device(config)# interface dialer 1`	Defines a dialer rotary group and enters interface configuration mode.
Step 7	**dialer aaa** **Example:** `Device(config-if)# dialer aaa`	Allows a dialer to access the AAA server for dialing information.
Step 8	**dialer aaa suffix** *suffix* **password** *password* **Example:** `Device(config-if)# dialer aaa suffix @samp password password12`	Allows a dialer to access the AAA server for dialing information and specifies a suffix and nondefault password for authentication.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining RADIUS

SUMMARY STEPS

1. enable
2. debug radius
3. show radius statistics
4. show aaa servers
5. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Device# debug radius`	Displays information associated with RADIUS.
Step 3	**show radius statistics** **Example:** `Device# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets.
Step 4	**show aaa servers** **Example:** `Device# show aaa servers`	Displays the status and number of packets that are sent to and received from all public and private AAA RADIUS servers as interpreted by the AAA Server MIB.
Step 5	**exit** **Example:** `Device# exit`	Exits the device session.

Configuration Examples for RADIUS

Example: RADIUS Authentication and Authorization

The following example shows how to configure the device to authenticate and authorize using RADIUS:

```
aaa authentication login use-radius group radius local
```

```
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius group radius local** command configures the device to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication.
- The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco software to use RADIUS authentication for lines using PPP with CHAP or PAP if the user has not already been authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec default group radius** command sets the RADIUS information that is used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network default group radius** command sets RADIUS for network authorization, address assignment, and access lists.

Example: RADIUS Authentication, Authorization, and Accounting

The following example shows a general configuration using RADIUS with the AAA command set:

```
radius-server host 10.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.

- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.
- The **login authentication admins** command applies the "admins" method list for login authentication.
- The **ppp authentication pap dialins** command applies the "dialins" method list to the lines specified.

Example: Vendor-Proprietary RADIUS Configuration

The following example shows a general configuration using vendor-proprietary RADIUS with the AAA command set:

Note The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see *Cisco IOS Security Command Reference: Commands M to R*.

```
radius server myserver
radius server address ipv4 192.0.2.2
non-standard
key 7 any key
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
```

The lines in this RADIUS authentication, authorization, and accounting configuration example are defined as follows:

- The **non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.
- The **key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **configure-nas** command defines that the Cisco device or access server queries the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network default group radius local** command assigns an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.

Example: Multiple RADIUS Server Entries for the Same Server IP Address

The following example shows how to configure the network access server to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as failover backup to the first one. (The RADIUS host entries are tried in the order they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2001
```

Example: RADIUS User Profile with RADIUS Tunneling Attributes

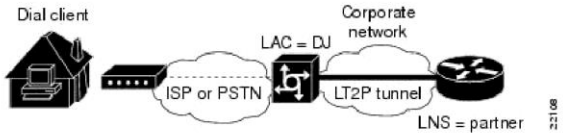
The following example shows a RADIUS user profile (Merit Daemon format) that includes RADIUS tunneling attributes:

```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
cisco-avpair = vpdn:l2tp-nosession-timeout=30
cisco-avpair = vpdn:l2tp-cm-retransmit-retries=10
cisco-avpair = vpdn:l2tp-cm-min-timeout=2
cisco-avpair = vpdn:l2tp-hello-interval=60
Service-Type = outbound
Tunnel-Assignment-Id_tag1 = ISP1
Tunnel-Client-Auth-Id_tag1 = LAC1
Tunnel-Client-Endpoint_tag1 = 10.0.0.2
Tunnel-Medium-Type_tag1 = IPv4
Tunnel-Password_tag1 = tunnel1
Tunnel-Server-Auth-Id_tag1 = LNS1
Tunnel-Server-Endpoint_tag1 = 10.0.0.1
Tunnel-Type_tag1 = l2tp
```

Examples: L2TP Access Concentrator Configuration

The following example shows a basic L2TP configuration for the L2TP access concentrator (LAC) for the topology shown in the figure below. The local name is not defined, so the hostname used is the local name. Because the L2TP tunnel password is not defined, the username password is used. In this example, VPDN is configured locally on the LAC and does not take advantage of the new RADIUS tunnel attributes.

Figure 1: Topology for Configuration Examples




```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
```

```
aaa authentication ppp default local
! Define the username as "DJ."
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Define VPDN group number 1.
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
! domain "cisco.com."
 request dialin
  protocol l2tp
  domain cisco.com
 initiate-ip to 172.21.9.13
 local name nas-1
```

The following example shows the configuration for the LAC if RADIUS tunnel attributes are supported. In this example, there is no local VPDN configuration on the LAC; the LAC, instead, is configured to query the remote RADIUS security server.

```
! Enable global AAA securities services.
aaa new-model
! Enable AAA authentication for PPP and list RADIUS as the default method to use
! for PPP authentication.
aaa authentication ppp default group radius local
! Enable AAA (network) authorization and list RADIUS as the default method to use for
! authorization.
aaa authorization network default group radius
! Define the username as "DJ."
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Configure the LAC to interface with the remote RADIUS security server.
radius host 171.19.1.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

Examples: L2TP Network Server Configuration

The following example shows a basic L2TP configuration with corresponding comments on the L2TP network server (LNS):

```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as "partner."
username partner password 7 030C5E070A00781B
! Create virtual-template 1 and assign all values for virtual access interfaces.
interface Virtual-Template1
! Borrow the IP address from loopback interface.
 ip unnumbered loopback0
! Disable multicast fast switching.
 no ip mroute-cache
! Use CHAP to authenticate PPP.
 ppp authentication chap
! Enable VPDN.
vpdn enable
! Create vpdn-group number 1.
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ.
 accept dialin l2tp virtual-template 1 remote DJ
```

```
  protocol any
  virtual-template 1
 terminate-from hostname nas1
local name hgw1
```

The following example shows how to configure the LNS with a basic L2TP configuration using RADIUS tunneling attributes:

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface GigabitEthernet1/0/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered loopback0
ppp authentication pap
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
RADIUS attributes	*RADIUS Attributes Configuration Guide* (part of the Securing User Services Configuration Library)
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)
L2TP, VPN, or VPDN	*Dial Technologies Configuration Guide* and *VPDN Configuration Guide*

Related Topic	Document Title
Modem configuration and management	*Dial Technologies Configuration Guide*
RADIUS port identification for PPP	*Wide-Area Networking Configuration Guide*

RFCs

RFC	Title
RFC 2138	*Remote Authentication Dial-In User Service (RADIUS)*
RFC 2139	*RADIUS Accounting*
RFC 2865	*RADIUS*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring RADIUS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Configuring RADIUS

Feature Name	Releases	Feature Information
Configuring RADIUS	Cisco IOS 11.1 Cisco IOS 12.1(5)T Cisco IOS 12.2(13)T Cisco IOS 12.2(27)SBA Cisco IOS 12.2(33)SRC Cisco IOS 15.4(1)S	The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. In Cisco IOS Release 15.4(1)S, support was added for the Cisco ASR 901S Router.
RADIUS Statistics via SNMP	Cisco IOS 15.1(1)S Cisco IOS 15.1(1)SY Cisco IOS 15.1(4)M	This feature provides statistics related to RADIUS traffic and private RADIUS servers. The following commands were introduced or modified: **show aaa servers**, **show radius statistics**.