LAUREA - AMMATTIKORKEAKOULU

Cisco Systemsin CCNA-sertifikaattiin pohjautuvien verkkoharjoitusten suunnittelu ja toteutus opintojaksolle Information Networks

. . . . . .

Niemi, Tero

2009 Leppävaara

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Yrityksen tietoverkot

Tero Niemi

Cisco Systemsin CCNA-sertifikaattiin pohjautuvien verkkoharjoitusten suunnittelu ja toteutus Information Networks opintojaksolle.

Vuosi 2009 Sivumäärä 268

Opinnäytetyössä suunniteltiin ja toteutettiin Laurea-ammattikorkeakoulun opintojaksolle Information Networks-verkkoharjoitukset, joissa käsiteltiin Ciscon CCNA-sertifikaattiin liittyviä aihealueita. Harjoituksien tarkoituksena on kehittää opiskelijoiden asiantuntijatehtävissa vaadittavaa verkkopuolen osaamista sekä lisätä Cisco IOS-käyttöjärjestelmän tuntemusta. Harjoituksien suunnittelussa painotettiin erityisesti ongelmanratkaisukyvyn lisäämistä sekä teoriapohjaisten luentojenpakettien soveltamista käytännössä. Harjoitukset toteutetaan osana Information Networks-opintojakson suorittamista Laurean tietoliikennelaboratoriossa.

Työn yleinen verkkoteoria osuus koostuu OSI-mallin toiminnasta, TCP/IP-protokollasta ja IPv4-protokollasta. Lisäksi teoriaosuudessa keskitytään erityisesti lähiverkon toimintaan ja laitteisiin, virtuaaliseen lähiverkon toimintaan, langattoman lähiverkon tekniikoihin ja laitteisiin sekä IPv6-protokollan toimintaan. Teoriaosuudessa käsitellään laajemmin reitityksen, reititysprotollien sekä pääsylistojen toimintaa.

Opinnäytetyön verkkoharjoitusten käsittelyosuudessa käydään läpi luodut yhdeksän verkkoharjoitusta. Harjoitukset käsitellään läpi osa-alueittain. Osiossa esitellään myös malliesimerkkejä käskyjen käytöstä harjoituksien yhteydessä. Harjoituksissa opiskelijat konfiguroivat Ciscon verkkolaitteita kuten kytkimiä, reitittimiä sekä langattoman verkon tukiasemia. Lisäksi opiskelivat käyttävät Ciscon Access Control Server (ACS) -ohjelmistoa langattoman verkon salauksen tekemisessä. Neljä ensimmäistä harjoitusta sisältävät perusverkkoteorian käsittelyä sekä laitteiden peruskonfiguraation tekemistä. Harjoitukset viidestä eteenpäin edellyttävät vaativampaa osaamista ja niissä opiskelijoilta vaaditaan esimerkiksi verkkotopologian rakentamista harjoituksien kuvien perusteella.

Opinnäytetyön empiirisessä osuudessa kerrotaan verkkoharjoitusten toteutusprosessista ja siitä, mitä vaiheita harjoitusten tekemiseen liittyi. Ensimmäisessä vaiheessa harjoitukset suunniteltiin ja tehtiin työhön liittyvä teoria-aiheen rajaaminen. Opiskelijapalautekyselyn perusteella saatua palautetta käytettiin avuksi uusien verkkoharjoituksien suuunnittelussa. Tämän jälkeen uudet CCNA-sertifikaattia tukevat verkkoharjoitukset luotiin vaatimuksia noudattaen. Uusia harjoituksia testattiin Laurean tietoliikennelaboratoriossa opintojakson yhteydessä. Harjoitukset on tarkoitus ottaa käyttöön vuoden 2009 keväällä.

Asiasanat: Cisco IOS, lähiverkko, virtuaalilähiverkko, langaton lähiverkko, reititys, pääsylistat, osoitekäännös

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology Programme
Information Systems and Data Communication

Tero Niemi

Planning and execution of Cisco Systems CCNA Certificate based network exercises for the course Information Networks

Year 2009 Pages 268

The purpose of this thesis was to plan and execute network exercises for a Laurea University of Applied Sciences course on Information Networks. The network exercises consist of a theory for the Cisco Certified Network Associate (CCNA) examination. The purpose of the exercises was to develop the knowledge of network expert duties and the Cisco IOS operating system. Planning the exercises was focused specially on developing problem-solving skills and applying course theory in practice.The students make the exercises as part of the Interconnecting Networks course at the Laurea Data Communication laboratory.

In the theoretical section about the OSI-model, Transmission Control Protocol/Internet Protocol and Internet Protocol version 4 are covered. In addition, the operation of the local area network and devices, the virtual area network, wireless local area network technics, wireless devices and the concepts of Internet Protocol version 6 are discussed. The concepts of routing, routing protocols and functioning of Access lists are most widely covered in the theory sections.

The exercise part covers all nine network exercises, which are covered one at a time. Examples of Cisco IOS commands are also added to the exercise part. In the exercises students configure Cisco network devices such as switches, routers and wireless network access points. Cisco Access Control Server is used for making wireless network encryption. The first four network exercises consist of basic network principles and configuration tasks. Exercises five to nine consist of more demanding tasks and students must, for example, understand how to build network topology based on exercise network pictures.

The empirical section of the thesis describes how the network exercises are implemented and what phases are used in the working process. First the exercises and theory areas were planned and a student feedback poll was used to help to exercise the planning process. Then new exercises were created to meet the requirements of CCNA–certification. The exercises were tested at the Laurea Data Communication Laboratory during the autumn at the final stage of the implementing process. The final exercises are planned to be implemented on the Interconnecting Networks course in the spring 2009.

Key words: Cisco IOS, local area network, virtual local area network, wireless local area network, routing, access lists, network address translation

SISÄLLYS

1 Johdanto

Laureaan viime vuosina kehitetyt osaamista tuottavat oppimisympäristöt mahdollistavat LdB-toimintamallin toteuttamisen ja tukevat opetussuunnitelman toteuttamista arjessa. Oppimisympäristöt tukevat rikastavien verkostojen kehittymistä, jaetun asiantuntijuuden yhteisöjen syntymistä ja uuden osaamisen luomista. Käytännön sovelluksia uudenlaisista oppimisympäristöistä ovat yhteisön innovaatioympäristöinä toimivat verkostoissa toteutettavat hankkeet ja projektit sekä erilaiset oppimis- ja kehittämistoiminnalle suunnitellut toimintatilat, osaamiskeskittymät, kehittämislaboratoriot ja työpajat. Työmuotona on jaettuun asiantuntijuuteen pohjautuva yhteistoiminta, jota tukee osaamisen jakamisen menetelmät: ohjaus ja opetustuokiot, havaintoesitykset, tiimipalaverit, palautetilaisuudet sekä seminaarit.

Laureassa hyödynnetään myös teknologian mahdollistamia virtuaalisia oppimisympäristöjä. Virtuaaliympäristö mahdollistaa kohtaamisen eri etäisyyksiltä silloin, kun se osallistujille parhaiten soveltuu. Verkko-oppimisen käsite sijoittuu virtuaaliympäristöön, jossa kohdataan ohjaus- ja neuvontapalvelujen myötä erilaisten oppimistehtävien sisältämien haasteiden parissa. (Opetusasiainhallinto 2007, 21-22.)

Tein opinnäytetyöni Laurea-ammattikorkeakoulun tietoliikennelaboratorioon. Tietoliikennelaboratorio on Laurea-ammattikorkeakoulun kehittämisympäristö, jonka tarkoituksena on tarjota oppimisympäristö, jossa opiskelijoilla on mahdollista soveltaa oppimaansa käytännössä. Laboratoriossa toteutetaan erilaisia projekteja sekä opinnäytetöitä. Tietoliikennelaboratorion asiakkaina toimivat Laureassa tietoverkkoja opiskelevat opiskelijat, jotka käyttävät laboratoriota hyödyksi verkkokursseihin liittyvien harjoituksien tekemisessä sekä erilaisissa projektitöissä. Tietoliikennelaboratoriossa tehtävät verkkoharjoitukset liittyvät Ciscon verkkolaitteiden mm. kytkimien, reitittimien sekä WLAN-tukiasemien konfigurointiin ja hallintaan.

Opinnäytetyön aiheena oli uusien verkkoharjoitusten suunnittelu Laurea-ammattikorkeakoulun Leppävaaran yksikössä toteutettavalle Interconnecting Networks-opintojaksolle. Verkkoharjoitukset perustuvat Ciscon julkaisemiin CCNA/ICND1 ja ICND2-kirjojen aihealueisiin. Verkkoharjoitukset toteutetaan tietoliikennelaboratorion laitteilla, ja ne ovat mukana yhtenä osa-alueena kurssin arvostelussa.

Opinnäytetyö sisältää teoriaosuuden CCNA-sertifikaatin suorittamiseen liittyvistä aihe-alueista. Teoriaosuus koostuu verkkotekniikan perusteista, lähiverkkoon liittyvästä teoriasta sekä lähiverkkolaitteista. Teoriaosuudessa käydään läpi virtuaalisia lähiverkkoja, langattomia verkkoja, reititystä ja reititysprotokollien perusteita sekä viimeisenä osa-alueena IPv6-protokollan toimintaa lyhyesti. Opinnäytetyön toisessa osassa tarkastellaan luotuja verkkoharjoituksia osioittain. Opinnäytetyön kolmannessa osassa tarkastellaan opinnäytetyön suunnittelu, toteutus, testaus sekä arviointi prosessia. Opinnäytetyön viimeinen osa sisältää työn kokonaisarviointia ja tavoitteiden läpikäyntiä.

Työ toteutettiin käyttämällä toimintapohjaista tutkimusmenetelmämallia. Järvinen & Järvinen kirjassaan Tutkimustyön metodeista (2000, 129-130.) määrittävät toimintapohjaisen tutkimusmenetelmä mallin. Toimintapohjaisessa tutkimuksessa tutkija osallistuu tutkittavan kohteen toimintaan tutkijan tai konsultin roolissa muutosagenttina. Toimintatutkimus koostuu viidestä vaiheesta: diagnosoinnista, jossa ongelma tunnistetaan ja määritellään, suunnitteluvaiheesta, jossa haetaan vaihtoehtoja ongelman ratkaisemiseksi sekä toteutusvaiheesta, jossa valitaan ehdolla olevista vaihtoehdoista parhaiten sopiva ja toteutetaan se. Toteutuksen jälkeen toimenpiteitä arvioidaan arviointivaiheessa ja työn lopussa pyritään tunnistamaan uusia löydöksiä, joita työ on tuottanut. Tätä mallia voidaan toistaa tarvittaessa useita kertoja, jotta haluttu lopputulos voidaan saavuttaa.

2 Käsitteitä

Cisco CCNA (Cisco Certified Network Associate) -sertifikaatin tarkoitus on kouluttaa ihmisiä Ciscon verkkolaitteiden hallintaan, konfigurointiin, ylläpitoon sekä vianhakuun. Sertifikaatin suorittaminen keskittyy keskisuuren yrityksen verkkoihin sekä yhteydenpitoon eri toimipisteiden välillä, tietoturvauhkiin sekä langattomiin verkkoihin.

Cisco IOS CLI (Internetwork Operating System Command Line Interface) -ohjelmistoa käytetään Ciscon valmistamien kytkimien ja reitittimien konfiguroinnissa. IOS-ohjelmiston avulla luodaan komentojonopohjainen yhteys kytkimeen tai reitittimeen. IOS-ohjelmisto tukee kolmea yleisintä yhteydenmuodostamismetodia konsoli-, Telnet-ja SSH-yhteyksiä.

Kytkin (Switch) on nykyisin lähiverkon keskeisin komponentti. Sen tehtävänä on kehysten tai solujen välittäminen mahdollisimman nopeasti lähdeportista kohdeporttiin annettujen ohjeiden mukaan. Peruskytkimet toimivat OSI-mallin toisessa kerroksessa eli siirtokerroksessa.

Reititin (Router) on lähiverkon keskeisiä laitteita. Reitittimen tehtävänä on yhdistää lähiverkon aliverkoja toisiinsa sekä rajata levitysviestien leviämistä verkossa. Reititin toimii pääasiallisesti OSI-mallin kolmannessa kerroksessa eli verkkokerroksessa.

LAN (Local Area Network) eli lähiverkko termillä tarkoitetaan maantieteellisesti rajattua pienehkön alueen sisäistä tietoliikennettä toteuttavaa ja suuren kapasiteetin omaavaa verkkoa, jota yksi organisaatio hallitsee. Lähiverkko koostuu kaapeleista, verkkolaitteista, työasemista ja palvelimista.

WLAN (Wireless Local Area Network) eli langattomalla verkolla tarkoitetaan verkkoa, jonka fyysinen osuus hoidetaan radiotaajuuksia käyttämällä. Ainoaksi kaapeloitavaksi osuudeksi langattomissa verkoissa jää kaapelin kytkeminen tukiaseman ja kytkimen tai reitittimen välille.

WAN (Wide Area Network) eli laajaverkko termillä tarkoitetaan verkkoa, jonka ulottuvuus vaihtelee paikkakunnalta toiselta jopa mantereiden väliseksi verkoksi. Laajaverkot yhdistävät lähiverkkoja ja niitä hallitsevat normaalisti teleoperaattorit.

VLAN (Virtual Lan) eli virtuaalisella lähiverkolla tarkoitetaan lähiverkkoa, joka voi olla hajautettuna useamman verkkolaitteen alueelle. Myös yksi ja sama verkkolaite voi kuljettaa useamman lähiverkon Ethernet-kehyksiä. VLAN lisää näin ollen myös verkon tietoturvaa.

IPv4 (Internet Protocol version 4) on internetin protokollan nykyinen noin 30 vuotta vanha versio. Sen avulla hoidetaan kaikki Internetissä tapahtuva liikennöinti. Protokollan suurimmaksi ongelmaksi nykypäivänä on noussut sen IP-osoitteille varaamat 32 bittiä, jotka eivät enää riitä takaamaan IP-osoitteita kaikille halukkaille.

IPv6 (Internet Protocol version 6) eli Internet protokollan kuudes versio on IPv4-protokollaa korvaamaan kehitetty uudempi versio vuonna 1998. Protokolla mahdollistaa 128 bitin käyttämisen osoiteavaruutena ja mahdollistaa näin suuren määrän osoitteita tulevaisuudessa.

3 Lähtökohdat

Laurean tietoliikennelaboratorio aloitti koulutusyhteistyön Mamentor Oy:n kanssa vuoden 2007 syksyllä. Yhteistyö pitää sisällään lähiopetusta sekä verkkomuotoista kouluttamista. Opetuksessa käytetään MentorAid-verkko–oppimistyökaluja, joiden avulla opiskelija saa käyttöönsä opintojakson materiaalin videomuotoisena, näin opiskelijan on mahdollista opiskella etänä. Opintokokonaisuudet pitävät sisällään teknisiä harjoituksia, jotka toteutetaan MentorAidin virtuaalisessa harjoitteluympäristössä. Lisäksi opiskelijat tekevät verkkoharjoituksia Laurean tietoliikennelaboratorion verkkolaitteilla.

Interconnecting Networks opintojakso pitää sisällään Ciscon CCNA (Cisco Certified Network Associate)-sertifikaatin suorittamiseen liittyvää verkkoteoriaa sekä käytännön harjoituksia. Kurssin teoriaosuus perustuu Ciscon julkaisemiin kahteen ICND (Interconnecting Cisco Network Devices)-kirjaan. Kirjojen uusimmat vuoden 2007 versiot otettiin käyttöön kurssin toteutuksella keväällä 2008. Kurssille vaadittavan opetusmateriaalin tuotti Mamentor Oy. Videopohjainen opetusmateriaali oli opiskelijoiden luettavissa MentorAid-järjestelmän kautta. Kurssiin liittyvät käytännön verkkoharjoitukset tehtiin tietoliikennelaboratorion tiloissa laboratorion käytössä olevilla verkkolaitteilla.

Aiheen opinnäytetyön kehittämiselle sain toimiessani tietoliikennelaboratoriossa harjoittelijana keväällä 2008. Olin mukana omalta osaltani toteuttamassa Interconnecting Networks opintojaksoa. Vastuualueenani opintojaksolla kuului tietoliikennelaboratoriossa tehtävien verkkoharjoituksien läpivienti ja ohjaaminen.

Opintojaksolla käytössä olevat verkkoharjoitukset perustuivat suurimmalta osaltaan Ciscon vanhempiin ICND-kirjoihin sekä Petri Viinikaisen vuonna 2006 opinnäytetyönään tekemiin verkkoharjoituksiin opintojaksoille Lähiverkot sekä Langaton tiedonsiirto ja teletekniikka. Keskustelemalla vastaavien opettajien Riku Salmenkylän, Seppo Koposen sekä yliopettaja Jyri Rajamäen kanssa päätimme, että verkkoharjoitukset on syytä tehdä tuleville opintojakso toteutuksille vastaamaan vuoden 2007 ICND-kirjoissa olevia asioita.

Opinnäytetyön tavoitteeksi muodostui uusien opiskelijoille suunnattujen verkkoharjoituksien kehittäminen Interconnecting Networks opintojakson tuleville toteutuksille. Tarkoituksena oli luoda uudet verkkoharjoitukset siten, että harjoituksien yhtenä lähtökohtana on verkkolaitteiden sekä teoriaosuuden hallitsemisen lisäksi CCNA-sertifikaatin suorittaminen. Uudet harjoitukset oli myös tarkoitus saada vastaamaan uusien ICND-kirjojen aihealueita, muuttamalla harjoituksien sisältöä edellisistä, poistamalla vanhentuneita aihealueita ja lisäämällä uusia asioita mukaan. Harjoituksien oli tarkoitus pitää sisällään ICND-kirjoissa olevat aihealueet, jotta harjoituksia olisi mahdollista toteuttaa käyttämällä tietoliikennelaboratorion käytössä olevia laitteita.

4 Kohdeorganisaatio

4.1 Laurea-ammattikorkeakoulu

Laurea on Suomen neljänneksi suurin monialainen ammattikorkeakoulu, joka toimii Uudellamaalla ja Itä-Uudellamaalla. Toimipisteet ovat Espoossa (Leppävaara ja Otaniemi), Hyvinkäällä, Keravalla, Järvenpäässä, Lohjalla, Porvoossa ja Vantaan Tikkurilassa. Ammattikorkeakoulun johtavia suomenkielisiä koulutusohjelmia on kolmetoista ja

englanninkielisiä kolme. Vuonna 2007 ylempään ammattikorkeakoulututkintoon johtavia suomenkielisiä koulutusohjelmia on kuusi ja englanninkielisiä yksi.

Ammattikorkeakoulututkintoon ja ylempään ammattikorkeakoulututkintoon johtavassa koulutuksessa sekä erikoistumisopinnoissa opiskelee yhteensä 8000 opiskelijaa. Ulkomaisia tutkinto-opiskelijoita on 350 ja vaihto-opiskelijoita vuosittain noin 200. Henkilöstöä Laureassa on noin 500. Laureassa suoritetaan vuosittain noin 1300 ammattikorkeakoulututkintoa, erikoistumisopintoja suoritetaan vuosittain noin 200.

Laurea on tutkiva ja kehittävä, uutta osaamista tuottava ammattikorkeakoulu. Osaamisen kehittäminen eri osaamisalueilla perustuu tutkittuun tietoon. Laurean pedagogisessa innovaatiossa, Learning by developing (LdB)–toimintamallissa lähtökohtana on aidosti työelämään kuuluva, käytäntöä uudistava kehittämishanke, jonka eteenpäinvieminen edellyttää opettajien, opiskelijoiden ja työelämäosaajien yhteistyötä ja jossa parhaimmillaan tuotetaan uutta osaamistietoa.

Laurea toimii eräällä kilpailukykyisimmistä alueista, Helsingin metropolialueella. Metropolialueen innovaatioympäristössä Laurea profiloituu erityisesti aluekehitysvaikutuksen, klusterikehityksen kytketyn t&k-toiminnan, verkosto- ja liiketoimintaosaamisen ja niihin perustuvien toimintamallien sekä hyvinvointialan ja –yrittäjyyden kehittämisessä. (Opetusasiainhallinto 2007, 14;Laurea-ammattikorkeakoulu 2008.)

4.2 Laurean tietoliikennelaboratorio

Tietoliikennelaboratorio on Laurea-ammattikorkeakoulun kehittämisympäristö, jonka tarkoituksena on tarjota oppimisympäristö, jossa opiskelijoilla on mahdollista soveltaa teoriaa käytännössä. Laboratoriossa toteutetaan myös monia projekteja sekä opinnäytetöitä. Tietoliikennelaboratorion asiakkaina toimivat pääosin Laureassa tietoverkkoja opiskelevat opiskelijat, jotka käyttävät laboratoriota hyödyksi verkkokursseihin liittyvien harjoituksien tekemisessä sekä erilaisissa projektitöissä. Tietoliikennelaboratoriossa tehtävät verkkoharjoitukset liittyvät Ciscon laitteiden mm. kytkimien, reitittimien sekä WLAN-tukiasemien konfigurointiin hallintaan sekä vianhakuun.

4.3 Interconnecting Networks-opintojakso

Interconnecting Networks opintojakso on Laurea-ammattikorkeakoulussa järjestettävä opintojakso, jonka tarkoituksena on opettaa tietojenkäsittelyä opiskeleville opiskelijoille perusteet verkkolaitteista ja niiden konfiguroinnista. Opintojaksolla opiskelee suomalaisia ja ulkomaisia opiskelijoita. Opintojakso järjestettiin ensimmäisen kerran keväällä 2007 ja

tulevaisuudessa opintojakso on tarkoitus järjestää kaksi kertaa vuodessa syksyisin sekä keväisin. Opintojakso koostuu luennoista, harjoituksista sekä kokeesta, joka suoritetaan opintojakson lopussa. Opintojakson läpipääsyn edellytyksenä opiskelijoiden on saatava kokeesta vähintään 50 % maksimipisteistä sekä osallistuttava vähintään puoleen tietoliikennelaboratoriossa järjestettävistä verkkoharjoituksista.

Opintojaksoon liittyvä teoriaosuus saadaan Ciscon CCENT/CCNA ICND1-ja ICND2-kirjoista, joiden tarkoitus opettaa CCNA-sertifikaattiin sisältyvät teoriaosuudet. Opintojaksolla opiskelijat käyttävät myös MentorAid-verkko-oppimistyökalua hyväkseen. MentorAid-oppimistyökalu on verkossa toimiva palvelu, josta opiskelijat voivat kuunnella luentoja sekä tehdä verkkoharjoituksia virtuaalisesti. Järjestelmään kirjaudutaan henkilökohtaisesti, minkä avulla järjestelmä seuraa opiskelijoiden aktiivisuutta pitämällä kirjaa luennoista, joita järjestelmän kautta on avattu. MentorAid-ympäristöstä saatavat luennot koostuvat CCNA-sertifikaatin suorittamiseen liittyvistä aihe-alueista. Luennot MentorAid ympäristöön on tuottanut Laurea-ammattikorkeakoulun yhteistyökumppani Mamentor Oy.

Opintojaksolla keskitytään konfiguroimaan erityisesti Ciscon verkkolaitteita IOS-käyttöjärjestelmän avulla. Verkkoharjoitukset koostuvat kytkimien, reitittimien sekä WLAN-tukiasemien konfiguroinnista. Harjoitukset koostuvat Ciscon CCNA-sertifikaatin suorittamiseen liittyvistä aihe-alueista. Harjoitukset suoritetaan Laurean tietoliikennelaboratorion laitteilla.

5 Verkkoihin liittyvää yleistä teoriaa

5.1 OSI-malli

ISO (Internation Standards Organization) kehitti OSI (Open Systems Interconnection) -mallin 1980-luvun alussa. OSI-mallin tarkoituksena oli tarjota ympäristö, jossa eri laitevalmistajat sekä käyttäjät pystyisivät kommunikoimaan keskenään. Eri valmistajien verkkojärjestelmät sekä laitteet oli tarkoitus rakentaa OSI-mallia noudattaviksi, jolloin tietoliikennejärjestelmien osat kommunikoisivat keskenään käyttäen hyväkseen OSI-mallin kerroksien protokollia. (Kaario 2002, 18.)

OSI-malli koostuu seitsemästä kerroksesta, jossa kerroksien tehtävänä on hoitaa kerrokseen kuuluvien protokollien keskinäistä kommunikointia. ISO/IEC-standardissa 7498-1 määritellään OSI-mallin kerroksien tehtävät.

5.1.1 Sovelluskerros (Application layer)

Sovelluskerroksen tehtävänä on määritellä tietokoneohjelmistoille yhtenäinen rajapinta verkkoon, jonka avulla sovellukset kommunikoivat. Yleisimpiä sovelluksia ovat sähköposti, tiedonsiirto tai etäkäyttöohjelmistot. Ohjelmistot käyttävät kommunikoinnissa hyväkseen protokolloa kuten FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) ja Telnet. Sovelluskerroksen protokollat toimivat suorana rajapintana sovelluksen ja tiedonsiirron välillä.

5.1.2 Esitystapakerros (Presentation layer)

Esitystapakerroksen tehtävänä on huolehtia datan ja tiedostojen muutospalveluista sekä tavoista miten data voidaan esittää sovellukselle. Esimerkkinä kuvaformaatit kuten JPG, ASCII tai TIFF käyttävät tätä kerrosta. Myös tietoliikenneverkkojen välinen tiedonsalaus tehdään tässä kerroksessa.

5.1.3 Istuntokerros (Session layer)

Istuntokerroksen tehtävänä on muodostaa ja ylläpitää sovellusten istuntoja, joiden avulla sovellus on yhteydessä verkkoon. Istuntojen kestot, niiden prioriteetit sekä istuntojen keskeyttäminen määritellään tässä kerroksessa. Esimerkkinä Windows XP:ssä käytettävä RPC (Remote Procedure Call) -protokolla, joka hoitaa ohjelmistojen proseduurikutsujen kuljettamista verkon yli käyttää tätä kerrosta hyväkseen.

5.1.4 Kuljetuskerros (Transport layer)

Kuljetuskerros toimii linkkinä ylempien sovelluskerroksien ja alempien datan kuljettamiskerroksien välillä. Kerros huolehtii yhteyden muodostamisesta järjestelmien välillä segmentoimalla ja uudelleen kokoamalla datavirran. Kerros määrittää luotettavan ja epäluotettavan yhteyden. Kerroksessa toimivat protokollat kuten UDP (User Datagram protocol) -protokolla ja TCP (Transmission Control Protocol) -protokolla.

5.1.5 Verkkokerros (Network layer)

Verkkokerroksen tehtävänä on päättää mitä tapaa käytetään datan tiedonsiirrossa ja miten datapaketit ohjataan verkon läpi. Reititys toimii tässä kerroksessa sekä erilaiset laadunvalvontaan liittyvät palvelut sekä vuonvalvontaa. Tärkeimmät protokollat kerroksessa ovat IP-(Internet Protocol) ja X25-protokolla.

5.1.6 Siirtokerros (Link layer)

Siirtokerroksen tehtävänä on huolehtia bittien tasolla luotettavasta siirtämisestä. Kerroksen tehtävä on huolehtia mm. virheistä, verkon topologiasta sekä vuon valvomisesta. Siirtokerros tarjoaa verkkokerrokselle datansiirtoyhteyden, jonka avulla verkkolaitteet keskustelevat keskenään. Siirtokerroksessa toimii myös MAC (Medium Access Control) -protokolla, jonka tehtävänä on siirtokerroksen riittävä jako käyttäjien kesken. Muita kerroksessa toimivia protokollia on mm. Token Ring, Token Bus sekä Ethernet-verkoissa toimiva CSMA/CD (Carrier Sense Multiple Access/Collision Detection) -protokolla.

5.1.7 Fyysinen kerros (Physical layer)

OSI-mallin fyysisen kerroksen tehtävänä on huolehtia bittien fyysisestä siirtämisestä. Näihin kuuluvat siirtotien sähköiset ominaisuudet, liittimet sekä jännitetasot. Kerroksessa tapahtuu siirtonopeuden, siirtoviiveen sekä siirtovirheiden tarkkailu. Kerroksessa määritellään asynkronoitu sekä synkronoitu datansiirto eli pakettilähetyksien erotteleminen toisistaan. Asynkronisessa tavassa pakettien alku ja loppu ilmaistaan sovitulla tavalla kun taas synkronoidussa tavassa käytetään kelloa jakamaan paketit toisistaan. Fyysinen kerros määrittelee mm. parikaapelit, koaksiaalikaapelit sekä optiset valokaapelit. (International Standards Organization 2008.)

5.2 OSI-mallin toiminta

OSI/IEC-standardissa 7498-1 määritellään miten informaation kulku eri tietokoneilla olevien ohjelmien välillä verkon siirtomedian kautta toimii. Kerrokset käyttävät keskinäisessä kommunikoinnissa PDU (Protocol Data Units)-siirtojaksoja. Kahden OSI-mallin kerrosten kommunikoidessa keskenään, kerroksien alapuolella oleva kerros tarjoaa palveluja ylempänä olevalle kerrokselle. OSI-malli estää suoran kommunikoinnin kahden eri kerroksen välillä. OSI-mallin avulla kommunikointi tapahtuu palvelusyhteyspisteiksi (Service Access Point) kutsutussa paikassa.

OSI-mallin kerrokset ovat riippuvaisia niitä alempien kerroksien palveluista. Kerroksien välisesssä kommunikoinnissa alempi kerros käyttää ylemmän kerroksen PDU;n ja asettaa sen oman kerroksensa datakenttään. Tämän jälkeen kerros voi lisätä pakettiin omia tietojaan. Informaation kulussa OSI-mallin kerrosten läpi tapahtuu viisi kapselointitoimintoa.

1 Datan muodostaminen.
2 Datan paketoiminen.
3 Verkko-osoitteen lisääminen otsikkotietoon.
4 Paikallisen osoitteen lisääminen siirtoyhteystason otsikkotietoon.
5 Paketin muuntaminen bittimuotoon siirtoa varten.

Yhtenä yleisimmistä verkon käyttötavoista voidaan pitää selainohjelmiston käyttämistä. Selainohjelmat käyttävät HTML-protokollaan hyväkseen kommunikoidessaan isäntäkoneiden välillä. HTML-protokollan kommunikointi OSI-mallin kerrosten välillä käy seuraavasti, käyttäjän lähettäessä viestin Web-palvelimelle, pyyntö sekä sen sisältämä data muunnetaan dataksi, jota käytetään siirrettäessä dataa tietoverkon yli kohta 1. Kuljetuskerros lisää otsakkeen datan alkuun, joka on tässä tapauksessa TCP, koska kyseessä on HTML-prosessi kohta 2. Verkkokerros lisää dataan otsakkeen, jossa ovat lähde ja kohdeosoitteet, tässä tapauksessa lisätään IP-otsake, jossa kerrotaan lähettäjän IP-osoite kohta 3. Siirtoyhteyskerros muuttaa datan datakehykseksi, jotta laite voi kommunikoida suoraan linkin päässä olevan toisen laitteen kanssa. Kehyksen pitää vastata kohdepäässä olevan laitteen kehystyyppiä. Tässä tapauksessa kehyksenä käytetään Ethernet II-tyyppistä kehystä. Kehys lähetetään paikalliselle reitittimelle ohjattavaksi eteenpäin kohta 4. Fyysinen kerros muuttaa kehyksen nolliksi ja ykkösiksi siirtotie siirtoa varten. Siirtotienä voidaan käyttää monia väyliä esim. lähiverkon kaapeleita, runkolinjoja tai nopeita laajaverkkoja, joiden kautta kehys ohjataan perille kohdeverkkoon. (International Standards Organization 2008.)

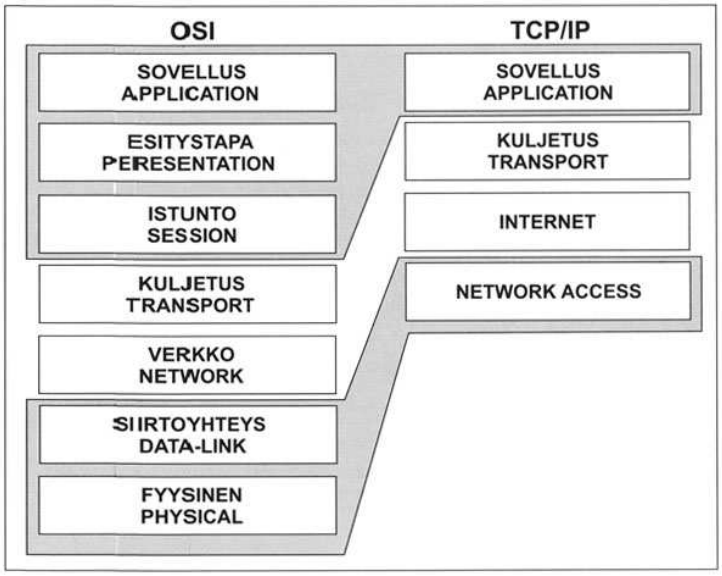
5.3 TCP/IP-protokolla

TCP/IP (Transmission Control Protocol/Internet Protocol) -protokolla kehitettiin alun perin DARPA-järjestön toimesta 70-luvulla. DARPA-järjestö toimii yhdysvaltalaisen puolustusministeriön (Department of Defense) alaisena. Alkuperäinen TCP/IP-protokollan kehitystarkoitus oli tietoliikenneyhteyksien mahdollistaminen DARPA-verkkoon kytkettyjen laitteiden välillä. Alkujaan TCP/IP-protokollaa käytti UNIX:in Berkeley Software Distribution-ohjelmistotalo, jossa protokollaa käytettiin yhdistämään verkossa olevia UNIX koneita toisiinsa. 1970-luvun puolivälissä pakettivälitteinen tekniikka löi itsensä läpi, koska pakettivälitteinen kytkentätapa mahdollisti yritysten kytkeytymisen toisiinsa ilman suoraan yhteyttä tai linkkiä.

TCP/IP-protokollaperhe tukee kolmannen ja neljännen kerroksien määritelmien lisäksi myös sovelluksia kuten sähköpostia, etäkäyttö ja päätteen emulointi ohjelmistoja sekä tiedostonsiirtoon käytettäviä sovelluksia. TCP/IP-protokolla sopii niin LAN kuin WAN-verkkojenkin tietoliikenteen yhdistämiseen. Protokolla koostuu OSI-mallin mukaisesti

kerroksiin pohjautuvasta mallista, mutta kerrokset poikkeavat jonkin verran OSI-mallin vastaavista. (Chappel 2002, 185-186.)

Kuviossa 1 esitellään TCP/IP-protokollan kerrokset. Kuviosta selviää, että TCP/IP-protokollan sovelluskerros vastaa OSI-mallin kolmea ylintä datan käsittelyyn liittyvää kerrosta. Verkkorajapintakerros pitää sisällään OSI-mallin datan fyysiseen siirtämiseen liittyvät kaksi alinta kerrosta. Lisäksi TCP/IP-protokollassa OSI-mallin verkkokerroksesta käytetään nimitystä Internet-kerros.



Kuvio 1: TCP/IP-protokollamallin rakenne (Hakala & Vainio 2005, 184).

5.3.1 Sovelluskerros (Application layer)

TCP/IP-protokollamallin kerroksissa toimivat protokollat määritellään RFC dokumentissa 1122. TCP/IP-protokollan sovelluskerros määrittelee toiminnot, jotka vastaavat OSI-mallin sovellus, esitystapa sekä istuntokerroksien toimintoja. Sovellusten protokollat tiedostonsiirto, sähköposti sekä etäkäyttö sijoittuvat sovelluskerrokselle. Toiminnot voivat sijaita isäntälaitteella tai reitittimellä. TFTP (Trivial File Transfer Protocol) ja FTP (File Transfer Protocol) -protokolla ovat esimerkkejä protokollista, jotka mahdollistavat etäkäytön sovelluskerroksella.

5.3.2 Kuljetuskerros (Transport layer)

Kuljetuskerroksessa toimii kaksi tärkeää protokollaa TCP (Transmission Control Protocol) ja UDP (User Datagram Protocol) –protokolla. Näiden kahden protokollan avulla suoritetaan tiedonsiirto verkossa. Suurimpana erona protokollien välillä voidaan pitää sitä, että TCP-protokolla on yhteydellinen protokolla. TCP-protokollaa voidaan pitää luotettavana protokollana, joka varmistaa pakettien toimittamisen perille käyttämällä kättelymenetelmää (acknowledgments). UDP-protokolla toimii yhteydettömästi eikä käytä kuittausmenetelmää, minkä johdosta se on nopea ja tehokas protokolla. UDP-protokolla jättää luotettavuuden varmistamisen ylempien kerroksien tai vastaavasti virheensietävän sovelluksen tehtäväksi.

5.3.3 Internet kerros (Internet layer)

TCP/IP-protokollan Internet kerros vastaa OSI-mallin verkkokerrosta toimintamallin perusteella. Kerroksen tehtävänä on vastata pakettien kuljettamisesta verkon läpi. Internet kerroksella toimii kaksi tärkeää protokollaa IP (Internet Protocol) -protokolla, jonka tehtävänä on mahdollistaa yhteydetön paras mahdollinen yritys (best effort) periaatteella ja siirtää tietosähkeet kohteeseensa. ICMP (Internet Control Message Protocol) -protokollan tehtävänä on mahdollistaa hallinta ja viestintätoiminnot. ICMP-protokolla kuljettaa viestit IP-tietosähkeiden mukana. Yleisimpiä ICMP-viestejä ovat mm. kohde tavoittamaton (Destination Unrachable), ajan umpeutumiseen liittyvä (time exceeded), sekä tavoitettavuuteen liittyvät (echo) ja (echo reply) -viestit.

5.3.4 Verkkorajapintakerros (Network Interface layer)

Verkkorajapintakerros määrittelee siirtoyhteyden ominaisuudet ja miten siirtotietä käytetään. Verkkorajapintakerros toiminnot vastaavat OSI-mallin siirtoyhteyskerroksen sekä fyysisen kerroksen toimintoja. Kerroksien toimintoja ei ole tarkemmin määritelty, vaan näillä kerroksilla voidaan käyttää monia eri protokollia. (Internet Engineering Task Force 1989.)

5.4 TCP/IP-protokollan toiminta

RFC-dokumentissa 1122 määrittellään miten TCP/IP-kerrokset toimivat keskenään. TCP/IP-protokollakerrosten toiminta perustuu kehysrakenteisiin. TCP/IP-protokollaa käyttävän sovelluksen lähetys alkaa kun FTP ohjelma tai internet selain lähettää bittejä siirrettäväksi protokollapinolleen. Datasta riippuen data voidaan joutua muuttamaan eri muotoon, data voidaan mm. joutua salaamaan, pakkaamaan tai muuntamaan eri maiden merkistöille sopivaan muotoon. Sovelluskerroksen protokolla toimii näin ollen rajapintana sovelluksen ja

protokollapinon välillä. Datan saavuttua TCP-kerrokselle, TCP-protokolla segmentoi datan ja lähettää sen eteenpäin IP-kerrokselle. Segmenttien koot riippuvat sovelluksesta, TCP-protokolla voi pilkkoa datan pieneen segmenttiin ja lähettää sen nopeasti jos sovellus näin vaatii. TCP-protokolla kopio segmentit muistiinsa, jotta data voidaan uudelleen lähettää tarvittaessa. Tätä varten TCP-protokolla numeroi kehykset sekä laskee niille tarkistussumman, jotta korruptoituneet kehykset voidaan havaita.

IP-kerros ottaa vastaan TCP-kerrokselta lähetetyn datasegmentin ja voi tarvittaessa myös pilkkoa dataa jos datasegmentti on liian suuri lähetettäväksi eteenpäin. IP-kerros varustaa IP-paketin osoitetiedoilla, joiden avulla verkon laitteet ohjaavat paketin oikeaan osoitteeseen. Tämän jälkeen segmentti lähetetään verkon kautta vastaanottajalle. TCP-segmentin vastaanottajatahon isäntäkone voi joutua kokoamaan segmenttien järjestystä oikeaksi, jos sanomien järjestys on verkossa sekaantunut. Segmenttien järjestyksen ollessa oikea, data pilkotaan vastaanottopään sovellukselle sopivan mittaisiksi kokonaisuuksiksi. Viimeisessä vaiheessa verkkosovellus purkaa segmentin salauksen tai pakkauksen, jos data käyttää niitä. Datan purkamisen jälkeen data lähetetään vastaanottavalle sovellukselle käsiteltäväksi. (Internet Engineering Task Force 1989.)

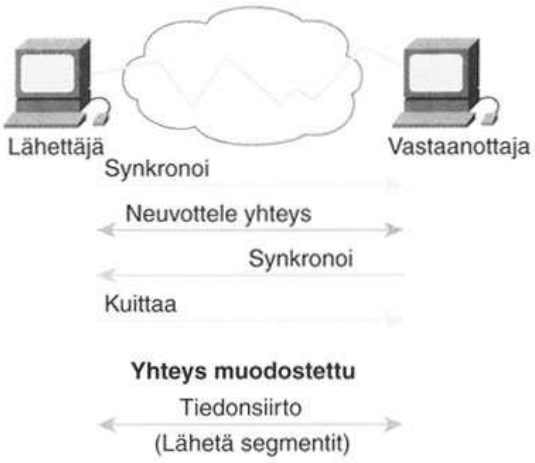
5.5 TCP-protokollan käyttämä kolmitiekättely menettely

RFC-dokumentin 1122 kohdassa 4.2 käsitellään TCP/IP-protokollan välistä kommunikointia. Protokolla käyttää kommunikommunikoidessaan ns. kolmitiekättelyä hyväkseen. Kolmitiekättely perustuu kahdenlaiseen numerointiin. Yhteys avataan lähettäjän lähettäessä avauspyynnön, jossa kulkee mukana lähetyksen järjestysnumero. Lähetyksen vastaanottaja vastaa tähän sanomaan kuittauksella, jossa kerrotaan mihin sanomaan kuittaus liittyy. Vastaussanomaan sisällytetään oma sanomanumero ja lähetetään takaisin lähettäjälle. Vastaussanoma kuitataan ensimmäinen dataa sisältävän sanoman mukana, tai erillisellä kuittaussanomalla.

TCP-kehyksessä on neljä kenttää, joita käytettään yhteydenmuodostuksessa. Näitä ovat SYN (synchronize) ja ACK (acknowledgment) -bitit sekä järjestys ja kuittaus numerot. Yhteyttä avattaessa lähettäjä lähettää sanoman, jossa SYN-bitti saa arvon 1 muiden bittien ollessa nollia. Vastapuoli lähettää omassa vastaussanomassaan sanoman jossa SYN-sekä ACK-bitit ovat ykkösiä ja kuittausnumero yhtä arvoa suurempi kuin lähetysviestissä. Lähettäjä osapuoli vastaa tähän vastausviestiin sanomalla, jossa ainoastaan ACK-bitti saa arvon yksi.

Tämän jälkeen alkaa varsinainen datan lähetys, jossa kaikissa käytetään ACK-bitin arvona ykköstä. Lähetettävän datan määrää käytettävä ikkunan koko, joka parantaa vuon valvontaa sekä luotettavuutta. Lähettäjän ja vastaanottavan koneen välillä välitetään tietoa

vastaanottoikkunan suuruudesta. Lähetyksen aikana tarkkaillaan myös verkon viivettä ajastimien avulla. TCP/IP-kättelyprosessin kulku vaiheittain on esitetty kuvassa 1.



Kuva 1: TCP/IP-protokollan kättely prosessi (Cisco Systems 2002, 28).

Yhteyden purkamiseen voidaan käyttää kolmea eri tapaa. Äkillinen purkaminen tapahtuu yhteyden tarjoajan katkaistaessa yhteyden ilman ennakkovaroitusta. Normaali yhteyden purkaminen tapahtuu sanomien lähettämisen jälkeen, jolloin yhteys katkaistaan välittömästi. Neuvoteltu yhteyden purkaminen tapahtuu sanomien lähettämisen jälkeen, mutta toisella osapuolella on oikeus kieltäytyä katkaisemasta yhteyttä. Normaalissa yhteydenpurkamisessa dataa voidaan menettää, jos yhteydenpurku tulee toiselle osapuolelle huonoon aikaan.

TCP-protokolla on sopiva protokolla käyttää kun halutaan varmistaa datan perillemeno, koska protokollalla on käytössään mekanismit rajoittaa nopeutta ongelmatilanteissa. Reaaliaikaisuuteen perustuvaan datansiirtoon TCP-protokolla ei sovellu, koska protokolla ei pysty lähettämään ryhmä tai joukkolähetyksiä. Tätä tarkoitusta varten UDP-protokolla on parempi vaihtoehto. (Internet Engineering Task Force 1989.)

5.6 IPv4-osoitteet ja osoiteluokat

Internetiin kytketyt laitteet erotellaan toisistaan IP-osoitteilla. IP-osoitteita jakavat kansainvälisellä tasolla IANA (Internet Assigned Numbers Authority) sekä maakohtaisesti teleoperaattorit (Internet Service Provider, ISP), julkiset organisaatiot tai korkeakoulut. Internet osoiteavaruus jaetaan osoiteluokkiin, joiden avulla määritellään käytettävissä oleva konemäärä sekä esimerkiksi käyttötarkoitus.

IP-osoite voidaan määritellä koneelle kiinteästi verkko asetuksen tekemisen yhteydessä tai verkossa oleva palvelin voidaan määritellä toimimaan DHCP (Dynamic Host Configuration Protocol) -palvelimena, joka jakaa IP-osoitteita määritetyn osoiteavaruuden sisältä. IP-osoite varataan yhdelle koneelle kerrallaan käyttöön sen tarvitsemaksi ajaksi. Tämän jälkeen IP-osoite voidaan vapauttaa toisen laitteen käyttöön. (Hakala & Vainio 2005, 191.)

RFC dokumentti 790 määrittelee IPv4 verkon osoitteen rakenteen. IPv4-osoite koostuu verkkotunnisteosasta (network identifier) sekä konetunnisteosasta (host identifier), joita käsitellään binäärilukusarjoina. IPv4-osoite muodostuu 32-bitistä, jotka jaetaan neljään kahdeksan bitin pituiseen kenttään (octet). Koko IP-osoiteavaruus jaetaan osoitesarjoihin, jotka puolestaan jaetaan osoiteluokkiin A-luokasta E-luokkaan. Osoiteluokka A sisältää osoitteet väliltä 000.000.000.000–127.255.255.255, osoiteluokka B-osoitteet 128.000.000.000–191.255.255.255 ja osoiteluokka C-osoitteet 192.000.000.000–223.255.255.255. Osoiteluokan D-osoitteet väliltä 224.000.000.000–239.255.255.255 on varattu Multicast-osoitteille ja osoiteluokan E-osoitteet väliltä 240.000.000.000–255.255.255.255 testauskäyttöön. Näitä osoitteita ei käytetä normaaleissa Unicast-lähetyksissä verkossa.

IPv4-osoiteavaruus sisältää myös erikoisosoitteita, jotka eivät ole käytössä reitityksessä. Näihin kuuluvat intranet verkkoihin varatut privaatit osoitteet väliltä 10.0.0.0-10.255.255.255, 192.168.0.0–192.168.255.255 sekä 172.16.0.0.–172.31.255.255. Poikkeuksia ovat osoite 0.0.0.0, jota ei enää käytetä reitityksessä sekä osoitteet väliltä 127.0.0.0–127.255.255.255, jotka toimivat ns. loopback-osoitteina. Loopback-osoite 127.0.0.1 viittaa takaisin itse laitteeseen, josta käytetään nimitystä localhost. Tätä osoitetta voidaan käyttää hyväksi esimerkiksi vianhakuun liittyvissä tilanteissa, jossa testataan koneen oman TCP/IP-protokollan toimivuutta verkkokortissa.

A-luokan osoitteita on käytössä 254 kappaletta, joista jokainen tukee yli 16 miljoonaa isäntäkonetta. B-luokan osoitteita on 64.000 kappaletta, jotka tukevat 64000 isäntää ja C-luokan osoitteita on käytössä yli 16 miljoonaa, jotka tukevat korkeintaan 254 isäntäkonetta. Näihin osoitteisiin liittyen on kehitetty ns. ensimmäisen oktetin sääntö, jolloin osoitteen luokka voidaan tunnistaa ensimmäisen oktetin numeerisesta arvosta. Esimerkiksi osoite 192.0.0.1 edustaa C-luokan osoitetta ensimmäisen oktetin arvon 192 perusteella. Reitittimen lukiessa osoitetta se käyttää tätä oktettia tunnistaakseen osoitteesta sen luokan mihin osoite kuuluu. Osoiteluokan selvittyä reititin tietää montako bittiä osoitteesta kuuluu verkko-osaan ja montako bittiä host osaan ja pystyy tämän tiedon perusteella reitittämään osoitteen oikeaan verkkoon, jos lisäbittejä ei ole tunnistettavissa. (Internet Engineering Task Force 1981a.)

5.6.1 Aliverkkomaskin käyttö

Aliverkkomaskia käytetään IP-osoitteen rinnalla erottelemaan verkko-osoitteen bitit ja koneen osoitteen bitit toisistaan. Aliverkkomaskin avulla raja voidaan määrittää mihin tahansa kohtaan verkko-osoitetta. Aliverkkomaskin avulla mahdollistetaan suurten osoiteluokkien jako pienemmiksi verkoiksi. Tätä toimenpidettä kutsutaan aliverkottamiseksi. Sekä päinvastaista toimenpidettä yliverkotusta, jolla mahdollistetaan osoitesarjojen yhdistäminen suuremmiksi verkoiksi. Aliverkotuksen avulla mahdollistetaan yhden verkon jakaminen pienempiin osiin kahdella tavalla. Perinteiselle luokka jakoon perustuvalla tavalla (Class based sub-netting) sekä luokattoman CIDR (Classless Inter-Domain Routing) -menetelmän avulla, jossa useammasta osoitesarjasta luodaan yksi näennäisesti yhtenäinen verkko. (Hakala & Vainio 2005, 196.)

5.6.2 Luokallinen aliverkotus

Luokallinen aliverkotus määritellään RFC dokumentissa 791. Luokallisessa aliverkotuksessa IP-osoite jaetaan aliverkkomaskin avulla kahteen osaan aliverkon tunnistavaan osaan sekä konetunnisteeseen. Aliverkkomaski muodostaa yhtenäisen ykkösbittien ketjun osoitteen alusta koneosoitteeseen alkuun asti, jolloin osoitteen verkko-osa määritys päättyy aliverkkomaskin viimeiseen ykkösbittiin. Aliverkkomaski voidaan esittää niin binääri kuin desimaalimuodossa. Esimerkiksi C-luokan verkko-osoite 200.1.1.0 voidaan aliverkottaa kahteen aliverkkoon käyttämällä aliverkkomaskia 255.255.255.128, tässä tapauksessa aliverkkojen osoitevälit olisivat 200.1.1.1–200.1.1.126 sekä 200.1.1.128–200.1.1.254. Kaikissa aliverkoissa ensimmäistä osoitetta, tässä tapauksessa osoitetta 200.1.1.0, jossa kaikki bitit ovat nollia, käytetään aliverkon verkko-osoitteena (network address). Vastaavasti osoitetta 200.1.1.1.255, jossa kaikki bitit ovat ykkösiä, käytetään aliverkon yleislähetysosoitteena (Directed Broadcast Address). (Internet Engineering Task Force 1981b.)

Vanhemmat käyttöjärjestelmät eivät käytä hyväkseen aliverkotuksessa käytettävien aliverkkojen ensimmäistä aliverkkoa eivätkä viimeistä aliverkkoa, koska ne vastaavat aliverkottoman C-luokan verkko-osoitetta ja yleislähetysosoitetta. Tämä asia on korjattu nykyisin ja kaikki uudemmat reitittimet ja IOS-versiot tukevat näihin aliverkkoihin kohdistuvaa reititystä. (Hakala & Vainio 2005, 198-199.)

5.6.3 Luokaton aliverkotus (Classless Inter-domain routing, CIDR)

Luokaton aliverkotus, jota kutsutaan myös lyhenteellä CIDR, sen toiminto määritellään RFC dokumentissa 1518. Luokattomalla aliverkotuksella tarkoitetaan konseptia, jolla IP-osoitteiden luokkarajat ovat poistuneet ja IP-osoitteet toimivat luokattomasti. Luokaton IP-osoite voi toimia aliverkkomaskin avulla pienessä aliverkossa, vaikka se kuuluisi A-luokan osoitteisiin luokkajaon perusteella. Luokattoman aliverkotuksen avulla reititystaulun kokoja voidaan pienentää huomattavasti yhdistämällä reititystaulun rivejä aliverkkomaskin avulla. Ennen luokattoman aliverkotuksen käyttöönottoa yksittäinen reititystaulussa ollut reitti varasi reititystaulusta yhden rivin. Esimerkiksi aliverkko 10.1.3.0 aliverkkomaskilla 255.255.255.0 ja aliverkko 10.1.0.0 aliverkkomaskilla 255.255.0.0 voidaan esittää reititystaulussa yhdellä rivillä. Tällöin verkko 10.1.3.0 voidaan esittää verkon 10.1.0.0 alaisena mainostuksena, koska osoitteet sisältävät saman IP-osoitteen kaksi ensimmäistä oktettia 10 ja 1.

Toinen etu luokattomien aliverkkomaskien käytöstä on IPv4-osoitteiden jakaminen, niin ettei asiakasyrityksille tarvitse luovuttaa enemmän osoitteita mitä yrityksellä on tarvetta. Esimerkiksi tapauksessa, jossa yritys A tarvitsee 8 osoitetta ja yritys B 28 osoitetta. Luokattoman aliverkotuksen avulla käytössä olevan C-luokan osoite 197.15.8.0, voidaan jakaa yritysten kesken siten, että A yritys saa 197.15.8.16 verkosta aliverkkomaskilla 255.255.255.240 osoitteet 197.15.8.17–197.15.8.30 ja yritys B saa verkosta 197.15.8.32 aliverkkomaskilla 255.255.255.224 osoitteet 197.15.8.33–197.15.8.62. Tätä menetelmää käyttäen säästetään huomattava määrä osoitteita, koska verkosta 197.15.8.0 jää iso määrä osoitteita jaettavaksi muille yrityksille. Ilman luokatonta reititystä edellä mainitut kaksi yritystä käyttäisivät kahdestaan kaikki verkko-osoitteet kyseisestä C-luokan verkosta. Luokattoman aliverkotuksen ansioista esimerkiksi Internetin käytössä olevien reitittimien reititystaulun kokoja on voitu pienentää yli 200.000 reitillä vuoteen 2007 mennessä. (Internet Engineering Task Force 1993.)

Luokatonta aliverkotusta tukevat kaikki nykyiset reititysprotokollat, lukuun ottamatta vanhinta RIPv1-protokollaa. Luokattoman reitityksen onnistumisen edellytyksenä ovat aliverkkomaskin tarkistaminen osoitetta kohden, jolloin aliverkkomaskin siirto täytyy tapahtua IP-osoitteen siirron yhteydessä. Toinen seikka liittyy reititystaulun läpikäyntiin. Nykyiset reititysprotokollat tarkistavat reititystaulun reitit ylhäältä alaspäin siten, että eniten ykkösbittejä sisältävät reitit luetaan ensimmäisinä. Jolloin edellä mainittuja yhdistettyä reittejä ei jäisi käsittelemättä. (Kaario 2002, 86.)

6 Lähiverkko (Local Area Network, LAN)

Lähiverkot on suunniteltu maantieteellisesti pienten alueiden verkoiksi, jotka mahdollistavat useiden käyttäjien yhtäaikaiset yhteydet nopean kaistanleveyden väylään. Lähiverkossa laitteet sijaitsevat fyysisesti lähellä toisiaan ja niiden hallinta tapahtuu paikallisesti. Lähiverkko toimii normaalisti yhden rakennuksen sisällä, mutta sovellusten nopeuduttua suuret lähiverkot jaetaan nykyisin esim. kerrosten tai yhtiön eri osastojen välisiksi pienimmiksi lähiverkoiksi. Näiden hdistämiseen käytetään reititintä. Yrityksen lähiverkkojen hallinta voidaan jakaa yhdelle taholle tai vastaavasti jokaisella lähiverkolla voi olla omat ylläpitäjänsä.

Lähiverkko koostuu verkkolaitteista, kuten kytkimistä, jotka yhdistävät verkon osia ja suodattavat liikennettä sekä reitittimistä, jotka mahdollistavat verkkojen välisen toiminnan. Yleisimpiä lähiverkkotekniikoita ovat Ethernet, Token Ring sekä FDDI, näistä Ethernet-tekniikkaa käytetään suurimmassa osassa nykyajan lähiverkkoja. (Chappel 2002, 7-8.)

6.1 Ethernetin kehitys

Hannu Jaakohuhta teoksessaan Ethernetin lähiverkot käy läpi Ethernetin historiaa, jota voidaan pitää noin 30 vuoden ikäisenä. Kehityksen alkuvaiheessa tekniikkana käytettiin 4800 kbs nopeudella toimivaa radiotietä käyttävää tekniikka. Nykypäivänä puhutaan 10000 Mbps jopa 100000 Mbps eli 100 Gbps siirtonopeuksiin yltävistä tekniikoista, jotka toteutetaan käyttämällä valokuitutekniikkaa. Ethernet on nykypäivänä maailman yleisin lähiverkkotekniikka. Ethernet perustui Havaijin yliopisto kehittämään ALOHA-verkkoon, joka toimi radioteitse Havaijin yliopiston kampuksen IBM-360 järjestelmän sekä ympäröivillä saarilla ja laivoissa olevien tukiasemien välillä. Järjestelmä perustui kilpavaraus tekniikkaan.

Varsinainen Ethernet sai alkunsa vuoden 1972 alussa Robert Metcalfen toimesta, hänen tehtävänään oli liittää Xeroxin ALTO-tietokone ARPANET-verkkoon. Vuoden 1973 keväällä ALTO ALOHA-verkko, kuten sitä kutsuttiin toimi ensimmäisen kerran ja siitä tuli maailman ensimmäinen lähiverkko, joka toimi tietokonelaitteiden välisessä tiedonsiirrossa. Verkko sai tuolloin myös uuden nimen Ethernet, joka toimi tuolloin 2,94 Mbps vauhdilla.

Ethernetin erottuminen 1970-luvun lopulla muista kilpailevista lähiverkkotekniikoista, johtui siitä, että Metcalfen tavoitteena oli kehittää Ethernetistä teollisuusstandardi, joka ei olisi sidottuna mihinkään valmistajakohtaiseen standardiin. IEEE (Institute of Electrical and Engineers) julkaisi vuonna 1983 Ethetnet standardin, jonka nimeksi määriteltiin IEEE 10Base5.

Ethernetin kansainvälisen standardin julkaisi ISO (International Standard Organization) vuonna 1989 numerolla ISO 88023.

Ethernetistä on historian aikana julkaistu monia eri standardeja perustuen eri nopeuksille ja tekniikoille. Vuonna 1984 standardoitiin ohut Ethernet 10base2-nimellä, joka perustui ohuen kaapelin käyttöön sekä verkkokorteissa sisäänrakennettuun transceiveriin. Vuonna 1986 standardoitiin 1 Mbps Ethernet nimellä 1Base5 ja vuonna 1990 standardoitiin 10 Mbps Etherhet nimellä IEEE 802.3i (toiselta nimeltään 10Base-T). Nykypäivänä yleisin 100 Mbps Ethernet standardoitiin vuonna 1995 nimellä IEE 802.3u (toiselta nimeltään 100Base-TX ja 100Base-FX), jota käytetään vielä yleisesti nykypäivänäkin. Nykyisin yleisin käytössä Ethernet nopeusluokka Gigabitin Ethernet standardointiin vuonna 1998 nimeltään (1000-Base-LX) sekä (1000 Base-SX). (Jaakohuhta 2002, 9,11-15,19-20,23,30-31.)

6.2 Ethernetin toiminta

Ethernetin perusperiaate on sen tiedonvälitysmekanismi, miten dataa voidaan välittää lähiverkoissa kytkettyjen laitteiden välillä. IEEE standardi 802.3 määrittelee Ethernetin toiminnan. Ethernetissä datan siirrosta vastaa MAC (Media Access Control) -protokolla, joka siirtää tietoa laitteiden MAC-osoitteiden perusteella. Ethernetissä kulkevia sanomia kutsutaan kehyksiksi (frames), jotka jaetaan toiminnan perusteella kolmeen eri luokkaan, Unicast, Multicast sekä Broadcast-kehyksiin.

Unicast-kehyksissä käytetään yksilöllistä lähde ja kohdeosoitetta. Osoitekentän tunnisteosassa vähiten merkitsevän bitin LSB (Least significant bit) -bitin tunnisteena käytetään arvoa 0. Suuri osa lähiverkoissa kulkevasta liikenteestä tapahtuu Unicast-kehyksen sisällä, koska Unicast- sanomat kulkevat ainoastaan lähettäjän ja vastaanottajan välillä.

Multicast-kehyksissä LSB bitin tunnisteena käytetään arvoa 1. Multicast-lähetykset kulkevat yhdeltä lähettäjältä tietylle joukolle. Tämäntyyppisestä lähetystavasta on hyötyä etenkin videoneuvottelusovelluksissa ja erilaisissa työryhmäsovelluksissa.

Broadcast-kehykset lähetetään kaikille laitteille samalla levitysviestialueella (Broadcast Domain), tämä saadaan aikaan muuttamalla vastaanottajan osoite heksadesimaalimuotoon FF:FF:FF:FF:FF:FF, lisäksi osoitebitit ovat ykkösiä. Broadcast-kehyksiä käytetään mainostamis (advertise) tarkoituksissa, jolloin palvelimet ja sovellukset käyttävät Broadcast-viestejä mainostamaan verkossa oloaan.

Ethernet-verkossa lähetys perustuu CSMA/CD (Carrier Sense Multiple Access/Collision detection) -menettelyyn, joka toimii varsin yksinkertaisella periaatteella. Koneen lähettäessä dataa tarkistetaan ennen lähetyksen alkamista, onko verkon tila vapaa (carrier sense). Verkon ollessa vapaana, kone aloittaa lähetyksen (multiple access), mutta jatkaa edelleen lähetyksen aikana verkon tilan tarkkailua. Kahden koneen lähettäessä samaan aikaa dataa, tapahtuu verkossa kehyksien törmäys (collision). Lähettävän koneen huomatessa törmäyksen (collision detection), kone lähettää törmäyssignaalin verkon kaikille koneille, jolloin koneiden kesken arvotaan uusi lähetysaika. Tämän tarkoituksena on estää koneiden yhtäaikainen kehyksien lähetys, jolloin vain yksi kone voi kerrallaan käyttää siirtotietä hyödykseen. (Internet Engineering Task Force 2008.)

6.3 Lähiverkon kaapelointi

Kaapeloinnin avulla verkon laitteet kuten työasemat, palvelimet sekä tulostimet liitetään verkkolaitteisiin. Kaapelointi toimii tiedonsiirtoreittinä verkkolaitteiden, päätelaitteiden ja palveluiden välillä. Ethernet-verkoissa voidaan käyttää monenlaisia kaapeleita, riippuen verkon toiminnasta ja määrittely tavoista. Ethernet-verkoissa käytettävät kytkennät tehdään nykypäivänä käyttäen koaksiaalikaapelia, parikaapelia tai valokaapelia. Lähiverkoissa olevat laitteet muodostavat tietyn topologian kytkentänsä perusteella. Yleisimmät lähiverkossa käytetyt topologiat ovat tähti, väylä, mesh sekä rengastopologia. (Jaakohuhta 2002, 35.)

6.3.1 Tähtitopologia

Vuonna 2002 julkaistussa Ciscon verkkoakatemia teoksessa käsitellään verkkojen eri topologioiden toimintaa. Tähtitopologian muotoon kytketyillä laitteilla on keskuslaite, johon kaikki laitteet kytketään. Keskuslaitteena käytetään yleensä kytkintä tai reititintä. Keskuslaitetta käytetään ohjaamaan dataa lähettävän laitteen ja vastaanottavan laitteen välillä. Tällä tavoin kytketyt laitteet ovat hyvin vikasietoisia, jolloin yhden yhteyden katkeaminen vaikuttaa ainoastaan kyseessä olevan yhteyden katkeamiseen. Keskuslaitteen hajoamisen vaikutus heijastuu vastaavasti koko verkon alueella. Tähtitopologian muotoon kytkettyjen laitteiden asennus ja ylläpito on helppoa ja vianselvitys on mahdollista tehdä keskitetysti. Hyvinä puolina voidaan pitää myös joustavuutta sekä kaapeloinnin selkeyttä, haittapuolena ovat kustannukset, jotka nousevat korkeiksi kaapeloinnin ja keskuslaitteen kustannusten takia.

6.3.2 Väylätopologia

Väylätopologiassa verkon laitteet kytketään peräjälkeen samaan väylään. Väylän alku ja loppupäähän asennetaan päätevastukset, jotta signaali ei heijastu kaapelin päästä takaisin ja aiheuta häiriöitä kaapelissa. Ilman päätevastuksia verkko on käytännössä käyttökelvoton liiallisista häiriöistä johtuen. Väylätopologian etuina ovat edullisuus ja helppo asennettavuus, haittapuolena ovat vikasietoisuus, jota väylämuotoisessa kytkentätavassa ei ole. Väylään kytketyissä laitteissa yhden laitteen hajoaminen vaikuttaa tällöin koko verkon toimintakykyyn. Hitaus on myös väylämuotoisten verkkojen ongelma törmäyksistä johtuen, jota aiheutuu kahden laitteen lähettäessä yhtäaikaista dataa. Kilpavaraus tekniikka (CSMA/CD) -tekniikka kehitettiin estämään väylämuotoisen verkon törmäyksiä.

6.3.3 Mesh–topologia

Mesh–topologia on suurten verkkojen kytkentätapa. Mesh-rakenteen verkkotopologiassa kaikki laitteet kytketään toisiinsa, jolloin verkosta tulee hyvin vikasietoinen ja luotettava. Yhden laitteen hajoamisella ei ole vaikutusta verkon toimintaan, koska paketti käyttää tässä tapauksessa toista laitetta liikenteen ohjauksessa. Topologian huonoina puolina ovat kallis hinta ja huono hallittavuus. Verkon ylläpitäjältä vaaditaan myös kokemusta Mesh-topologiasta, koska verkon hallinta on monimutkaista.

6.3.4 Rengastopologia

Rengastopologiassa verkon laitteet muodostavat renkaan keskenään, jossa kaikki verkkolaitteet kytketään toisiinsa. Rengastopologian etuina ovat hyvä tehokkuus ja verkkoresurssien pääsyn tasa-arvoisuus kaikille laitteille. Signaalin voimakkuus pysyy rengastopologiassa hyvänä, koska jokainen verkkolaite generoi signaalin uudestaan, sen kulkiessa laitteen läpi. Haittapuolena ovat huono vikasietoisuus, jolloin yhden laitteen vikaantuessa koko verkko muuttuu toimintakyvyttömäksi. Rengasmuotoisessa topologiassa verkkoon tehdyt muutokset vaikuttavat koko verkon toimintaan, jolloin yhden laitteen lisääminen tai poistaminen muuttaa verkon toimintakyvyttömäksi. (Cisco Systems 2002, 419-422.)

6.3.5 10BASE2 (Thin Ethernet) -kaapelointi

Kaikki Ethernet verkoissa käytettävät kaapelointitavat on määritelty IEEE standardissa 802.3. 10 Base2-kaapelointijärjestelmät perustuvat koaksiaalikaapeleihin. Kaapelointia käytetään pienten yritysverkkojen kaapeloinnissa. Koaksiaalikaapeli on noin 5mm paksuista yleensä

harmaan väristä kaapelia. Kaapelissa voi olla maksimissaan 30 laitetta segmenttiä kohden, jonka maksimipituus on 185 metriä. Kaapelilla voidaan saavuttaa 10Mbps siirtonopeus. (Internet Engineering Task Force 2005a.)

6.3.6 10BASE5 (Thick Ethernet) -kaapelointi

10 BASE5 kaapelointia käytetään yleisesti runkoverkkojen rakentamisessa sekä olosuhteissa, jotka vaativat raskasta kaapelointia, koska kaapeli on melko kallista valmistaa. 10 BASE5-kaapelointi perustuu koaksiaalikaapelin käyttöön, jonka ulkovaipan väri on keltainen. Kaapelilla voi kytkeä maksimissaan 100 laitetta, laitteiden etäisyyksien ollessa vähintään 2.5 metriä. Ilman vahvistimia kaapelilla päästään 500 metrin segmentin pituuteen. Kaapelilla voidaan saavuttaa 10Mbps siirtonopeus. Nykypäivänä 10BASE2 sekä 10BASE5 kaapeloinnilla rakennetut verkon ovat harvinaisia ja niiden valmistaminen ja rakentaminen on lopetettu. Nykypäivänä verkon ylläpitäjä voi joutua edellisten kaapelointien kanssa tekemisiin ainoastaan ylläpito tai korjaus tehtävissä. (Internet Engineering Task Force 2005a.)

6.3.7 10BASE T-kaapelointi

10BASE T kaapelointi rakennetaan käyttäen parikaapelia (UTP, Unshielded Twisted Pair). Niillä rakennetut verkot ovat tähtitopologian tai laajennetun tähtitopologian mukaisia. Verkon keskellä käytetään laitteita yhdistämässä, joko kytkintä tai reititintä. 10 BASE T-kaapelointiin perustuvalla parikaapelilla päästään 10Mbps nopeuteen ja sen maksimipituus voi olla 100 metriä. (Internet Engineering Task Force 2005a.)

6.3.8 100 BASE T (Fast Ethernet) -kaapelointi

Fast Ethernet kaapelointi perustuu parikaalin käyttöön. Suurin eroavaisuus on parikaapelin laadulla, jonka ansioista kaapeloinnilla päästään 100 Mbps nopeuteen. 100 BASE TX ja 100 BASE T4 ovat variaatioita 100 BASE T-kaapeloinnille. 10 BASE TX on suosituin 100 BASE T variaatio, jossa käytetään CAT 5 kategorian parikaapelia. Kaapeleista on käytössä yhtä aikaa kaksi paria. 100 BASE T4-kaapeloinnissa käytetään kategorian 3 kaapelia, josta käytetään kaikkia neljää johdin paria yhtä aikaa. 100 BASE VG-AnyLAN-kaapeloinnin kehitti Hewlett Packard, tekniikka perustuu kategorian 3,4 tai 5 kaapeleille ja sitä käytetään Ethernet tai Token Ring-verkkossa. Tekniikalla päästään 250 metrin maksimi etäisyyteen. (Internet Engineering Task Force 2005b.)

6.3.9 1000 BASE T (Gigabit Ethernet) -kaapelointi

1000 BASE T Gigabitin Ethernet kaapelointi perustuu parikaapeliin. 1000 BASE T-kaapeloinnissa suositellaan käytettäväksi CAT 5 tai CAT 6 tason kuparikaapelia. Kaapeleista käytetään tällöin kaikkia neljää johdin paria yhtä aikaa. Tekniikalla saavutetaan 1000 Mbps nopeus ja 100 metrin maksimi etäisyys. (Internet Engineering Task Force 2005c.)

6.4 Lähiverkon laitteet

6.4.1 Keskitin (Hub)

Keskittimet toimivat lähiverkon keskipisteessä, josta yhdistetään verkon eri kaapelointitopologiat. Keskittimet jakautuvat kolmeen eri päätyyppiin, aktiivisiin, passiivisiin ja älykkäisiin. Passiivinen keskitin ottaa vastaan informaatiota yhdestä portista ja lähettää informaation toisesta portista eteenpäin toimien vain kahden pisteen välillä. Passiiviset keskittimet eivät sisällä toimintoja, jolla signaalia voitaisiin prosessoida lisäksi ne toimivat ilman omaa virtalähdettä.

Aktiivinen keskitin ns. moniporttitoistin ottaa vastaan tietoa passiivisen tavoin yhdestä portista, mutta generoi sen jälkeen signaalin ja käyttää uudelleen ajastusta ennen signaalin eteenpäin lähettämistä. Aktiiviset keskittimet jakavat kaistanleveyttä käyttäjien välillä, jolloin kaistanleveys vähenee käyttäjämäärän lisääntyessä. Älykkäät keskittimet eroavat aktiivisista keskittimistä elektroniikassa, älykkäitä keskittimiä hallitaan ohjelmallisesti ja niissä voi olla myös kytkeviä ominaisuuksia.

Kytkeviä keskittimiä kutsutaan myös moniporttisillaksi, ne selvittävät portteihinsa liitetyt MAC-osoitteet automaattisesti, MAC-osoitteen tarkistus tehdään erikseen jokaisen paketin kulkiessa keskittimen läpi. Kytkevät keskittimet poikkeavat myös lähetys vaiheessa muista keskittimistä, ne välittävät liikenteen ainoastaan määrättyyn kohdeporttiin, lisäksi kaistanleveys tarjotaan jokaiselle portille erikseen. (Cisco Systems 2002, 441-442.)

6.4.2 Silta (Bridge)

Silta toimii OSI-mallin ensimmäisellä ja toisella kerroksella. Siltaa käytetään yhdistämään kahta eri verkkoa ja verkon liikenteen samanaikaiseen suodattamiseen. Sillat sijaitsevat verkon reunalla, jossa ne vahvistavat signaalia signaalin kulkiessa toiseen verkkoon. Sillan täytyy myös osata tulkita verkkojen kehysrakenteita. Lähisilta toimii kahden fyysisestä toisistaan lähellä olevan verkon välisen liikenteen yhdistämisessä. Etäsillat toimivat

vastaavasti kahden kauempana olevan verkon väliseen liikenteen yhdistämiseen. Silta vaatii tässä tapauksessa erillisen yhteyden kahden sillan välillä. (Kaario 2002, 29-30.)

6.4.3 Kytkin (Switch)

Kytkimet toimivat lähiverkossa eri verkko osien yhdistämisessä. Kytkimet pystyvät yhdistämään verkkosegmenttejä verkkojen välisesti sekä verkon ja koneen välillä. Kytkimet eroavat keskittimistä siinä, että ne toimivat samanaikaisesti sekä suodattavat liikennettä kytkimeen kytkettyjen laitteiden porttitietojen avulla. Kytkimen avulla voidaan vähentää verkossa tapahtuvia törmäyksiä, koska kytkimen väylät estävät kytkimen sisäisiä törmäyksiä tapahtumasta. Kytkin toimii normaalisti OSI-mallin ensimmäisellä ja toisella kerroksella, mutta kytkin voi toimia myös ylemmissä protokollakerroksissa. Tällöin puhutaan ns. kolmannen tai neljännen kerroksen kytkimistä, kehyksien priorisoinnista riippuen. (Kaario 2002, 30.)

6.4.4 Reititin (Router)

Reititin toimii OSI-mallin kolmannessa kerroksessa. Reitittimen tehtävänä lähiverkon sisällä on yhdistää aliverkkoja tai eristää niitä toisistaan, reititin myös rajaa levitysviestien (Broadcast ja Multicast) leviämistä lähiverkon sisällä. Reititin voi myös toimia lähiverkon ja laajaverkon välissä sovittamassa niitä fyysisesti toisiinsa. Reitittimet vastaavat lähiverkossa pakettien osoitteiden määrittämisestä sekä niiden kääntämisestä fyysisiksi osoitteiksi.

Reitittimiä on käytössä joko staattisia tai dynaamisia. Staattisesti konfiguroidut reitittimet käyttävät hyväkseen staattisia reittejä, jotka syötetään laitteeseen manuaalisesti. Staattiset reitittimet eivät kommunikoi verkon muiden laitteiden kanssa vaan noudattavat reittejä, jotka niihin on kiinteästi määritelty. Dynaamiset reitittimet käyttävät kommunikoinnissa muiden laitteiden kanssa hyväkseen reititysprotokollia, joiden avulla paras reitti neuvotellaan paketin toimittamiseksi perille.

Reitittimen tehtävänä lähiverkossa protokollatasolla on reitittää datapaketteja kohteeseen pakettien mukana olevan reititysosoitteen perusteella. Protokollatieto kulkee LLC tai MAC-kehyksen datakentässä, josta reititin pystyy sen lukemaan. Reitittimellä on käytössään oma MAC-osoite, jolla ei normaalisti ole yhteyttä reitittimen lähiverkko-osoitteeseen. Osoitteet saadaan sidottua toisiinsa käyttämällä ARP (address resolution protocol) -protokollaa. Reititysprotokollan lisäksi reitittimen välillä on usein käytössä hallintaan, virheilmoituksiin tai reititystaulujen päivitykseen liittyviä protokollia. (Jaakohuhta 2002, 110-111,114;Cisco Systems 2002, 462.)

6.4.5 Palomuuri (Firewall)

Palomuurit sijaitsevat lähiverkon ja julkisen verkon rajalla. Palomuurin tehtävänä on estää ulkopuolisen liikenteen pääsy lähiverkon sisälle ja rajoittaa liikennettä verkon sisältä ulospäin. Palomuureilla pyritään erityisesti estämään ulkopuolinen haitallinen liikenne ja ilkivalta yritysten verkoista. Palomuuri toimii analysoimalla sen läpi kulkevien IP-pakettien sisältöä. Palomuuri toimii vähintään IP-kerroksen tasolla, mutta osa palomuureista pystyvät analysoimaan myös korkeampien tasojen tietoja.

Palomuurit voivat olla ohjelmistopohjaisia tai laitepohjaisia. Ohjelmistopohjaiset palomuurit ovat kokoelma sovelluksia, jotka valvovat ulos ja sisäänpäin kulkevaa verkkoliikennettä. Ohjelmistopohjaiset palomuurit ovat yleensä reitittimeen lisättyjä ratkaisuja ja laitepohjaiset palomuurit liikenteen rajoittamiseen rakennettuja erillislaitteita. Näistä vaihtoehdoista palomuurin ja reitittimen toimintojen erottaminen keskenään on suositellumpi vaihtoehto, koska pakettien reitittäminen ja suodattaminen kuluttavat laitteen prosessointikapasiteettia. (Cisco Systems 2002, 460; Kaario 2002, 32.)

6.4.6 Cisco ASA (Cisco Adaptive Security Appliance)

Ciscon teoksessa CCNA/ICND1 kuvataan Cisco ASA palomuuri/reitittimen toimintaa. Cisco ASA-palomuuri/reititin on Ciscon sovellus yrityskäyttöön, joka mahdollistaa palomuuri toiminnot, reitityksen sekä salauksen samassa laitteessa. Cisco ASA-laitteen palvelut käyttävät nimitystä Anti-x, jolla tarkoitetaan tietoturva kokonaisuutta. Tietoturvakokonaisuus pitää sisällään virustorjunta ominaisuudet eli verkkoliikenteen tarkkailun tunnetuista viruksista, vakoiluohjelmisto ominaisuudet eli vakoiluohjelmien pääsyn estämisen lähiverkkoon, sähköposti viestien skannauksen sekä roskapostien poistamisen. Näiden toimintojen lisäksi Cisco ASA-laitteella voidaan tehdä URL-osoitteiden skannausta ja rajausta sekä sähköpostiviestien rajaamista.

ASA-reititin tukee myös monimutkaisempien hyökkäysten estämisistä, joita ovat mm. tietyt kehittyneimmät madot ja järjestelmätason hyökkäykset. CISCO ASA-palomuuri reititin sisältää kehittyneen IPS (Intrusion Preventation System) -järjestelmän. Edellä mainittuja uhkia varten on kehitelty yksinkertaisempia IDS (Intrusion Detection Systems) -sovelluksia, jotka tutkivat verkkoa ja pyrkivät löytämään mahdolliset uhat ja raportoimaan uhasta palomuurilaitteelle. Kehittyneemmät IPS-sovellukset toimivat samalla periaatteella uhan etsimisessä, mutta pyrkivät reagoimaan uhkaan välittömästi ja estämään esim. madon pääsemistä verkon sisälle ennen ylläpitäjän puuttumista asiaan.

Cisco ASA–palomuuri/reititin tukee VPN (Virtual Private Network) -yhteyksiä SSL (Secure Sockets Layer) tai IPsec (IP Security) -pohjautuvaan tekniikkaan avulla. Yhteyden avulla kotikoneelta voidaan muodostaa salattu ja turvallinen yhteys yrityksen verkkoon tai tiettyyn resurssiin pääsemiseksi.

Cisco ASA-palomuuri/reitititntä käytetään lähiverkossa yhdistämässä ulkoverkkoa ja sisäverkkoa. Reitittimestä muodostetaan yhteys myös ns. DMZ (demilitarized zone) -alueelle, jonne sijoitetaan palvelimia kuten www-palvelin ja sähköpostipalvelin tai muita yrityksen palvelimia, jossa tarvitaan poikkeavia tietoturva-asetuksia muuhun verkkoon nähden. (Cisco Systems 2007a, 158-161.)

6.4.7 Työasemat ja palvelimet lähiverkossa

Lähiverkossa käytettävillä työasemilla eli asiakaskoneilla tarkoitetaan laitteita, jotka toimivat yksilöinä paikallisella tasolla eli käyttävät omia sovelluksiaan. Lisäksi ne pystyvät ottamaan yhteyttä omaan palvelinkoneeseensa sekä käyttämään sen resursseja ja palveluita hyväkseen. Isäntä nimitystä käytetään yleisesti verkon kaikista laitteista kuten työasemista, palvelin koneista, suurkoneista ja reitittimistä. Verkkopalvelimet ovat tehotietokoneita, joiden tehtävänä on tarjota palveluja ja resursseja verkon muille tietokoneille.

Palvelinten käyttötarkoitus vaihtelee verkosta riippuen. Palvelinverkossa tarjotaan keskitettyä palvelua verkon asiakaskoneille. Keskustietokoneen eli palvelimen tehtävänä on tällöin luoda yhteys verkon kaikkien koneiden välillä, tarjota keskitettyjen verkkopalveluiden käyttö sekä tarjota tietoturvallinen yhteys verkkoon ulkopuolelta. Palvelimen tarjoamia palveluita lähiverkossa voivat olla mm. tiedostojen jakaminen, tulostaminen tai sovelluspalvelimena toimiminen. Näitä tehtäviä varten voidaan tarvita myös useampia palvelimia, jolloin tiettyä tehtävää voi hoitaa erityisesti siihen suunnattu palvelin. Asiakas palvelin verkossa palvelimen on oltava tehokas, jotta se pystyy sujuvasti pyörittämään verkkokäyttöjärjestelmä, ylläpitohenkilökunnalta vaaditaan myös hyvää koulutusta.

Vertaisverkossa ei käytetä keskitettyä palvelinta tai keskitettyä tietoturvasovellusta. Jokainen työasemakone verkossa muodostaa oman palvelimensa, joka tarjoaa palveluita muille verkon koneille. Vertaisverkossa olevan koneen tarjoamat palvelut voidaan määritellä erikseen sovellusten avulla. Vertaisverkko on yksinkertainen toteuttaa sekä helppo hallita, mutta sen avulla mahdollistetut palvelut ovat rajoittuneita. (Cisco Systems 2002, 438.)

6.4.8 Terminaalipalvelin (Terminal Server)

Terminaalipalvelimen tehtävänä lähiverkossa on jakaa yhteyksiä muihin laitteisiin. Terminaalipalvelimena käytetään yleensä reititintä, joka on varustettu hitailla asynkronisillla sarjaporteilla. Portit ovat kytkettyinä muihin verkon laitteisiin kuten kytkimiin ja reitittimiin laitteiden konsoli porttien kautta. Terminaalipalvelimeen voidaan ottaa Telnet-muotoinen yhteys terminaali päätekoneelta emulaattori ohjelmistolla tai käyttää salattua yhteyttä esimerkiksi SSH-ohjelmiston avulla. Terminaalipalvelin mahdollistaa yhdestä paikasta yhteydenoton kaikkiin verkon laitteisiin, joihin palvelin on kytkettynä. Terminaalipalvelinta käytetään yleisesti avuksi lähiverkoissa vikatilanteiden selvittämisessä ja laitteiden ylläpidossa. Terminaalipalvelimen avulla voidaan muodostaa yhteys esimerkiksi vioittuneeseen laitteeseen sarjaportin kautta tilanteessa, missä normaalia yhteyttä laitteeseen ei syytä tai toisesta saada muodostettua. (Cisco Systems 2008a.)

TFTP–palvelin (TFTP server)

TFTP–palvelin on TFTP (Trivial File Transfer Protocol) -protokollaa käyttävä palvelinkone, jota käytetään enimmäkseen IP–puhelimien, kytkimien ja reitittimien konfiguraatio tiedostojen säilytyksessä ja tiedostojen siirrossa. TFTP–protokolla on rakennettu mahdollisimman yksinkertaiseksi käyttäjän kannalta, se ei sisällä autentikointia FTP–protokollan tavoin eikä se pysty listaamaan palvelinkoneen hakemistorakennetta. TFTP–protokolla käyttää UDP–protokollaa ja porttia 69 tiedostojen siirrossa. (Sollins 1992.)

TFTP–palvelimena toimivaan koneeseen asennetaan TFTP–ohjelmisto, jonka avulla palvelinkone voi jakaa esimerkiksi reitittimien ja kytkimien konfiguraatio tiedostoja. TFTP–palvelimeen voidaan ottaa yhteys suoraan Cisco IOS–ohjelmistolla IP-osoitteen perusteella. TFTP-palvelin ohjelmistoja ovat esimerkiksi mm. Philippe Jouninin valmistama Tftpd 32–ohjelmisto ja WinAgents ohjelmistotalon TFTP server for Windows sovellus. Tftpd 32-ohjelmisto on näistä yleisesti Ciscon suosittelema sovellus käytettäväksi kytkimen ja reitittimien konfiguraatiotiedostojen tallennuksessa.

6.4.9 Cisco IOS–käyttöjärjestelmä

Cisco–IOS (Internetworking Operating System) on Cisco Systemsin kehittämä käyttöjärjestelmä, jota käytetään pääasiassa Ciscon valmistamissa reitittimissä, kytkimissä sekä langattomissa tukiasemissa. Cisco IOS-ohjelmiston hallinta perustuu komentojonopohjaiseen käyttöliittymään (Comman Line Interface, CLI). IOS-järjestelmän käyttöliittymä tukee terminaali pääteohjelmistolla otettavia yhteyksiä, joiden avulla laitteen

ylläpitäjä syöttää komennot laitteelle tekstipohjaisilla käskyillä. Yhteyksiä voidaan ottaa kolmella eri metodilla konsoliyhteyden avulla, Telnet–pohjaista yhteyttä käyttämällä tai SSH (Secure Shell) -yhteyttä käyttämällä. (Cisco Systems 2007a, 205.)

Verkkolaitetta esimerkiksi reitintä tai kytkintä voidaan konfiguroida konsoliportin tai AUX-portin kautta kytkemällä tietokone edellä mainittuihin portteihin ja avaamalla terminaali yhteys laitteeseen. Tämä menetelmä on yleisesti käytössä uusien laitteiden kohdalla, joihin asetuksia ei ole tehty aiemmin. Normaalitilanteissa laitteen konfigurointi voidaan tehdä virtuaaliporttien avulla kytkemällä parikaapeli laitteeseen ja ottamalla yhteys virtuaaliportin kautta. IOS–ohjelmisto tukee useita samanaikaisia virtuaaliyhteyksiä, jolloin laitetta voidaan konfiguroida yhtäaikaisesti. Virtuaaliliitännän kautta otetut yhteydet tulisi aina suojata salasanoilla, jolloin estetään laitteen luvaton hallinta. Laitteen konfiguraatio voidaan myös kokonaisuudessaan hakea ulkopuoliselta TFTP-palvelimelta tiedostona, joka kopioidaan laitteelle verkon kautta.

Cisco IOS-ohjelmistoa käynnistettäessä käynnistysrutiini suorittaa kolme tehtävää ensimmäisenä laitteisto tarkistaa POST (power on self test) -testillä laitteiston kunnon. Seuraavaksi laitteisto lataa IOS-ohjelmiston image-tiedoston, joka sisältää käyttöjärjestelmän datan. Viimeisessä vaiheessa IOS-ohjelmisto suorittaa käyttöjärjestelmän konfiguroinnin konfiguraatiotiedoston mukaan. Tiedosto luetaan nvram muistista tai TFTP-palvelimelta, jos tiedostoa ei löydy IOS-järjestelmä palaa asetustilaan (Setup mode). Asetustilassa laitteen peruskonfigurointi voidaan tehdä manuaalisesti ohjatun toiminnon kautta. (Chappell 2002, 112-115.)

6.4.10 IOS-komentotilat

Laura Chappelin teoksessa Cisco reitittimet kuvataan Cisco IOS-järjestelmän komentotiloja. Cisco IOS-ohjelmisto koostuu hallinta tiloista, joilla laitetta hallitaan. Käyttäjätila (user mode) sisältää peruskäskyjä kuten esimerkiksi tulostukseen, testien suorittamiseen ja etäyhteyden ottoon liittyviä käskyjä, näillä käskyillä ei ole suurta vaikutusta itse laitteen toimintaan. Käyttäjätilan tunnistamisessa käytetään (>) merkkiä ennen käskyn kirjoittamista.

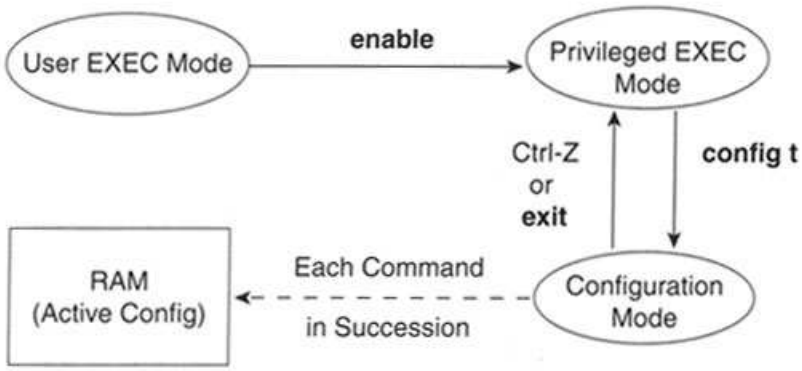
Pääkäyttäjätila (Privileged mode) sisältää parametrien asetuksiin liittyviä käskyjä sekä laitteen toimintaan liittyviä korkean tason testi käskyjä. Pääkäyttäjätilan ja sen alapuolella olevien konfiguraatiotilojen käskyjen avulla voidaan tehdä kaikki asetukset laitteessa, minkä vuoksi pääkäyttäjätilaan pääseminen estetään aina salasanalla. Cisco–IOS sisältää salasanamääritykset linjakohtaisesti sekä pääkäyttäjätilaan pääsemiseksi. Salasana voidaan määrittää selväkielisenä tai kryptatussa muodossa. Pääkäyttäjätilaan pääsemiseksi

kirjoitetaan käsky *enable* käyttäjätilassa. Pääkäyttäjätilan tunnistamisessa käytetään merkkiä (#).

Setup–tilan tarkoitus on luoda laitteelle perusasetukset kysymyssarjan perusteella. Kysymykset koskevat laitteen perusasetuksia kuten esimerkiksi laitteen nimeä, IP-osoitteita, salasanoja ja Vlan asetuksia. Setup–tilaan pääsemiseksi kirjoitetaan käsky *setup* pääkäyttäjätilassa, laite käynnistyy Setup-tilaan myös tapauksessa, jossa laite käynnistetään uudelleen, eikä laite löydä konfiguraatio tiedostoa TFTP-palvelimelta tai NVRAM-muistista.

Globaali konfiguraatiotila (Global configuration mode) on tila, jossa laitteen varsinaiset asetukset tehdään. Tilaan pääsemiseksi ylläpitäjä kirjoittaa komennon *configure terminal* pääkäyttäjätilassa. Globaalissa konfiguraatiotilassa voidaan tehdä esimerkiksi reitittimen reititykseen ja pääsylistoihin liittyvät komennot. Globaalin konfiguraatiotilan tunnistaa tunnisteesta (config #).

Cisco IOS–ohjelmisto sisältää globaalista konfiguraatiotilasta alempia tiloja noin 17 kappaletta. Näiden tilojen avulla voidaan tehdä tarkempia asetuksia laitteen konfiguroinnissa mm. kohdentaa asetukset koskemaan yksittäistä liitäntää, reititysprotokollaa tai virtuaalista liitäntää. Cisco IOS–ohjelmistossa voidaan liikkuja tilojen välillä eteenpäin käyttämällä komentoja *enable* ja *configure terminal*. Komennoilla *exit*, *disable* tai näppäinyhdistelmällä ctrl+Z päästään liikkumaan tiloissa takaisinpäin. Komento *exit* tai *log out* käyttäjätilassa tehtynä katkaisee terminaaliyhteyden laitteeseen. Cisco IOS-ohjelmiston käyttäjätiloissa liikkuminen ja komennot on havainnollistettu kuviossa 2.



Kuvio 2: Cisco IOS-käyttäjätilat (Cisco Systems 2007b, 215).

Cisco IOS-ohjelmisto sisältää sisäänrakennetun Help–toiminnon, joka perustuu konteksti pohjaiseen toimintaan. Toiminnon avulla on mahdollista hakea käskyyn liittyvien komentojen listauksen. Help-toimintoa voi käyttää ”?” merkin avulla, kysymysmerkkiä käytetään

korvaamaan komento, josta ei ole varmuutta. Kysymysmerkki sijoitetaan tässä tapauksessa komennon perään välimerkillä eroteltuna. Kysymysmerkkiä voi käyttää myös käskyn perässä ilman välilyöntiä, jolloin Help-toiminto listaa komennot, jotka alkavat käytetyillä merkeillä ennen kysymysmerkkiä. (Chappell 2002, 117-119,123.)

6.5 Kytkentä lähiverkossa

Kytkentätekniikalla vähennetään Ethernet-verkkojen ruuhkautumista liikennettä pienentämällä, tämä lisää käytettävissä olevaa kaistanleveyttä. Lähiverkossa tapahtuva kytkentä jakautuu kahteen tehtävään datakehysten kytkentään ja kytkentäoperaatioiden ylläpitoon. Datakehysten kytkennällä ohjataan kehys kytkimen sisään tulevasta portista ulos lähtevään porttiin. Kytkimen toinen tärkeä tehtävä on kytkentätaulun rakentaminen ja ylläpito. Kytkimet ohjaavat kehyksiä lähiverkoissa käyttäen MAC-osoitetauluja hyväkseen, tätä kutsutaan toisen kerroksen kytkemiseksi. Jos kytkin ei tiedä, minne kehys pitää lähettää se käyttää koko verkkoon lähetettävää Broadcast-sanomaa selvittääkseen oikean kohteen. Kohteen osoitteen selvitessä, kytkin tallentaa tiedon omaan kytkentätauluunsa. Reitittimet käyttävät kolmannessa kerroksessa tapahtuvaa kytkentää paketin reitittämiseen, tässä tapauksessa kytkentä tapahtuu verkkokerroksen tietojen perusteella. (Cisco Systems 2002, 49-51.)

6.5.1 Kytkentämenetelmät

Kytkentä jaetaan teknisesti kolmeen luokkaan, näitä ovat Store and Forward-kytkentä, Cut-through-kytkentä sekä Fragment-free-kytkentä. Store and Forward-kytkentä tarkoittaa kytkentätapaa, jossa kytkin vastaanottaa koko kehyksen ennen kehyksen lähettämistä eteenpäin. Tällä saavutetaan hyvä virheenkorjaus taso, koska koko kehys luetaan läpi, vastaavasti tämä aiheuttaa viivettä verkossa. Store and Forward-kytkentämentelmä on yleisin kytkentämenetelmä vähintään 100 Mbps lähiverkoissa.

6.5.2 Cut-through-kytkentä

Cut-through-kytkentä toimii päinvastaisesti, Cut-through menetelmää käyttävä kytkin lähettää kehyksen välittömästi eteenpäin niin nopeasti kuin se on mahdollista. Cut-through-kytkentä on nopea tapa kytkeä kehyksiä, mutta virheellisten kehyksien määrä kasvaa. Tämä johtuu siitä, että kytkin ei tarkista kehyksien sisältämiä virheitä ennen kehyksien lähettämistä eteenpäin.

6.5.3 Fragment-free kytkentä

Fragment free-kytkennän toimintalogiikka perustuu Cut-through-kytkentään logiikaltaan. Eroavaisuutena Fragment free-kytkennässä virheenkorjausta pyritään parantamaan lähettämällä kehys eteenpäin vasta kun siitä on luettu 64 ensimmäistä tavua. Kytkentätapa perustuu CSMA/CD-menetelmän toimintaan, jossa 64 ensimmäisen tavun jälkeen kehyksien välinen törmäys on mahdollista havaita. Tämä menetelmä parantaa virheellisten kehyksien havaitsemista, mutta toimii vastaavasti hieman hitaammin kuin Cut-through-kytkentämenetelmä. (Cisco Systems 2007a, 181.)

7 Langaton lähiverkko (Wireless Local Area Network, WLAN)

Langattomien verkkojen avulla ihmiset voivat viestiä keskenään ja olla yhteydessä sovelluksiin ilman fyysistä tietoverkkoa. Tämä mahdollistaa vapaan liikkumisen rakennuksen sisällä, kaupungissa tai jopa ympäri maailmaa. Langattomien verkkojen avulla ihmiset voivat käyttää sähköpostia tai selata internetiä vapaasti valitsemassaan paikassa esimerkiksi kotona. Langattomat verkot siirtävät kuparin tai kuituverkon tapaan dataa tietokonelaitteiden välillä, mutta ne mahdollistavat myös video ja puhelinneuvottelu sovellukset. Langattomat verkot käyttävät tiedonsiirrossa hyväkseen joko radiosignaalia tai infrapunavaloa. (Geier 2005, 4.)

7.1 Langaton lähiverkko, WLAN

Langaton lähiverkko muistuttaa suorituskykynsä, rakennusosien, kustannusten sekä toimintansa suhteen perinteistä langallista Ethernet verkkoa. Langattomat lähiverkot ovat yleisiä kannettavissa tietokoneissa mistä johtuen julkisia langattomia verkkoja löytyy yhä useammista paikoista lentokentistä, hotelleihin ja koululaitoksiin, joissa langattoman verkon käyttö on joko ilmaista tai maksullista. Langattoman verkon vallitseva standardi on IEEE 802.11, joka toimii joko 2,4 Ghz tai 5 Ghz taajuudella. 802.11-standardin yhteensopivuusongelmista johtuen Wi-FI Alliance kehitti Wireless Fidelity (Wi-FI)-standardin, joka käyttää 802.11 toimintoja, mutta sen yhteensopivuus on taattu muiden Wi-Fi-standardia tukevien laitteiden kanssa. Wi-Fi:n avoimuus on nostanut sen suosiota, joka on tärkeä osa julkisissa langattomissa verkoissa.

IEEE 802.11-standardista on kehitetty useita eri versioita, jotka edustavat eri teknologiasukupolven laitteita. Alkuperäinen 802.11-standardi käytti siirtonopeutena 2Mb/s ja uusin 802.11n versio käyttää siirtonopeutenaan yli 100Mb/s siirtonopeutta. Kaikki standardit toimivat taajuusalueinaan joko 2,4 Ghz tai 5Ghz alueet, jotka jaetaan edelleen maakohtaisiin kanaviin säädöksien mukaisesti. Suurimman keskinäisen eron standardien väliin tekee niiden

käyttämät modulointi tavat, joita on käytössä useita erilaisia. (Geier 2005, 9;Hakala & Vainio 2005, 152.)

7.1.1 Langaton verkkokortti (Wireless Network card)

Langattomat verkkokortit muodostuvat olennaisen osan langattomien verkkojen toiminnasta. Langattomien verkkokorttien avulla koneet ovat yhteydessä langattomien tukiasemien kautta lähiverkkoon. Langattomat verkkokortit tukevat normaalisti 802.11a tai 802.11b/g-standardiin perustuvaa ratkaisumallia tai mahdollisesti kumpaakin versiota standardeista. Langattoman verkkokortin ja tukiasemien yhteensopivuuden edellytyksenä on, että laitteet käyttävät samaa langattoman verkon standardia. Langattomia kortteja on saatavilla yleisesti pöytäkoneisiin ja kannettaviin tietokoneisiin. (Geier 2005, 106.)

7.1.2 Langaton tukiasema (Wireless Access-Point)

Langaton tukiasema on keskeisin langattoman verkon laite. Langattomia tukiasemia käytetään levittämään langattoman verkon kattavuusaluetta tietylle alueelle esimerkiksi kattamaan yhden luokan. Tukiasemat voivat toimia monessa tehtävässä, mutta niiden pääasiallinen tehtävä on toimia langattoman lähiverkon ja jakelujärjestelmän välisenä siltana. Tukiasemat sisältävät HTTP–pohjaisen käyttöliittymän, jolla tukiasemaan liittyviä asetuksia voidaan tehdä selainyhteyden kautta. Tukiasemassa voi olla varusteena myös sarjaliitäntä, jolla laite voidaan konfiguroida esimerkiksi Telnet–ohjelmiston avulla.

Tukiasemat on hyvä valita verkossa käytettävien standardien mukaisesti, jolloin ne tukevat suoraan verkon muita laitteita. Tukiaseman käyttöönotossa sille määritellään muutamia tärkeitä asetuksia. SSID (Service Set Identifier) -tunnuksella määritellään käytetylle verkolle tunnus, jonka käyttäjät syöttävät koneille ennen verkkoon kirjautumista. Lähetysteholla määritellään teho watteina, jota tukiasema käyttää lähetykseen. Radiokanavan valinta tukiasemassa on tärkeää, jos useampaa tukiasemaa käytetään yhtäaikaisesti saman kantaman sisällä. Tukiaseman radiokanava voidaan valita väliltä 1-11. Tukiasemaan kytketään normaalisti myös vähintään WEP–tason salaus päälle, jolloin tukiaseman käyttäminen vaatii salausavaimen käyttöä. (Geier 2005, 106-107;Hakala & Vainio 2005, 158.)

7.1.3 Langaton reititin (Wireless Router)

Langaton reititin toimii samoin kun Ethernet reititin eli sen toiminta pohjautuu verkkojen keskinäiseen yhdistämiseen. Langatonta reititintä käytetään yhdistämään useita langattomia verkkoja ja kiinteitä langallisia verkkoja toisiinsa. Langattoman reitittimen toiminnan hoitaa normaalisti Ethernet reititin, johon on asetettu langattoman verkon tukiasematoimintoja.

Langattomissa reitittimissä käytetään yleisesti NAT–protokollaa ja DHCP–palvelua, jolloin langatonta verkkoa käyttävät koneet saavat yksityiset IP–osoitteet ja näkyvät ulospäin yhtenä IP–osoitteena. Langatonta reitititintä tarvitaan tapauksessa, jossa yrityksen useamman paikallisen verkon laitteet haluavat jakaa saman IP-osoitteen keskenään. Langattomia reitittimiä käytetään pääasiassa isoissa laitoksissa kuten sairaaloissa tai isoissa yrityksien konttoreissa, joissa on käytössä useampia langattomia verkkoja. (Geier 2005, 108.)

7.1.4 Langaton toistin (Wireless Repeater)

Langattomien toistimien pääkäyttötarkoitus on vahvistaa langattoman verkon signaalia kattavuusalueen ulkopuolelle ja laajentaa näin ollen verkon kattavuusaluetta. Langattomia toistimia käytetään tukiasemien sijasta. Langaton toistin toimii itsenäisesti ottamalla vastaan radiosignaaleja ja lähettämällä ne uudelleen. Toistimien avulla langaton verkko saadaan ulottumaan alueille, joille normaalisti ei voida rakentaa langatonta verkkoa. Langattomien toistimien käytössä suurin ongelma on niiden käyttämä radiotaajuus, joka toimii samalla kanavalla kuin verkon tukiasemat. Tästä syystä tukiasemien käyttöä tulisi rajoittaa, koska ne aiheuttavat verkossa turhia törmäyksiä. (Geier 2005, 109;Hakala & Vainio 2005, 164.)

7.1.5 Etäsilta (Bridge) ja monipistesilta (Multipoint Bridge)

Langattomien etäsiltojen tehtävänä on yhdistää langattomien verkkojen käyttämiä siirtoteitä. Langaton etäsilta pystyy yhdistämään esimerkiksi yrityksen kaksi vierekkäistä toimipistettä toisiinsa kytkimien kautta. Etäsilta käyttää kytkimien yhdistämisessä niiden MAC-osoitetta ja salausta hyväkseen. Etäsillat käyttävät antenneina erityisiä suunta-antenneja, joiden avulla törmäykset jäävät verkossa vähäiseksi. Monipistesilta toimii etäsillan tavoin verkkojen yhdistämisessä, mutta yhdistää kytkimien sijasta kokonaisia langattomia verkkoja toisiinsa. Monipistesilta käyttää verkkojen yhdistämisessä käytännössä aina salausta, mutta liikenteen ohjaamiseen ei tarvita vastaanottavan ja lähettävän laitteen MAC–osoitteita. Monipistesillan avulla voidaan yhdistää myös langaton ja langallinen verkko toisiinsa tarvittaessa. (Hakala & Vainio 2005, 162-163.)

7.1.6 Langaton Antenni (Wireless Antenna)

Langattoman verkon laitteista suurin osa käyttää langattoman verkon antennina ympärisäteilevää antennia. Ympärisäteilevä antenni käyttää alhaista tehovahvistusta, eikä se keskitä signaalia erityisesti mihinkään suuntaan, jolloin sen peitto-alue ei välttämättä riitä kaikissa tapauksissa. Suunnattavat antennit sopivat paremmin tiloihin, joissa halutaan langattoman verkon peiton olevan kapealla pitkänomaisella alueella esimerkiksi pitkällä käytävällä. Suuntaavia antenneja on eri käyttötarkoituksiin niiden tarjoaman radioaaltojen

keskittämisominaisuuksien mukaan. Lautasantennit ja putkiantennit tarjoavat parhaan tehon tiettyyn suuntaan, jolloin antennin lähetys pysyy suhteellisen kapealla alueella. Sektori-ja paneeliantenniratkaisut tarjoavat signaalin rajoittamiseen liittyviä ominaisuuksia. (Geier 2005, 110; Hakala & Vainio 2005, 165-166.)

7.2 802.11-standardin MAC-kerros

Alkuperäinen standardi 802.11 julkaistiin vuonna 1997. Langattomien laitteiden yleistyessä vasta 2000-luvulla standardia tukevia laitteita ei ole enää saatavissa, mutta uudemmat standardit pohjautuvat 802.11-standardissa määriteltyyn MAC-kerrokseen. MAC-kerroksen avulla määritellään langattomien verkkojen käyttämä siirtotie ja hallinnoidaan sitä laitteiden välillä. MAC-kerros varaa siirtotien kehyksien lähettämiselle, siirtotienä käytetään radiokanavaa. Siirtotien varaamiseksi MAC-kerroksella on käytössä kaksi menetelmää, joko DCF (distributed coordinated funcion) -menetelmä tai PCF (point coordination function) -menetelmä. DCF-menetelmä perustuu CSMA/CA (Carried Sense Multiple Access/Collision Avoidance) -algoritmiin, jossa tukiasemat kilpailevat siirtotien varaamisesta lähettämällä kehyksiä siirtotielle satunnaisesti. Siirtotien ollessa varattu laite odottaa tietyn ajan ja lähettää kehyksen hetken kuluttua uudestaan. PCF-menetelmässä tukiasema lähettää ruuhkavapaina aikoina kiertokyselyjä, jolloin lähettävälle asemalle saadaan lähetysvuoro siirtotielle. Muut asemat eivät voi tällöin lähettää omia kehyksiään. Tukiasema kiertää PCF-menetelmässä ruuhka-ajan ulkopuolelle määritellyn listan mukaan muita asemia läpi ja vaihtaa ruuhka-aikoina käyttämään DCF-menetelmää. PCF-menetelmässä dataliikenne saadaan ohjattua tasaisemmin ruuhkajaksojen väliin. PCF-menetelmän huono puoli on se, että sitä tukevia laitteita on saatavissa vähän, tulevaisuudessa menetelmän käyttö on yleistymässä. (Internet Engineering Task Force 2007.)

7.2.1 802.11-standardiin perustuva skannaus

802.11 standardi määrittää verkkokorttikohtaisen skannauksen, joka voidaan tehdä aktiivisesti tai passiivisesti. Passiivinen skannaus on pakollinen kaikissa verkkokorteissa, siinä tukiasema lähettää beacon-viestin avulla tietoa olemassaolostaan, jota radiopohjainen verkkokortti vastaavasti käsittelee. Verkkokortti hakee sille määritetyltä kanavalta signaalinlaadultaan parasta tukiasemaa, jota kannattaa tiedonsiirtoon käyttää.

Valintapohjainen skannaus tapahtuu verkkokortin aloitteesta, siinä verkkokortti lähettää probe-kyselyn sitä lähellä oleville tukiasemille, joihin kaikki tukiasemat vastaavat probe response viestillä. Tässä tapauksessa tukiasema saa välittömästi vastauksen ja voi aloittaa datan lähetyksen heti odottamatta tukiasemien beacon-viestejä, vastaavasti

valintapohjaisessa skannauksessa verkko liikenteen määrä kasvaa probe-kyselyjen johdosta. (Internet Engineering Task Force 2007.)

7.2.2 802.11-standardiin perustuva todennus

802.11 standardin määrittämä langattoman verkon todennus tapahtuu joko avoimesti tai jaettuun avaimeen perustuvasti. Avoimessa todennuksessa verkkokortti pyytää tukiasemalta lupaa liikennöintiin lähettämällä sille todennuspyyntökehyksen, johon tukiasema vastaa todennusvastauskehyksellä joko kielteisesti tai myönteisesti. Tämän jälkeen liikennöinti, joko alkaa tai verkkokortti lähtee pyytämään lupaa joltakin toiselta tukiasemalta.

Jaettuun avaimeen perustuvassa todennuksessa liikennöinti alkaa vasta WEP-avaimen hyväksymisen jälkeen. Verkkokortti aloittaa lähetyksen lähettämällä todennuspyyntökehyksen liikennöinnin aloittamiseen. Tukiasema vastaa pyyntöön lähettämällä todennuskehyksen, joka sisältää salauksessa käytettävän haastetekstin ja lähettää vastauksen verkkokortille. Verkkokortti tekee tämän jälkeen haastetekstille salauksen käyttämällä WEP (Wired Equivalent Privacy) -tekniikkaan perustuvaa avainta ja lähettää tukiasemalle uuden todennuskehyksen. Tukiasema purkaa tämän jälkeen salauksen ja vertaa purettua haastetekstiä alkuperäiseen, jos tekstit vastaavat toisiaan, lähettää tukiasema vastauksena hyväksyvän todennuskehyksen. Jos viestit eivät vastaa toisiaan, lähettää tukiasema hylätyn todennuskehyksen. WEP-tekniikkaan perustuvaa salaustapaa ei voida käyttää korkeampaa tietoturvaa vaativissa verkoissa, koska se on suhteellisen helppo purkaa. IEEE 802.11i-protokollan versiossa tietoturvaa on paranneltu WPA2-pohjaisen salauksen myötä. (Internet Engineering Task Force 2007.)

7.2.3 802.11-standardin perustuva assosioituminen

Assosioitumisella tarkoitetaan oikeutta käyttää tukiasemaa, kaikki verkkokortit, jotka haluavat liikennöidä tietyn tukiaseman verkkoon, joutuvat assosioitumaan kyseiseen tukiasemaan. Assosiointi alkaa verkkokortin lähettämällä assosiointikehyksellä, kehys sisältää tiedot verkosta, sen tukemat nopeudet sekä SSID-tunnisteen. Tukiasema vastaa kehykseen lähettämällä assosiointivastauskehyksen, jossa lähetetään verkon tukiasemien tai aseman käyttämistä koskevat tiedot verkkokortille sekä assosioitumistunnuksen verkon käyttöä varten. Assosiointiprosessi hoidetaan aina ennen liikennöinnin aloittamista.

802.11 standardi määrittää myös muita valinnaisia toimintoja kuten, RTS-CTS (Request-to-Send/Clear-to-Send) -toiminnon, jolla voidaan parantaa liikennöintiä verkkokorttien välillä, jotka käyttävät samaa tukiasemaa. RTS-CTS toiminto sisältää myös mahdollisuuden fragmentoida kehyksiä tietyn kokoisien kehyksien raja-arvon ylityttyä. Fragmentoinnissa

verkkokortti jakaa suuren kehykset pienempiin osiin, jotka alittavat kehyksille määrätyn raja-arvon. Lisäksi verkkokortit sisältävät virransäätöominaisuuden, jolla verkkokortti menee lepotilaan akkujen säästämiseksi. Lepotilassa olevan verkkokortti ei lähetä paketteja ja vastaanottaa ainoastaan tietyn väliajoin tulevat beacon-lähetykset tukiasemasta tiedustellakseen kortille päin tulleista kehyksistä. (Internet Engineering Task Force 2007.)

7.3 802.11-standardin kehitystyö

Alkuperäinen 802.11-standardi julkaistiin vuonna 1997. Siihen on määritelty taajuushyppyspektriin FHSS (Frequency Hopping Spread Sperctrum) sekä suorasekvenssispektriin DSSS (Direct Sequency Spread Spectrum) -perustuvat fyysiset kerrokset 2.4 GHz taajuudella sekä 2Mbps nopeudella. Tekniikoille ei löydy nykypäivänä enää laitteita myynnistä niiden hitauden takia, ainoastaan FHSS-tekniikan tuki ulkona toimiviin järjestelmiin voidaan pitää hyvänä ratkaisuna, jos FHSS-tekniikkaan perustuvia laitteita on käytössä. (Geier 2005, 124.)

7.3.1 802.11a-standardi

802.11-standardiin on kehitelty vuosien aikana teknisiä parannuksia, joista ensimmäisenä julkaistiin vuonna 1999 802.11a-standardi, joka määrittelee OFDM (Orthogonal Frequency Division Multiplexing) -tekniikalla toimivan 5Ghz kaistan 54 Mbps nopeudella. Tekniikalla päästään 30 metrin etäisyyteen nopeudesta riippuen. Tämän etäisyyden saavuttaminen yhdellä tukiasemalla voi osoittautua hankalaksi 54Mbs nopeutta käyttäen, jolloin alueen kattamiseksi tarvitaan enemmän tukiasemia. Tekniikan etuna on sen käyttämä 5 GHz kaista, jonka avulla voidaan siirtää esimerkiksi liikkuvaa kuvaa ja tarjota parempaa suorituskykyä kuin muilla tekniikoilla. (Internet Engineering Task Force 1999a.)

7.3.2 802.11b-standardi

802.11b-standardi julkaistiin samaan aikaan 802.11a:n kanssa. Standardi kehitettiin alkuperäisen 802.11-standardin jatkoksi tarjoten suuremman siirtonopeuden. Standardi käyttää 2,4 GHz taajuutta ja 11Mbs nopeutta. Standardia tukevilla laitteilla voidaan saavuttaa sisätiloissa 100 metrin kantama, jolloin käytettävien tukiasemien määrä jää huomattavasti alhaisemmaksi kuin 802.11a:ta käytettäessä. Useimmat nykyajan langattomat verkkolaitteet tukevat tätä standardia. Haittapuolena standardissa on sen vapaiden kanavien määrä, joka tarjoaa käytännössä 3 yhtäaikaista 2,4 GHz kanavaa samanaikaisesti käytettäväksi. Toinen haittapuoli on sen häiriöherkkyys langattomien laitteiden ja esimerkiksi mikroaaltouunin kanssa sekä tekniikan epäyhteensopivuus 802.11a:ta tukevien laitteiden kanssa. Standardia

tukevat laitteet soveltuvat parhaiten käytettäväksi perustason nettikäytössä kuten sähköpostin ja Internetin selaamisessa. (Internet Engineering Task Force 1999b.)

7.3.3 802.11g-standardi

802.11g-standardi julkaistiin vuonna 2003. Standardi kehitettiin laajennuksena aiempaan 802.11b standardiin ja se nosti 2,4 GHz kaistan käyttämän nopeuden aina 54Mbs:iin saakka OFDM-tekniikkaa käyttäen. Standardissa suurena etuna on sen yhteensopivuus 802.11b:tä tukevien laitteiden kanssa. Tilanteessa, jossa yrityksellä on käytössä kahden eri standardin laitteita pitää muistaa, että se rajoittaa verkon kokonaissuorituskykyä, syystä että 802.11b laitteet vaativat suojalusmekanismien asentamista. Tämä johtuu standardien käyttämien modulointien eroavaisuudesta keskenään. Häiriöherkkyysongelmat ja vähäinen kanavamäärä koskevat samoin myös 802.11g standardia kuin 802.11b standardia. (Internet Engineering Task Force 2003.)

7.4 Langattoman verkot salausmenetelmät

Langattomien verkkojen salakuuntelu on helppoa, koska langattomien verkkojen tiedonsiirtoon käytetään radioaaltoja. Luvaton verkkoon kytkeytyminen on helpompaa, esimerkiksi talon ulkopuolelta voidaan ottaa yhteys yrityksen verkkoon kannettavalla tietokoneella, jossa on langaton verkkokortti. Langattomiin verkkoihin on rakennettu suojauskäytäntöjä liikenteen salakuuntelun ja luvattoman käytön ehkäisemiseksi. Suojausmekanismeista yhtenä tärkeänä osana ovat salaus ja autentikointiprotokollat.

Salausmenetelmät jaetaan kahteen luokkaan niiden käyttämän tekniikan mukaan. Symmetriset salausmenetelmät käyttävät samaa avainta salauksen tekemisessä ja purkamisessa. Symmetristä salausta voidaan käyttää laitteissa, jotka luottava toisiinsa esimerkiksi yrityslähiverkoissa laitteiden välillä. Symmetrisessä salauksessa on tärkeää muuttaa salauksessa käytettävää avainta mahdollisen usein, jotta tietoturva saadaan pidettyä riittävän korkealla. Symmetriset salausmenetelmät käyttävät avaintenjakelumenetelmää, joilla salauksessa käytettävää avainta vaihdetaan, jopa yksittäisten lähetysten välillä.

Julkiseen avaimeen perustuva salaus käyttää epäsymmetrisiä avaimia, joista toinen on julkinen avain ja toinen yksityinen avain. Julkinen avain on yleinen avain, jonka saa käyttöönsä kuka tahansa salausta käyttävä henkilö. Yksityinen avain on salattu avain, joka on tiedossa ainoastaan laitteessa, joka purkaa salauksen. Julkisen avaimen salauksen toiminnan kannalta julkisien ja yksityisten avaimien on vastattava salauksen kannalta toisiaan, tällöin kummalla avaimella tahansa on mahdollista salata ja purkaa dataa. Julkiseen avaimeen

perustuvat salausmenetelmät ovat tehokkaita käyttää, koska salaukseen vaadittava julkinen avain voidaan toimittaa kelle tahansa. (Geier 2005,178-179; Hakala & Vainio 2005 167.)

7.4.1 WEP (Wired Equivalent Privacy)-salausmenetelmä

WEP–protokolla on 802.11-standardiin perustuva MAC–kerroksessa toimiva valinnainen salaus ja todennusstandardi. WEP–protokollalla tehty salaus perustuu RSA–yhtiöön RC4-pohjautuvaan salausalgoritmiin. WEP–protokollalla tehty salaus käyttää symmetristä salausmenetelmää ja 128-bittistä salausavainta. WEP–protokolla ei sisällä mekanismia avainten vaihtamiseksi, jolloin datan salaamisessa käytetään ainoastaan yhtä avainta. Tämän seikan johdosta sitä ei voida käyttää tietoturvaa vaativissa käyttöolosuhteissa. Hakkerit voivat hakkeroida WEP–protokollan käyttämän avaimen ohjelmiston avulla jopa noin 1Gb liikenteen seuraamisen jälkeen.

WEP–protokollaa tukevat suurin osa verkkokorttien ja tukiasemien valmistajista, jolloin sen käyttöä voi suositella tilanteessa, jossa suojaamattoman yleisen verkon käyttöä halutaan rajata. WEP–salauksella voidaan estää ulkopuolisen ihmisen luvaton verkon käyttö, mutta sitä ei suositella käyttämään verkoissa, jossa on esimerkiksi tiedostoa jakavia palvelimia. (Geier 2005,181,183; Hakala & Vainio 2005, 168-169.)

7.4.2 TKIP (Temporal Key Integrity protocol)–salausmenetelmä

TKIP–salausmenetelmä käyttää WEP–pohjautuvan salauksen tavoin salauksen tekemisessä RC4-algoritmia. Suurin ero TKIP–salausmenetelmän ja WEP–salausmenetelmän välillä on salaus avaimien käytössä. TKIP-salausmenetelmä toimii symmetrisesti, mutta sisältää paremman salausavaimen vaihtoon liittyvän mekanismin. TKIP–salauksessa verkkokortit ja tukiasemat käyttävät väliaikaista 128 bittistä avainta, jota vaihdetaan aina 10000 paketin välein. Dynaamisen menetelmän avulla saavutetaan huomattava tietoturvan lisäys verkossa. TKIP–salaus on tarjolla jo useimmissa lähiverkkojen tuotteissa ja siihen siirtyminen WEP–pohjaista verkkoa käyttävistä laitteista on helppoa. Päivitysten tekeminen vaatii yleensä ainoastaan laitteiden ohjelmistopäivitykset. WEP–pohjaiset laitteet pystyvät lisäksi keskustelemaan TKIP–pohjaisten laitteiden kanssa käyttäen ainoastaan WEP-muotoista salausta. (Geier 2005,183.)

7.4.3 AES (Advanced Encryption Standard)-salausmenetelmä

AES-salausmenetelmä pohjautuu huomattavasti raskaampaan Rine-Dale–salausalgoritmiin, joka tarjoaa erittäin vahvan salausmenetelmän. AES–menetelmän ongelma on sen korkea prosessoritehovaatimus, mutta tehokoneilla sen käyttäminen on suositeltavaa. AES vaatii toimiakseen rinnakkaisen prosessorin käyttöä. Jos yrityksellä on tarvetta käyttää vahvaa

salausta langattoman tietoliikenteensä suojaamiseen, AES–salauksen käyttö on paras mahdollinen vaihtoehto. (Geier 2005,184.)

7.4.4 WPA1.0 (Wireless Fidelity Protected Access)-salausmenetelmä

Wi-Fi Alliancen WiFi Protected Access on yleisin käytössä olevan salausmenetelmä kannettavissa laitteissa. Menetelmä tarjoaa dynaamiseen avaimeen perustuvan salauksen, johon käytetään kaksisuuntaista todennusta. WPA–salaus käyttävät asiakkaat käyttävät eri salausavaimia, joita vaihdetaan TKIP–salauksessa käytettävän 10000 paketin välein. WPA (Wireless Fidelity Protected Access) -protokolla sisältää EAP (Extensible Authentication Protocol) -protokollan käyttäjien autentikoinnin parantamiseen ja TKIP–salaus menetelmän tai AES–salausmentelmän WEP–pohjaisen salauksen parantamiseen. WPA on siis käytännössä yhdistelmä 802.11i:stä, joka tarjoaa TKIP-salaukseen pohjautuvan menetelmän sekä 802.1x-standardin mekanismit.

Suurimmat heikkoudet WPA-salauksessa liittyvät RC4-salauksen käyttöön sekä DoS (Denial of Service) -palvelunestohyökkäyksien reagointiin. WPA–protokolla reagoi palvelunestohyökkäyksiin sammuttamalla verkon minuutiksi käytöstä, joka vaikuttaa välittömästi WPA–salausta käyttävän yrityksen tai laitoksen toimintaan. (Geier, 2005, 184;Hakala & Vainio 2005,169.)

7.5 Cisco Secure Access Control Server (ACS)

Cisco ACS–server on Cisco Systemsin ohjelmistosovellus, joka on tarkoitettu langattomien verkkojen tukiasemien hallintaan. Ohjelmisto tukee keskitettyä hallintaa, jonka avulla laitteiden hallinta on mahdollista tehdä verkon kautta langattomasti, langallista verkkoa käyttämällä tai etähallinnalla.

ACS-palvelin mahdollistaa keskitetyn langattoman verkon tietoturvan, jossa ACS-palvelin toimii verkossa laitteena, johon tietoturvamääritykset asetetaan. Langattoman verkon käyttäjät ja laitteet tunnistetaan palvelimessa ennen verkon resursseihin pääsyä. ACS-palvelin sisältää tuen RADIUS ja TACACS+ AAA (Authentication, Authorization and Accounting) -protokollille, joiden avulla mahdollistetaan tietoturvallinen kirjautuminen verkkoon. ACS-palvelimen mahdollistaa:

1 Laitteiden hallinnan ja ylläpidon, jonka avulla verkon ylläpitäjät ja ylläpitoon liittyvät komennot voidaan määritellä. Myös henkilöiden resurssien pääsyn auditointi on mahdollista. ACS-palvelin sisältää kattavat raportointi ominaisuudet verkkoliikenteen ylläpitämistä ja vianhakua varten.

2 Etähallinta yhteydet, VPN yhteyksien tai muiden etähallinta laitteiden kautta, jotka mahdollistavat suojatun yhteyden luomisen palvelimelle.

3 Langattoman verkon käyttäjien ja tukiasemien autentikointi ja authorisointi mahdollisuuden langattoman tietoturva säännösten mukaisesti.

4 Langallisten verkkojen VLAN tuen sekä pääsylistojen määrittämisen porttikohtaisesti.

5 Tuen ulkopuolisille tietoturvapalvelimille, joiden avulla verkon tietoturvapolitiikkaa on mahdollista ylläpitää ja vaihtaa raportteja.

ACS-palvelin sisältää käyttäjätietokannan, joka tukee Windows Active Directoryä, LDAP tai ODBC-protokollaa. Suurempaa tietoturvaa vaativiin verkkoihin ACS-palvelimeen on mahdollista liittää myös RSA SecureID Authentication Manager ohjelmistoa tai Radius-palvelinta tukevia vahvempia autentikointi-järjestelmiä. ACS-palvelin tukee suurinta osaa nykyisistä autentikointi protokollista. Autentikointiin voidaan käyttää mm. PAP (Password Authentication portocol), CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) sekä PEAP (Protected EAP) -protokollia.

ACS-palvelinta hallitaan graafisella käyttöliittymällä, johon yhteys muodostetaan selaimella, salatun yhteyden kautta myös komentojonopohjaisen CLI (Command Line Interface) -liitännän käyttäminen on mahdollista. ACS-palvelin käyttää tietokannan hallinnassa helppokäyttöistä RDBMS (Relational Database Management System) -hallintasovellusta, jonka avulla yhteys tietokantaa muodostetaan selaimen kautta. Ohjelmisto on saatavilla Windows Server 2003 käyttöjärjestelmälle. Muina vaatimuksina ovat 1.8Ghz prosessori, vähintään 1Gb keskusmuistia sekä 1GB kiintolevytilaa. (Cisco Systems 2008b.)

8 Virtuaalinen lähiverkko (VLAN)

Virtuaalilähiverkoilla tarkoitetaan tekniikoita, joilla voidaan jakaa yksi fyysinen useaksi eristetyksi verkoksi. VLAN-tekniikan avulla yksi kytkin voi kuljettaa Ethernet-kehyksiä jokaisesta virtuaalisesta verkosta, siten että virtuaalisen lähiverkon laitteet kommunikoivat ainoastaan omassa lähiverkossaan olevien laitteiden kanssa. VLAN-tekniikan avulla lähiverkon kehyksiä voidaan jakaa myös eritason palveluluokkiin.

Lähiverkon etuina ovat tietoturvan lisääntyminen, (käyttäjäryhmät voidaan erotella jo Ethernet tasolla) palvelun laatua tukevien verkkojen toteuttamisen mahdollisuuksien parantuminen sekä verkkojen suunnittelun parantuminen, koska lähiverkkojen avulla eri

ryhmiin kuuluvat käyttäjäryhmät voivat sijaita eripuolilla fyysistä verkkoa. Yksi VLAN-tekniikan tärkeimpiä ominaisuuksia on verkkojen kuormituksen vähentäminen, VLAN-tekniikan avulla verkkojen väliset yleisviestit (Broadcast) -viestit voidaan rajata virtuaalisen verkon sisälle. (Kaario 2002, 41.)

8.1 VLAN verkon toteutustavat

VLAN muodostaa verkon, joka segmentoidaan esimerkiksi projektiryhmien, loogisten toimintojen tai käytettävien sovellusten perusteella. Kytkimen kaikki portit määritellään kuuluvaksi johonkin käytettävistä olevista VLAN-verkoista. Yleislähetysviestit jaetaan samaan VLAN-verkkoon kytkettyjen laitteiden kanssa, muut laitteet eivät tällöin kyseisiä viestejä näe. Tämä parantaa verkon kokonaissuorituskykyä. VLAN-tekniikkaa voidaan käyttää kytkimessä neljällä tavalla. Näitä ovat MAC-osoitteeseen pohjautuva kytkentä, kytkimen porttiin perustuva kytkentä, verkko-osoitteeseen perustuva kytkentä sekä tietoliikenneprotokollaan perustuva kytkentä. (Cisco Systems 2002, 71.)

8.1.1 MAC-osoitepohjainen VLAN

MAC-osoitteeseen perustuvissa VLAN verkoissa, laitteet määritellään MAC-osoitteiden perusteella sama laite voi kuulua useampaan VLAN:iin samanaikaisesti. Laitteiden kesken muodostuu oma levitysviestialue. Laiteosoitteisiin pohjautuvassa tunnistamisessa edellytyksenä on, että laite on kytkettynä verkkolaitteen porttiin ja laitteen osoite pitää olla listattuna VLAN-verkon sallittujen laitteiden listalla. MAC-osoitteisiin perustuvissa VLAN-verkoissa osoitteet joudutaan lisäämään ja poistamaan käytännössä käsin, joten ylläpito tehtävät ovat työläitä, vastaavasti verkon tietoturvaa voidaan pitää hyvänä. (Kaario 2002, 237; Jaakohuhta 2002, 161.)

8.1.2 Porttikohtainen VLAN

Porttimäärittelyihin perustuvissa VLAN:ssa määritellään jokainen kytkimen portti kuuluvaksi tiettyyn VLAN:iin, tätä menetelmää käytetään yleisesti työryhmäkytkimissä. Porttikeskeisissä VLAN:ssa samaan VLAN:iin liitetyt porttien solmut saavat tunnisteena samanarvoisen VLAN ID-tunnisteen. Tällä menetelmällä työasema voi kuulua ainoastaan yhteen VLAN:iin kerralla. Jos portit hajautetaan toimimaan useamman kytkimen välillä, voi ratkaisun toteuttaa valmistajakohtaisesti. Porttikohtaisen VLAN:n toteuttaminen on helppoa, eikä vaadi ylläpitäjältä suuriakaan toimenpiteitä. (Jaakohuhta 2002, 162; Cisco Systems 2002, 71.)

8.1.3 Verkko-osoitepohjainen VLAN

Verkko-osoitteisiin perustuvat VLAN:t ovat protokollasidonnaisia, jokaisen protokollan verkko-osoitteet muodostavat omat VLAN-verkkonsa. Osoitteisiin lasketaan kaikki IP aliverkon osoitteet sekä samaan osoiteavaruuteen liitetyt laitteet. Tätä tapaa käytetään yleisesti IP-verkoissa. Useamman verkon ollessa kyseessä kullekin aliverkolle varataan yksi VLAN aliverkko ja jäljelle jäävä muiden protokollien liikenne voidaan eristää omaksi VLAN verkoiksi.

Tietoliikenneprotokolliin perustuvat VLAN:t ovat helppoja hallita, koska kytkimet hoitavat dynaamisesti laitteiden tunnistamisen laitesiirtojen yhteydessä. Tekniikan etuina voidaan pitää käyttäjien lisäämisen ja siirtämisen helppous sekä keskitetty tiedottaminen jos verkossa havaitaan esim. tuntematon käyttäjä. Haittapuolena ovat hallintatyön lisääntyminen hallintaohjelmiston tietokannan luomisessa ja ylläpidossa. (Jaakohuhta 2002, 162;Cisco Systems 2002, 73; Kaario 2002, 237.)

8.2 Virtuaalilähiverkon runkoprotokolla (VLAN Trunking Protocol, VTP)

VTP-protokollan on OSI-mallin toiselle kerrokselle sijoittuva protokolla. Sen tehtävänä on jakaa VLAN informaatiota lähiverkossa kytkimien välillä. VTP-protokollaa käyttämällä ylläpitäjä voi asentaa yhdelle kytkimelle VLAN-asetukset valmiiksi, jonka jälkeen tieto käytetyistä VLAN:sta jaetaan verkon muille kytkimille VTP-protokollan avulla. VTP-protokollan jakama VLAN informaatio pitää sisällään VLAN paketin ID-kentän sekä nimi kentän. Verkon kytkimet päivittävät omat VLAN tietonsa näiden tietojen perusteella.

VTP-protokolla toimii kolmessa tilassa, jokainen verkkokytkin asetetaan yhteen näistä tiloista. Palvelin tilassa (server mode) oleva kytkin lähettää omat VLAN tietonsa muille kytkimille, vastaavasti asiakas tilassa (client mode) oleva kytkin kuuntelee lähetyksiä ja päivittää niiden mukaan omaa VLAN -tietokantaansa. Kolmas tilan on läpinäkyvä tila (transparent mode), tässä tilassa oleva kytkin ei reagoi itse lähetettyihin VLAN -tietoihin, mutta toimii tiedon lähettäjänä eteenpäin verkossa. (Cisco Systems 2007b, 16-17.)

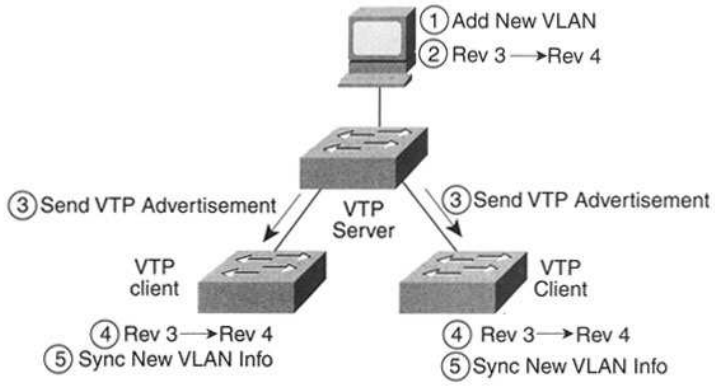
8.2.1 VTP-protokollan toiminta

Cisco Systemsin teoksessa CCENT/CCNA ICND2 kerrotaan VTP-protokollan toiminnasta. VTP-protokollan toiminta alkaa kytkimissä, jossa VTP-protokollan tilaksi on määritelty palvelin tila. VTP-palvelimena toimiva kytkin lähettää VTP-viestin omien porttiensa kautta verkkoon, VTP-protokollan lähettämät viestit kulkevat ainoastaan porteista, jotka on konfiguroitu ISL tai 802.1Q tyyppisiksi ns. trunk porteiksi. Trunk portin kautta lähetetään paketteja eteenpäin,

jotka kuuluvat useampiin VLAN-verkkoihin. Tämän jälkeen VTP-palvelimiksi ja asiakkaiksi konfiguroidut kytkimet vastaanottavat paketit ja päivittävät omat VLAN-tietokantansa näiden perusteella. Pakettien vastaanottamisen ja käsittelyn jälkeen kytkimet lähettävät VTP-päivitysviestin eteenpäin verkossa, joiden avulla verkon kytkimet päivittävät VLAN-tietonsa.

VLAN päivityspaketit kuljettavat mukanaan VLAN-tietokannan tarkistusnumeroa, jonka arvoa lisätään yhdellä jokaisen käsittelyn jälkeen. Tämän menettelyn ansioista tietokanta pysyy ajan tasalla. Kytkimet päivittävät oman tietokantansa tapauksessa, jossa kytkin vastaanottaa paketin, jonka tarkistusnumero arvo on niiden omaa tarkistusnumeron arvoa suurempi. VTP-palvelimet ja asiakkaat lähettävät VTP-viestejä viiden minuutin välein verkkoon, tällä tavoin uusi verkkoon lisätty kytkin saa päivitetyt VLAN tiedot. Kytkin vastaanottaa päivitysviestit palvelin tai asiakas tilassa toimiessaan.

Kuvassa 3 on esitetty VTP-protokollan päivitysprosessin vaiheet. VTP-palvelimelle konfiguroidaan uusi VLAN-tietokanta kohdassa 1. Tietokannan versio numero päivittyy numeroon 4 automaattisesti päivityksen yhteydessä kohdassa 2. Tämän jälkeen kytkin lähettää VTP-mainostusviestit VTP-Client kytkimille kohdassa 3, mainostusviestit sisältävät version 4 mukaisen tietokannan. Client-kytkimet huomaavat uudemmat version 4 mukaiset VTP-päivitysviestit kohdassa 4. Viimeisessä vaiheessa kohdassa 5 Client-kytkimet päivittävät omat VTP-tietokantansa uutta versionumeroa vastaaviksi.



Kuva 2: VTP-protokollan päivitysprosessin kulku (Cisco Systems 2007b,18).

VTP-pakettien lähettämisen ja vastaanottamisen onnistumisen edellytyksenä vaaditaan tiettyjä ehtoja kytkimien kesken, kytkimissä pitää olla konfiguroituna ISL tai 8021Q-standardin mukainen trunk portti ja VLAN alueen nimen on täsmättävä kytkimien tietokannassa. VTP-protokolla tukee myös salasanakäytäntöä, jos salasana on määritelty lähetyspäässä vastaanottopään kytkimessä pitää olla vastaava salasana asennettuna. Salasana kuljetetaan paketin mukana salatussa muodossa, tällä tavoin estetään ulkopuolisen ihmisen tai laitteen muuttamasta kytkimen VLAN tietoja.

VTP-protokollan läpinäkyvässä tilassa kytkin ei vastaanota itse VTP lähetyksiä vaan lähettää ne vain eteenpäin verkossa. Läpinäkyvässä tilassa olevalle kytkimelle voidaan asentaa omia VLAN tietoja, joita kytkin ei mainosta ulospäin. Tämä asetus on hyvä asentaa kytkimiin, joiden ei haluta levittävän tietoja ulospäin esim. erilaisissa laboratorioympäristöissä, joissa halutaan toimia ulkoverkosta suljetusta ympäristössä. Ainoa tapa välttää haluttaessa VTP-protokollan käyttämistä on asentaa kaikki kytkimet läpinäkyvään tilaan, koska VTP-protokollaa ei voida kytkeä pois päältä. VLAN-tietokanta tallennetaan kytkimissä tiedostoon vlan.dat, joka tallentuu FLASH-muistiin. Tämän tiedoston poistamisella ja resetoimalla kytkin toimenpiteen jälkeen, VLAN tiedot poistuvat kytkimestä. (Cisco Systems 2007b, 17-21.)

8.2.2 VTP-rajaus (VLAN Pruning)

VTP-rajauksella tarkoitetaan VTP-kehyksien lähetyksen rajaamista kytkimille, joilla ei ole portteja samassa virtuaalilähiverkossa. VTP-protokollan avulla kytkimet tekevät VLAN-rajauksen automaattisesti ja estävät VTP-kehyksien lähetykset porteistaan, joihin on kiinnitetty kytkin tai reititin, jossa ei ole kyseistä VLAN-verkkoa asennettu. Tällä menetelmällä verkkoon saadaan lisää kaistanleveyttä käyttöön, poistamalla turhia sanomalähetyksiä verkon sisällä. (Cisco Systems 2007b, 22.)

8.3 Virityspuualgoritmi (Spanning Tree Protocol, STP)

STP-protokolla on vanhin Ethernetissä käytetyistä varayhteysmenettelyistä. STP-protokollan avulla estetään silmukoiden syntyminen lähiverkossa. STP-protokollan huonona puolena voidaan pitää sen pitkää uudelleenkytkeytymisaika, jonka pituus vaihtelee 30-90 sekunnin välillä. Hyvinä puolina voidaan pitää sen kattavuutta koko verkon yli sekä sen yhteensopivuutta kaikkien laitevalmistajien kesken. STP-protokolla sopii hyvin kytkinpohjaiseen verkkoon, jossa asetukset tehdään kaikkien kytkinten välillä, joiden halutaan olevan osana verkon vikasietoista rakennetta. (Jaakohuhta 2002, 189.)

8.3.1 Virityspuualgoritmin käyttämät parametrit

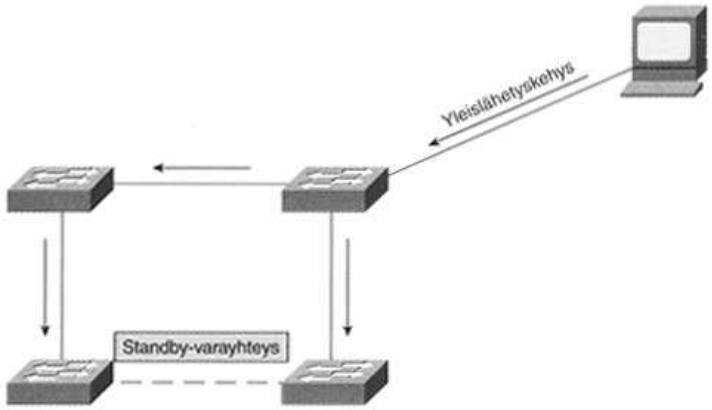
IEEE 802.1D standardi määrittää STP-protokollan käyttämät parametrit. STP-protokolla käyttää hyväkseen kaikkia protokollan alueella toimivaan laitteeseen asetettavia parametreja, kuten sillan prioriteetti, edullisin reitti, välitysviive sekä mainosviestien lähetysväli, joita käytetään verkon tilan selvittämisessä. Sillan prioriteetti (bridge priority) -parametrilla määrätään juurikytkimen asema protokollan alueella. Ellei asetusta tehdä, juurikytkimeksi valitaan laite, jolla on pienin MAC-osoitteen arvo. Edullisin reitti (path cost) -parametrilla määrätään edullisin reitti kytkimeltä juurikytkimeen. Välitysviive (forward delay)

-parametrilla määritellään aika, minkä kuluessa verkko palautuu toimintakykyiseksi verkon topologiamuutoksen jälkeen. Mainosviestien lähetysväli (hello time) -parametrilla määritellään aika, minkä kuluessa protokollan alueella olevat laitteet viestittävät toisilleen olemassaolostaan. Oletuksena parametrin arvona käytetään kahta sekuntia. (Internet Engineering Task Force 2004.)

8.3.2 Virityspuualgoritmin toiminta

STP-protokollan toiminta määritellään standardissa IEEE 802.1D. STP-protokollan toiminta perustuu verkon topologiamuutoksien havaitsemiseen. Muutokset voidaan havaita alueelta, jossa virityspuualgoritmi on otettu käyttöön verkkolaitteiden välillä. Tämä tarkoittaa käytännössä sitä, että virityspuualgoritmi huolehtii siitä, että jokaisen verkkolaitteen välillä ainoastaan yksi yhteys voi olla kytkettynä samanaikaisesti. Samanaikaisten yhteyksien ollessa auki yhtä aikaa muodostuu Ethernet verkkoon silmukka, joka aiheuttaa verkon tukkeutumisen pakettien kiertäessä loputtomasti laitteiden välillä.

STP-protokollan toiminta on esitetty kuvassa 4. Kuvassa on havainnollistettu tilanne, jossa kahden alemman kytkimen välinen yhteys toimii varayhteytenä tilanteessa, jossa liikenteen välitys ylempien kytkimien kautta on katkennut.



Kuva 3: Virityspuualgoritmin toiminta (Cisco Systems 2002, 499).

STP-protokollan aluetta hallitaan kytkimellä, joka toimii juurikytkimenä tai juurisiltana (root bridge). Juurikytkimestä eteenpäin laitteiden kesken muodostuu puumainen rakenne verkosta. Juurikytkimeksi valitaan verkosta kytkin, jolla on korkein prioriteetti eli pienin numeroarvo MAC-osoitteessa. Juuren valitsemisen jälkeen verkkoon määritellään varajuurikytkin, joka toimii juurikytkimenä tilanteessa jossa juurikytkin ei ole käytössä.

Juuren ja varajuuren valinnan laitteet hoitavat normaalitilanteessa automaattisesti, mutta ylläpitäjä voi myös määritellä asetukset manuaalisesti.

Juurikytkin lähettää verkkoon säännöllisesti BPDU (Bridge Protocol Data Unit) -paketteja, selvittääkseen verkossa vallitsevan tilan ja mahdollisen tarpeen muutoksille. Vikatilanteen syntyessä kytkimet estävät hyötyliikenteen kulkemisen ja avaavat varayhteyden laitteiden välille, jossa katkos on havaittu. Kytkimet selvittävät tämän jälkeen yksikäsitteisen reitin verkkolaitteiden välille, jonka jälkeen liikenne päästetään kulkemaan normaalisti uutta reittiä pitkin. Normaalisti edellä mainittuun prosessiin kuluu aikaa verkon hierarkiasta riippuen noin 30-90 sekuntia. (Internet Engineering Task Force 2004.)

Ciscon teoksessa CCNA/ICND 2 määritellään STP-protokollan porttiroolien valintamenettelyn toiminta. STP-protokollassa porttien roolien valinta tapahtuu siten, että jokaiselle kytkimien porteille määritellään rooli. Juurikytkimen portit ovat aina ohjaavassa tilassa (forwarding state). Muiden kytkimien portteja, joilla on edullisin reitti juurikytkimeen, kutsutaan juuriporteiksi (root port). Nämä portit ovat ohjaavassa tilassa. Jokaisen verkkosegmentin kytkintä, jolla on edullisin yhteys juurikytkimeen, kutsutaan määritetyksi sillaksi (designated bridge). Tähän kytkimeen yhdistettyä porttia kutsutaan määritetyksi portiksi (designated port). Tämä portti asetetaan ohjaavaan tilaan. Kaikki muut kytkimien portit asetetaan tämän jälkeen estävään tilaan (blocking state).

STP-protokollan toiminta on kolmivaiheinen, ensimmäisessä vaiheessa verkosta valitaan juurikytkin, jonka portit asetetaan ohjaavaan tilaan. Toisessa vaiheessa määritellään muille verkon kytkimille juuriportit, jotka asetetaan ohjaavaan tilaan. Viimeisessä vaiheessa määritellään muille kytkimille määritetyt portit, jotka asetetaan ohjaavaan tilaan. Loput portit asetetaan tämän jälkeen estävään tilaan.

STP-protokollan havaitessa vikatilanteen verkossa algoritmi, muuttaa porttien tiloja. STP-protokollassa porteilla on viisi erilaista tilaa, ohjaavassa tilassa portti toimii normaalisti ja välittää dataa. Toinen päätila on estävä tila, jossa tiedon välitys portista estetään. Porttien siirtyessä näiden kahden tilan välillä portit käyvät läpi kaksi tilaa, joita ovat kuunteleva tila (listening state) sekä oppiva tila (learning state). Kuuntelevassa tilassa portti ei ohjaa dataa vaan odottaa tietoa uusista MAC taulun-osoitteita, jotka ovat tässä tilassa vanhentuneita. Oppivassa tilassa portti ei ohjaa dataa, mutta saa tietoja uusista MAC-osoitteista. STP-protokollan havaitessa verkossa vikatilanteen, estävässä tilassa oleva portti siirtyy kuuntelevaan tilaan, josta se jatkaa oppivan tilan kautta ohjaavaan tilaan. Normaalitilanteessa portin siirtyminen estävästä tilasta ohjaavaan tilaan kestää noin 50 sekuntia. Viive koostuu 30 sekunnin siirtymäajasta sekä BPDU-viestien lähetysviiveestä, joiden pituus yhteensä kestää noin 20 sekuntia. (Cisco Systems 2007b, 65,69-71,75.)

8.3.3 Virityspuualgoritmin lisäominaisuudet

STP-protokollaan on kehitetty vuosien aikana muutamia lisäyksiä. Näistä tärkeimpiä toiminnallisia parannuksia ovat Ciscon kehittelemät EtherChannel kanavointi, PortFast porttitila, sekä portin BPDU Guard ja Root Guard toiminnallisuudet. Nämä toiminnallisuudet ovat esitelty Ciscon teoksessa CCNA/ICND2.

Etherchannel kanavoinnin tarkoituksena on välttää verkossa tapahtuvaa viivettä vikatilanteessa. Tämä saavutetaan yhdistämällä verkkosegmentit toisiinsa kahdella rinnakkaisella linkillä. Tästä johtuen linkin katkeamisessa johtuvaa viivettä ei synny, jos toinenkin linkeistä pysyy ylhäällä. Tämä vähentää tilanteita, jossa STP-protokolla aiheuttaa verkkoon viivettä. STP-protokolla käyttää Etherchannel linkkiä yhtenä liitäntänä, jolloin kaikki portit ovat ohjaavassa tai estävässä tilassa. EtherChannel kanavoinnin avulla kaikki rinnakkaiset linkit toimivat yhtä aikaa ja tarjoavat verkkoon lisää kapasiteettiä.

PortFast tarkoittaa tilaa, jossa kytkimen portti asettuu välittömästi ohjaavaan tilaan välittämättä STP-protokollassa olevista porttien tiloista. PortFast voidaan kytkeä verkossa ainoastaan verkon päätelaitteisiin kuten tietokoneisiin tai palvelimiin, josta ei ole yhteyttä STP-protokollaa käyttävään verkkolaitteeseen.

BPDU-tilaa käytetään lisäämään verkon tietoturvallisuutta. Kytkimen portti, joka asetetaan BPDU Guard-tilaan, asettuu automaattisesti estävään tilaan havaittuaan verkosta lähetetyn BPDU-viestin. Tällä tavoin estetään verkon ulkopuolisen laitteen saamasta juurikytkimen asemaa. Uhkana voivat olla myös ulkopuolisen kytkimen asentaminen verkkoon verkkoliikenteen tarkkailemiseksi tai ylimääräisten verkkotukosten aiheuttamistarkoituksessa. Tämäntyyppisiä ongelmia voidaan estää sulkemalla kytkimen portti välittämästä liikennettä. BPDU–Guard ominaisuutta käytetään yleisesti päätelaiteissa, jotka eivät ole yhteydessä muihin verkkolaitteisiin yhdessä PortFast-tilan kanssa.

Root Guard ominaisuudella estetään verkkoon lisätyn uuden ulkopuolisen kytkimen lähettämät BPDU-viestit. Root Guard ominaisuus estää ylempiasteisen naapurikytkimen lähettämät BPDU-viestit tapauksessa, jossa bridge ID arvo on suurempi kuin olemassa olevalla juurikytkimellä. Kyseinen portti ei käsittele tässä tapauksessa BPDU-viestiä ja portti sulkeutuu ohjaamasta liikennettä. (Cisco Systems 2007b, 76-78.)

8.4 Nopea virityspuualgoritmi (Rapid Spanning Tree Protocol, RSTP)

RSTP-protokolla kehitettiin vuoden 2001 lopulla, suurin syy tähän oli normaalin STP-protokollan hitaus. RSTP-protokollan standardi tunnuksena käytetään merkintää IEEE 802.1w. RSTP-protokollan toimintaperiaate on sama kuin normaalin STP-protokollan ja se määritellään myös standardissa 802.1D. RSTP-protokolla valitsee aluksi juurikytkimen samoilla periaatteilla kuin normaali STP-protokolla. Tämän jälkeen muille kytkimille valitaan lyhin reitti juurikytkimelle ns. root port sekä designated port. Lopuksi valitaan mitkä portit ovat ohjaavia portteja sekä mitkä portit asetetaan suljettuun tilaan. RSTP-protokollan suurin etu on sen nopeus vaihtaa porttien tiloja verkkoon ilmestyvän vian seurauksena. RSTP-protokolla pystyy reagoimaan verkon muutoksiin normaalitilanteessa alle 10 sekunnin viiveellä, koska sen ei tarvitse odottaa tilojen välistä viestien vaihtoa.

RSTP-protokollassa porttien tilat eroavat STP-protokollan vastaavista. RSTP-protokollassa portit ovat joko ohjaavassa tilassa (forwarding state) tai hylkivässä tilassa (discarding state). Hylkivä tila eroaa STP-protokollan sulkevasta tilasta siinä, että se ei ohjaa dataa, mutta kuuntelee BPDU-pakettiviestejä. RSTP-protokolla käyttää myös oppivaa tilaa siirtyessä ohjaavan ja hylkivän tilan välillä, mutta protokolla käyttää tilaa ainoastaan lyhyen ajan.

RSTP-protokollassa kytkimen portit käyttävät samoja rooleja kuin STP-protokollassa juuriportin ja määrätyn portin osalta. Porttien roolit toimivat samoin kuin STP-protokollassa juuri portit sekä määrätyt portit asetetaan ohjaavaan tilaan ja muut portit asetetaan estävään tilaan. RSTP-protokolla käyttää lisäksi vaihtoehtoista roolia (alternative state), jonka tarkoituksena on määrittää paras vaihtoehtoinen reitti juuriportille, tämä portti asetetaan hylkivään tilaan. RSTP-protokolla käyttää myös varaportti (backup port) roolia, joka otetaan käyttöön tapauksessa, jossa kytkimestä on kytketty kaksi porttia samaan segmenttiin. Varaportti roolin omaavan portin tilaksi määritellään normaalitilanteessa hylkivä, vikatilanteessa kytkin vaihtaa määritetyn portin tilalle portin rooliksi varaportti. (Internet Engineering Task Force 2004.)

9 Reititys (Routing)

Reitityksellä tarkoitetaan tapaa, jolla IP-paketti löytää oikean reitin lähdeverkosta kohdeverkkoon paketin osoitetietojen perusteella. IP-reititys muodostuu kahdesta eri prosessista, ensimmäisessä prosessissa paketit välitetään mekaanisesti reitittimen läpi tuloportista lähtöporttiin reititystaulun reititystietojen perusteella. Tästä prosessista käytetään nimitystä forwarding. Toisessa prosessissa reititysprotokollat välittävät reititystaulun tietoja IP-verkon reitittimien välillä eri menetelmillä reititysprotokollasta

riippuen. Tästä prosessista käytetään nimitystä routing. IP-pakettien välitys suoritetaan verkkojen välillä jaksottaisesti. Pakettia käsittelevä reititin välittää paketin aina oikeaan suuntaan seuraavalla reitittimelle, joka jatkaa paketin ohjausta seuraavaan kohteeseen. Näin jatketaan kunnes paketti etenee oikealle reitittimelle, joka sijaitsee IP-paketin kohdeverkossa. Reititin ei siis tiedä paketin koko reittiä, ainoastaan seuraavan kohteen. (Kaario 2002, 82.)

9.1 Reitityksen periaate

Teoriatasolla sovelluksen lähettäessä pakettia eri verkossa olevaan kohteeseen sovellus vastaanottaa siirtoyhteyskehyksen. Verkkoprosessi tutkii tämän jälkeen otsikon ja päättelee paketin kohdeverkon. Tämän jälkeen prosessi tutkii reititystaulun tietojen perusteella oikean reitin paketille. Alkuperäinen kehys hylätään tämän jälkeen ja paketti kapseloidaan uudestaan liitännän siirtoyhteyskehykseen ja talletetaan jonoon odottamaan toimitusta seuraavaan kohteeseen. Tämä prosessi suoritetaan polun jokaisessa reitittimessä, kunnes paketti saapuu reitittimelle, joka on liitetty kohteena olevaan verkkoon. Paketti kapseloidaan lopuksi kohdeverkon siirtoyhteys kehyksellä ja toimitetaan perille kohdeverkkoon.

Reititysprotokollat levittävät tietoa mainostusviestien avulla. Mainostusviestit eroavat keskenään käytetystä reititysprotokollasta riippuen. Tästä johtuen Internet joudutaan jakamaan osiin, joissa käytetään aina tiettyä reititysprotokollaa. Näiden osien ns. autonomisten alueiden sisällä suositellaan käytettäväksi määrättyä protokollaa kaikissa verkkolaitteissa. Alueiden rajoilla käytetään vastaavasti reitittimiä, jotka pystyvät välittämään tietoa eri protokollien kesken. Autonomisten järjestelmän sisäisistä protokollista käytetään nimitystä IGP-protokolla (Interior Gateway Protocol) ja järjestelmien välisistä protokollista nimitystä EGP-protokolla (Exterior Gateway Protocol).

Autonomisiin järjestelmiin kuuluu tavallisesti yhden yrityksen omistama ja hallinnoima verkko. Suurimmat yritykset voivat omistaa ja esimerkiksi valtion laitokset voivat omistaa monia autonomisia järjestelmiä. Kansainvälinen yhtiö ICANN (Internet Corporation for Assigned Network Numbers) huolehtii internet osoitteiden jakamista autonomisille järjestelmille. Järjestelmille myönnetään järjestelmä numero ASN (autonomous system number), jolla voidaan erotella organisaatiot toisistaan ja varmistamaan myös se, että paketit eivät ohjaudu samaan verkkoon toistamiseen. (Cisco Systems 2002, 19-20;Cisco Systems 2007a, 451;Kaario 2002 82-83.)

9.2 Reititystaulun toiminta

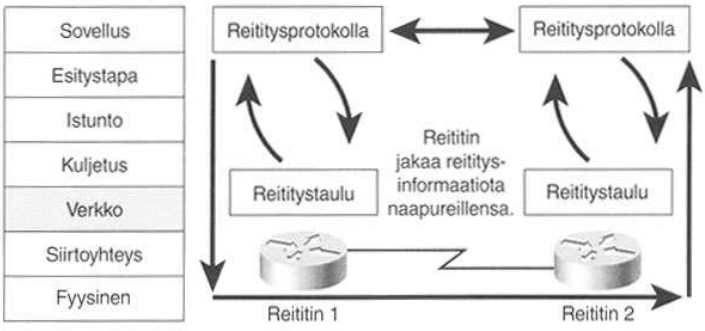
Reititin käyttää reititystaulua hyväkseen reititystä tehdessään. Reititin lukee vastaanotetusta IP-paketista IP-otsikon kohdeosoitteen. Reititystaulun sisältö järjestetään tämän jälkeen maskin pituuden mukaan laskevaan järjestykseen, jolloin tarkemmin määritetyt reitit tulevat taulussa ylimmäiseksi. Reititin aloittaa reittien käsittelemisen taulun yläosasta, tämän jälkeen taulun läpikäynti koostuu kahdesta vaiheesta. Laura Chappellin teoksessa Cisco Reitittimet, kerrotaan reititystaulun toimintalogiikasta.

Reitittimien toiminta koostuu kahdesta vaiheesta:

1 Reititin tutkii taulun rivi riviltä ylhäältä alaspäin.

2 Oikea reitti löytyy jos kohteen IP-osoitteen ja rivin aliverkkomaskin AND-operaation tuloksena saadaan rivin reittiosoitteen tulos.

Tätä vaihetta jatketaan niin kauan kunnes reititin löytää ensimmäisen täsmäävän osoitteen reititystaulusta. Oikean reitin löydyttyä, reititin tutkii rivillä olevia muita tietoja kuten, seuraavan hypyn osoite kenttää ja seuraavan hypyn kenttäkuvausta. Näiden tietojen perusteella reititin osaa välittää IP-paketin oikeaan osoitteeseen käyttämällä oikeaa porttia. Jos osoite löytyy reitittimen omasta verkosta, reititin käyttää MAC-osoitetta ohjaamaan paketin oikealle verkkolaitteelle. Reitityksen kaksi päätoimintavaihetta on havainnollistettu kuvassa 5.



Kuva 4: Reitityksen toiminta (Chappell 2002, 84).

Oletusreitillä määritellään reitti reitittimeen, jonka kautta pystytään ohjaamaan tuntemattomat paketit eteenpäin. Oletusreitti määritellään reititystauluun tilanteessa, jossa reitityksessä käytettävää seuraavan hypyn tietoa ei ole määritelty. Oletusreitin tarkoitus on ohjata tässä tilanteessa, tuntemattomat paketit käyttäen tätä reittiä. Verkon ylläpitäjä määrittää staattiset reitit lisäämällä ne käsin reititystauluun. (Chappell 2002, 83; Kaario 2002, 84.)

9.3 Reititykseen liittyvät protokollat

Reitityksessä käytetään apuna OSI-mallin verkkokerrokselle sijoittuvia protokollia. Seuraavat protokollat ovat välttämättömiä TCP/IP-verkoissa, ne avustavat pakettien reitityksessä ja osoitteiden selvityksessä.

9.3.1 DHCP-protokolla (Dynamic Host Control Protocol)

DHCP-protokollan toiminta määritellään RFC-dokumentissa 2131. DHCP-protokolla toimii verkossa jakamassa IP-osoitteita automaattisesti verkkoon lisätyille laitteille. DHCP-protokolla asennetaan palvelinkoneelle, josta se toimii asiakas/palvelin periaatteella. DHCP-protokollan toiminta edellyttää aina palvelimena toimivan laitteen. Protokollan toiminta etenee seuraavasti, ensimmäisessä vaiheessa verkkoon lisätty uusi laite lähettää DISCOVER-sanoman yleislähetyksenä, jolla se hakee itselleen IP-osoitetta. Sanomaan vastaa DHCP-palvelin, joka hallitsee kyseisen alueen verkkolaitteita. Seuraavassa vaiheessa palvelinkone lähettää asiakas koneelle OFFER-sanoman, jolla se tarjoaa IP-osoitetta laitteelle. Asiakas kone voi tämän jälkeen, joko hyväksyä osoitteen REQUEST-sanomalla tai kieltäytyä osoitteesta DECLINE-sanomalla. Viimeisessä vaiheessa palvelinkone vahvistaa osoitteen varauksen ACK-sanomalla, jos asiakaskone on hyväksynyt tarjouksen. Verkkotopologian muuttuessa kesken neuvottelun, voi palvelinkone myös lähettää negatiivisen kuittauksen NAK-sanoman muodossa.

Neuvottelujen päätteeksi asiakaskone saa uuden IP-osoitteen, joka on voimassa siihen määritellyn varausajan mukaisesti. IP-osoite voidaan vapauttaa myös manuaalisesti sammuttamalla kone tai pyytämällä uutta IP-osoitetta. Tässä tapauksessa DHCP-protokolla lähettää RELEASE-sanoman palvelimelle. DHCP-protokolla sisältää myös INFORM-sanoman, jota käytetään tilanteessa, jossa asiakaskone tarvitsee lisämäärityksiä. (Internet Engineering Task Force 1997b.)

9.3.2 ARP-protokolla (Address Resolution Protocol)

ARP-protokollan toiminta määritellään RFC dokumentissa 826. ARP-protokollan tehtävänä lähiverkoissa on verkkolaitteen MAC-osoitteen selvittäminen laitteen IP-osoitteen perusteella. ARP-protokolla lähettää verkkoon ARP-kyselyn, jonka avulla protokolla tiedustelee kyseisen laitteen MAC-osoitetta. ARP-protokolla lähettää ARP-kyselyn Broadcast-lähetyksenä verkkoon. Kysely sisältää IP-osoitteen, jonka Ethernet osoitetta halutaan selvittää sekä kyselyn lähettämän koneen IP-osoitteen. Laite joka omistaa kyselyn kohteena olevan IP-osoitteen vastaa kyselyyn lähettämällä vastauksena oman IP-osoitteensa sekä oman MAC-osoitteensa. ARP-protokollan vastaanotettua halutun MAC-osoitteen, osoite tallennetaan laitteen ylläpitämään ARP-tauluun. Tallennuksen jälkeistä säilytysaikaa on mahdollista säätää manuaalisesti, oletuksena ARP-kyselyn tieto tallentuu tauluun löytyneiden laitteiden osalta 20 minuutiksi, verkosta löytymättömien laitteiden tieto pysyy taulussa ainoastaan kolme minuuttia. (Internet Engineering Task Force 1982.)

9.3.3 ICMP-protokolla (Internet Control Message Protocol)

ICMP-protokollan toiminta määritellään RFC dokumentissa 792. ICMP-protokollaa käytetään verkossa, viestien välittämiseen vikatilanteissa. ICMP-protokolla käsittää noin kolmekymmentä erilaista sanomaa, jota käytetään hyväksi ilmoittamassa pakettien perillemenosta. Sanomat jaetaan kahteen ryhmään ICMP-virhesanomiin sekä ICMP-kyselyihin. Yleisempiä ICMP-sanomia ovat kaiutukset (echo), joita esimerkiksi ping ja traceroute ohjelmat käyttävät. Näillä ohjelmilla voidaan mm. testata verkko-osoitteen olemassaoloa tai selvittää mitä reittiä paketti kuljetetaan kyseiseen osoitteeseen. Toinen yleinen sanomatyyppi on saavuttamasta kohteesta ilmoittavat sanomat, jotka ilmoittavat pääasiassa teknisen syyn miksi paketti ei saavuttanut kohteena olevaa verkkoa. Näistä sanomista yleisimpiä ovat esimerkiksi seuraavat ilmoitukset. Net Unreachable, joka kertoo sen, että reittiä kyseiseen verkkoon ei tiedetä. Host Unreachable-viestillä kerrotaan, että kohteena olevaa konetta ei löydetä verkosta, Protocol Unreachable-viesti kertoo lähettäjän protokollan olevan tuntematon ja Port Unreachable-viesti kertoo puolestaan, että käytettävää porttinumeroa ei löydetä. (Internet Engineering Task Force 1981c.)

9.3.4 DNS-protokolla (Domain Name System Protocol)

DNS-protokollan toiminta määritellään RFC dokumentissa 920. DNS-protokollan tarkoitus on toimia internet IP-osoitteiden muuttamisessa kirjoitetuiksi internet osoitteiksi esim. http://www.laurea.fi sekä päinvastoin. DNS-protokolla toimii hajautetusti kuormituksen jakamiseksi sekä tietoturvan kannalta. DNS-protokollan avulla internet osoitteet jaetaan

moniin hierarkkisiin toimialueisiin, jotka vastaavasti jaetaan alitoimialueisiin. Ylimmän alueen toimialueet muodostuvat esimerkiksi kaupallisista osoitteista, joiden päätteinä käytetään lyhennystä .com. Muita ylemmän tason osoitteita ovat esimerkiksi. maiden osoitteiden tunnukset kuten suomen .fi, ei kaupalliset organisaaiot .org sekä yhdysvaltojen koulutuslaitokset .edu ja hallintolaitokset .gov. Toisen tason toimialue nimiin luetaan kuuluvaksi mm. yrityksien, tuotenimien sekä oppilaitosten osoitteet kuten http://www.helsinki.fi/yliopisto. Kolmannen tason käyttäminen on vapaaehtoista, sillä voidaan erotella mm. oppilaitoksen tai yrityksen osastojen väliset sivut toisistaan.

DNS kyselyt toimivat hierarkkisesti, jolloin ne ohjautuvat aluksi oman tason nimipalvelimelle, josta ne ohjataan yksi porras kerrallaan ylemmälle tasolle. Tätä toimintoa jatketaan niin kauan kunnes osoitteen ensimmäinen tunnettu osa löydetään. Puumaisen hierarkian ansioista osoitehierarkian ylin osa pystyy tunnistamaan kaikki mahdolliset ylimmät osoitetunnisteet. Osoitteen alkuosan tunnistamisen jälkeen osoitteen seuraavaa osaa lähdetään selvittämään hierarkiassa alaspäin kunnes osoite on kokonaisuudessaan tunnistettu. Osoitteen tunnistamisen jälkeen kohdeosoite muutetaan IP-osoitteeksi ja paketti voidaan reitittää verkossa oikealle laitteelle. (Internet Engineering Task Force 1984.)

9.4 Staattinen reititys (Statical routing)

Staattinen reititys tarkoittaa manuaalista reititystä, jota ylläpitäjä hallitsee. Reitittimelle syötetään halutut reitit käsin ja niitä ylläpidetään manuaalisesti. Ylläpitäjä joutuu myös päivittämään reititystiedot aina verkkotopologian muuttuessa. Staattisella reitityksellä vähennetään verkon ylikuormitusta, koska reititystietoja ei tarvitse lähettää se myös antaa ylläpitäjälle mahdollisuuden rajata, mitä verkon osia mainostetaan. Staattinen reititys lisää vastaavasti ylläpitäjän työtä, mitä suurempaa verkkoa ylläpitäjä hallitsee, sitä enemmän konfigurointi työtä aiheutuu sen ylläpidosta.

Staattista reititystä voidaan käyttää etenkin verkkoturvallisuutta vaativissa verkoissa, jossa tarvitaan verkko-osioiden salaamista. Toinen käyttötarkoitus on ns. stub verkot, jotka tarkoittavat verkkoja, joihin pääsyyn käytetään ainoastaan yhtä reittiä. Staattinen reititys ei riitä suurissa tai monimutkaisissa verkoissa, sen ylläpitoon kuluvan ajan vuoksi. (Cisco Systems 2002, 20;Chappell 2002, 82.)

Staattinen reitti määritellään Ciscon reitittimissä käskyllä *ip route* globaalissa konfiguraatiotilassa. Komento ip route muodostuu kolmesta osasta, *ip route* komennon jälkeen lisätään haluttu verkko-osoite, jonne reitti halutaan luoda sekä aliverkon maski kyseiseen verkkoon. Viimeisenä osana lisätään liitännän tunnus tai ip-osoite minkä kautta reitti halutaan ohjata ns. Next Hop Address. Esimerkiksi käsky *ip route 10.100.100.0*

255.255.255.0 10.100.10.5 lisää reitittimelle reitin verkkoon 10.100.10.0, joka käyttää maskia 255.255.255.0. Reititin ohjaa liikenteen kyseiseen verkkoon käyttämällä ensimmäisenä porttina omaa porttiaan, jonka osoite on 10.100.10.5. (Cisco Systems 2007b, 182-183.)

9.5 Staattinen oletusreitti (Static default route)

Oletusreitillä tarkoitetaan reittiä, joka täsmää kaikkien lähetettävien pakettien kanssa. Oletusreitti on hyödyllinen tapauksessa, jossa yksi reititin reitittää kaikkea verkosta lähtevää liikennettä eteenpäin yhtä reittiä pitkin. Oletusreitillä määritellään osoite, minne paketti ohjataan tapauksessa, jossa paketin kohdeosoite on tuntematon. (Cisco Systems 2007b, 186.)

Staattinen oletusreitti määritellään Ciscon reittimiin käytämällä käskyä *ip route* globaalissa konfiguraatiotilassa ja antamalla tämän jälkeen kohdeverkon osoitteeksi ja maskiksi neljä peräkkäistä 0 numeroa, syystä että staattisessa oletusreitissä kohdeverkkoa ei tiedetä. Seuraavan hypyn osoite eli portti tai portin ip-osoite määritellään viimeisenä. Staattinen oletusreitti reitittimen portin *10.100.10.5* kautta määritellään esimerkiksi seuraavalla käskyllä *ip route 0.0.0.0 0.0.0.0 10.100.10.5*. Komennolla *show ip route*, pääkäyttäjätilassa tehtynä, saadaan listattua reitittimen reititystaulun sisältö. Reitittimen reititystaulusta löytyvät kaikki reitittimeen konfiguroidut staattisen reitit sekä oletusreitit. (Cisco Systems 2007b, 186-187.)

9.6 Luokallinen ja luokaton reititys

Oletusreitti tulkitaan reitittimissä reititystavan mukaan. Ciscon reitittimet käyttävät termejä luokallinen (classfull) sekä luokaton (classless) reititys. Luokattomassa reitityksessä reititin käyttää oletusreitin osoitetta aina tilanteessa, jossa paketin osoite on epäselvä. Luokallinen reititys käyttää oletusreittiä samoilla perusteilla kuin luokaton reititys, poikkeuksena on tilanne, jossa reititin löytää paketin osoitteen toisten reittien kautta.

Osoitteen tulkitseminen eroaa edellisissä reititystavoissa hieman toisistaan. Luokattomassa reitityksessä IP-osoite jaetaan kahteen osaan aliverkko osaan sekä isäntä osaan. Luokattomat reititysprotokollat mainostavat myös jokaisen aliverkon aliverkkomaskia paketin mukana. Luokattomia reititysprotokollia ovat mm. RIPv2, EIGRP sekä OPSF-protokollat. Luokalliset protokollat jakavat osoitteen kolmeen osaan verkko-osaan, aliverkko osaan sekä isäntä osaan. Luokallisten protokollien verkko-osoite jakautuu aina A, B sekä C osoiteluokkajaon perusteella. Luokalliset protokollat eivät myöskään lähetä aliverkkotietoja lähetyksissään, näihin protokolliin kuuluvat mm. VLSM, RIPv1 sekä IGRP-protokollat. (Cisco Systems 2007b, 190-191.)

9.7 Reititystaulun hallinta

Cisco Systemsin teoksessa CCNA/ICND2 käydään läpi reititystaulun toimintaa. Reititystaulun koon hallitsemisessa reitittimet käyttävät menetelmää nimeltään reittien yhteenveto (route summarization). Route summarization-menetelmä pitää reititystaulussa olevat reitit järjestyksessä niiden verkko-osoitteiden perusteella. Menetelmän avulla voidaan vähentää reititystaulujen reittien määrää korvaamalla monet samaan verkkoon menevät reitit yhdellä reitillä, joka sisältää kaikkien aiempien reittien osoitteet. Tätä menetelmä käyttäen saavutetaan reititystaulujen koon vähentyminen, reitittimen muistinkäyttöä voidaan vapauttaa sekä vähentää verkon konvergenssia. Manuaalisessa reitityksessä, reittien yhteen kokoamisen suorittaa verkon ylläpitäjä.

Luokallista reititysprotokollaa käyttävät reitittimet eivät mainosta aliverkkomaskin tietoa muille laitteille. Sen sijaan ne käyttävät menetelmää nimeltä autosummarization. Tämän menetelmän avulla luokallista reititysprotokollaa käyttävät reitittimet, joilla on yhteys vähintään yhteen A, B tai C-luokan verkkoon, mainostavat muille laitteille yhtä reittiä koko verkko osoitteella toiseen verkkoon. Tämän menetelmän avulla reitittimet osaavat reitittää paketin oikeaan osoitteeseen.

Tilanteessa, jossa luokallisesta verkosta lähetetty paketti joutuu kulkemaan vähintään yhden aliverkon yli, jossa käytetään eri luokallista aliverkkoa, autosummarization menetelmä joudutaan poistamaan käytöstä. Tästä verkosta käytetään termiä (distinguous network), koska reititin ei osaa tehdä eroa esimerkiksi kahden 10.0.0.0/8 verkon välillä ilman aliverkkomaskimääritystä. Autosummarization menetelmän käyttö on pakollista luokallisissa protokollissa, jolloin edellä mainitussa tilanteessa joudutaan siirtymään luokattoman protokollan käyttöön. (Cisco Systems 2007b, 211,218-219,220-222.)

9.8 Dynaaminen reititys (Dynamical routing)

Dynaaminen reititys toimii automaattisesti, ylläpitäjän työksi jää ainoastaan dynaamisen reitityksen kytkeminen päälle. Tämän jälkeen reititysprosessi hoitaa tietojen päivittämisen automaattisesti verkon topologian muuttuessa. Dynaaminen reititys mahdollistaa reititystaulujen automaattisen muodostamisen ja ohjauksen nopeasti ja ilman virheitä, joita staattisessa reitityksessä voi tapahtua. Dynaamisessa reitityksessä reitittimet vaihtavat keskenään päivitystietoja reitittimien välillä päivitysprosessin aikana. Dynaamisen reitityksen toiminta perustuu reititysprotokollien suorittamaan tiedonvälitykseen. Reititysprotokollan avulla määritellään miten reititystietojen päivityksiä lähetetään, mitä tietoa päivityksissä

jaetaan, miten usein päivityksiä lähetetään sekä miten tietojen vastaanottajat paikallistetaan verkosta. (Cisco Systems 2002, 20; Chappel 2002, 83,85.)

9.9 Reititysprotokollat

Cisco Systemsin teoksessa CCNA/ICND2 sekä K, Kaarion teoksessa TCP/IP-verkot kuvataan reititysprotokollien toimintaa. Reititysprotokollien tehtävänä on hoitaa kommunikointia reitittimien kesken ja pitää reitit kaikkiin aliverkkoihin järjestyksessä tietyn periaatteen mukaisesti. Reititysprotokolla jakaa reitittimelle tarvittavat tiedot reititystä varten siten, että reitittimet osaavat lähettää pakettiin kohdeverkkoa kohti ilman reitityssilmukoiden syntymistä. Reitityssilmukoita varten IP -paketit sisältävät Time to Live-kentän (TTL). Tämän kentän avulla pystytään eliminoimaan reitityssilmukoiden syntyminen. TTL-kenttään asetettu numeerinen arvo, vähentyy jokaisella reitittimellä ja arvon saavuttaessa nollan paketti poistuu verkosta. Paketin poistamisesta tiedotetaan paketin lähettäjälle, ICMP (Internet Control Messaging Protocol) -protokollan avulla.

Reititysprotokollat on jaettu ryhmiin useampaan ryhmään. Reititysprotokollien jako voidaan tehdä, joko protokollan teknisen toteutuksen mukaan tai protokollan tehtävän mukaan, tehtävän mukaan perustuvassa jaossa protokollat erotellaan autonomisten järjestelmien sisäistä sekä niiden välistä tiedonsiirtoa hoitaviksi.

EGP-protokollat hoitavat reititystä autonomisten järjestelmien välillä. Ne hoitavat reittejä ulkomaailmaan, joista ollaan yhteydessä moniin erityyppisiin järjestelmiin. Näitä protokollia hallitsevat puhelinyhtiöt ja muut palveluntarjoajat, näistä yleisin on BGP (Border Gateway Protocol) -protokolla.

IGP-protokollat hoitavat reititystä autonomisten järjestelmien sisällä. Nämä ovat tyypillisiä reititysprotokollia lähiverkossa. Nämä protokollat voidaan jakaa kahteen toiminnalliseen luokkaan etäisyysvektori protokolliin (distance vector protocol) sekä linkkitila protokolliin (link state protocol).

Lähiverkoissa voidaan käyttää useampaa reititysprotokollaa yhtä aikaa. Tässä tapauksessa reititysprotokollat asetetaan järjestykseen, niiden ominaisuuksien kesken. Tästä menetelmästä käytetään nimitystä hallinnollinen etäisyys (administrative distance). Etäisyys määritellään numeroarvolla, joka kertoo protokollan uskottavuudesta yksittäisellä reitittimellä. RIP-protokollan administrative distance arvoksi on määritelty 120 ja OSPF-protokollan arvoksi 90. Luotettavimmaksi reititysmuodoksi arvolla määritellään staattinen reititys, joka saa arvon 1. Luotettavin mahdollinen tapa yhdistää kaksi reititintä saadaan yhdistämällä kaksi laitetta suoraan kaapelilla toisiinsa, tämä saa pienimmän mahdollisen

arvon 0. Administrative Distance arvon muuttaminen reitittimessä yksittäisten reittien tai protokollien kesken on mahdollista tarvittaessa. (Cisco Systems 2007b, 316-317;Kaario 2002, 87-88.)

9.10 Etäisyysvektoriprotokolla

Etäisyysvektoriin pohjautuvat algoritmit jakavat kopioita reititystaulustaan muille reitittimille verkossa. Reitittimet reagoivat verkon topologia muutoksiin välittömästi ja ilmoittavat niistä muille reitittimille. Tämä tapahtuu käytännössä seuraavasti, verkkoreitittimen vastaanotettua reititystaulun toiselta samassa verkossa olevalta reitittimeltä, reititin lisää etäisyysvektorin numeroarvoa. Tämän jälkeen reititin siirtää taulun eteenpäin toiselle naapurilleen. Prosessi toistetaan verkkoreitittimien kesken kaikkiin suuntiin. Tämän menetelmän avulla algoritmi kokoaa tietoa verkosta ja sen etäisyyksistä ja pitää niiden avulla topologiatietokantaa. Etäisyysvektoriprotokollia ovat mm. RIPv1 (Routing Information Protocol) ja siitä uudempi kehitetympi versio RIPv2 (Routing Information Protocol version 2). (Chappell 2002, 88-89.)

9.10.1 Konvergenssin määritelmä

Termillä konvergenssi määritellään verkon suorituskykyä vikatilanteessa. Verkon tilan muuttuessa reitittimet käynnistävät prosesseja, joilla muuttunut tilaa rekisteröidään.Tämän jälkeen suunnitellaan uudet reitit sekä muutetaan reititystaulun sisältö vastaamaan uusia reittejä. Koko tätä prosessiketjua kutsutaan verkossa tapahtuvaksi konvergenssi ilmiöksi. Konvergenssi kertoo verkon toipumisesta vikatilanteessa, osa verkoista konvergoituu nopeammin osa hitaammin. Konvergenssiin vaikuttavia tekijöitä ovat mm. verkossa käytetyt laitteet ja protokollien tukemat ominaisuudet sekä verkon topologia. (Cisco Systems 2007a, 455.)

9.10.2 Virheenkorjaus etäisyysvektoriprotokollissa

Laura Chappelin teoksessa Cisco Reitittimet kuvataan virheenkorjauksen toimintaa etäisyysvektoriprotokollissa. Verkon konfiguraatiossa tapahtuneet virheet tai hidas konvergenssi voivat aiheuttaa verkossa reitityssilmukoita. Reititysprotokollissa on kehitelty mekanismeja, joilla reitityssilmukat voidaan eliminoida verkosta. Virheellisten päivitysten ja pakettien loputon kiertäminen verkossa aiheuttaa loputtoman silmukan ns. count to infinity tilanteen. Tämän estämiseksi IP-pakettiin on lisätty TTL-kenttä, jonka arvoa vähennetään paketin ohittaessa yksittäisen reitittimen verkossa. TTL-arvon saavuttaessa nollan, reititin poistaa paketin verkosta. Protokollat määrittävät TTL-arvoksi tietyn maksimiarvon, joka asetetaan paketille ennen sen lähettämistä verkkoon. Tämä arvo eroaa protokollasta riippuen, esimerkiksi RIP-protokolla asettaa arvoksi 16. Tällä menettelyllä

etäisyysvektoriprotokollat toimivat itse korjaavina protokollina. Virheenkorjaus ei ole kuitenkaan välitöntä, vaan tapahtuu viiveen kanssa, jolloin verkossa voi olla silmukka rajatun ajan.

Split horizon toiminta perustuu sääntöön, joka estää reititysprotokollien mainostamisen takaisin paketin tulosuuntaan. Tämän säännön avulla reititin ei yksinkertaisesti salli liikenteen mainostusta takaisin sen tulosuuntaan. Tarkoituksena on estää turha liikenteen mainostaminen takaisin laitteille, joista liikennettä mainostetaan jo kyseiselle reitittimelle. Split horizon säännön käänteinen muoto Poison Reverse sääntö, pyrkii estämään reitityssilmukoita kopioitumisen epäselvää reittiä pitkin. Reitittimen havaitessa epäselvän reitin se asettaa reitin tavoittamattomaksi, jolloin muut virheelliset mainostukset toista reittiä pitkin eivät saavuta reititintä. Reititys silmukka havaitaan verkossa, jos paketin metric-arvo huomataan kasvavan riittävän korkealle. Reitti poistetaan, mikäli paketin Metric-arvo kasvaa 1.1 kertaiseksi normaalista.

Tilanteessa, jossa verkossa huomataan vikatilanne ja reititin on ns. myrkyttänyt reitin toiselle laitteelle, käytetään ns. liipaistua päivitystä (triggered update). Tämän mekanismin avulla reititin voi lähettää oman reititystaulunsa tiedot rinnakkaisille reitittimille välittömästi vian havaittuaan. Normaalitilanteessa päivitysviestejä lähetetään noin 30 sekunnin välein, joka aiheuttaa viivettä verkossa. Verkon muut reitittimet puolestaan lähettävät liipaistuja päivityksiä eteenpäin aaltoina, jotka leviävät nopeasti koko verkkoon. Tällä menetelmällä kaikki verkon laitteet saavat nopeasti tiedon verkossa tapahtuvasta viasta.

Hold Down-ajastin on virheenkorjaus toiminto, joka estää päivitysviestien leviämisen verkossa normaalisti. Hold Down-ajastimen avulla viallinen reitti pidetään suljettuna, asettamalla reittiin kohdistuvat päivitysviestit kielletyksi tietyksi aikaa. Hold Down-ajastin poistuu käytöstä seuraavissa tilanteissa, joko ajastimeen määrätty aika kuluu loppuun, reititin vastaanottaa toimivan päivityksen kyseisestä verkosta tai toiselta naapurireitittimeltä saapuu alkuperäistä reittiä paremman Metric-arvon omaava päivitys. (Chappell 2002, 92-96.)

9.10.3 Virheenkorjauksen toiminta

Cisco Systemsin teoksessa CCNA/ICND2 määritellään virheenkorjausmekanismien toimintajärjestys:

1 Reititin lähettää päivitystietoja verkkoon tietyin väliajoin. Päivitysväli määrittyy protokollan mukaan esimerkiksi RIP-protokolla käyttää päivitysvälinä 30 sekuntia. Päivityksiä lähetetään koko verkon alueelle, poislukien split horizon säännöllä kielletyt reitit.

2 Topologiamuutoksen sattuessa verkossa reititin, joka huomaa muutoksen myrkyttää reitin, jossa havaitaan muutos. Tämän jälkeen reititin lähettää välittömästi liipaistun päivityksen, joka sisältää tiedot kyseisestä reitistä.

3 Verkko reititin, joka vastaanottaa liipaistun päivityksen myrkyttää kyseisen reitin omasta portistaan. Tämän jälkeen reititin lähettää liipaistun päivityksen eteenpäin verkossa.

4 Reitittimet lähettävät poison reverse viestin takaisin reitittimelle, mistä poison route viesti saapui. Tämän ansioista reitittimet eivät vastaanota jatkossa viallisia reittimainostuksia.

5 Kaikki reitittimet asettavat viallisen reitin pitoon ja käynnistävät Hold-Down ajastimen. Reitittimet eivät vastaanota mitään tietoa reittiä pitkin Hold-Down ajastimen ollessa käynnissä. Viesti vastaanotetaan reittiä pitkin ainoastaan tapauksessa, jossa se saapuu reitittimeltä, jolta alkuperäinen viesti lähetettiin.

(Cisco Systems 2007b. 331-332.)

9.11 RIP (Routing Information Protocol) -reititysprotokolla

RIP-protokolla oli ensimmäinen kehitelty etäisyysvektoriprotokolla 1980-luvulla. RIP-protokollan reititystoiminta perustuu verkkojen välisten hyppyjen lukumäärään laskemiseen. Protokolla tukee maksimissaan 15 hyppyä, tämän arvon ylittävä hyppymäärä tarkoittaa ääretöntä määrää hyppyjä. RIP-protokolla lähettää muiden reititysprotokollien tavoin reittien päivitysviestejä verkkoon, tämä tapahtuu 30 sekunnin välein, vastaamattomiin viesteihin protokolla reagoi asettamalla hyppyjen lukumääräksi äärettömän ja poistamalla kyseisen reitin reititystaulustaan. (Kaario 2002, 90-91.)

RIP-protokollan toiminta määritellään RFC-dokumentissa 1058. Protokollan toiminta perustuu RIP-pyyntöjen avulla tapahtuvaan tiedonvaihtoon. Pyyntöön vastaava reititin käy läpi oman reititystaulunsa sisällön RIP-pyynnön tietueiden mukaisesti. Tämän jälkeen pyyntöön vastataan viestillä, jossa hyppyjen määräksi asetetaan arvo, joka kyseisellä reitittimellä on etäisyytenä haluttuun kohteeseen. Kenttään asetetaan arvo ääretön, jos reititin ei löydä haluttua reittiä. Protokolla pystyy lähettämään myös koko reititystaulunsa sisällön toiselle reitittimelle, tällöin lähetetään tätä tarkoitusta varten luotu RIP-pyyntö. (Internet Engineering Task Force 1988.)

9.12 RIPv2-protokolla

Nykyisin reitittimissä käytetään RIP-protokollasta kehiteltyä versiota, josta käytettään lyhennystä RIPv2. RIPv2-protokollan toiminta määritellään RFC-dokumentissa 2082. RIPv2 tärkeimmät uudistukset ovat mahdollisuus aliverkkomaskiin liittyvän tiedon siirtämiseen sekä seuraavan hypyn osoitteen siirtämiseen. Ilman näitä kahta ominaisuutta reititys on nykypäivän tietoverkoissa mahdotonta, koska aliverkkomaskin avulla pystytään erottelemaan ulkoverkon ja sisäverkon osoitteet IP-osoitekentästä. (Kaario 2002, 91.)

RIPv2-protokollaan sisällytettiin uusina kenttinä aliverkkomaskikenttä sekä seuraavan hypyn IP-osoitekenttä. Lisäksi tilaa varattiin routing domain kentälle, jolla määrätään autonomisen järjestelmän numero EGP-protokollaa varten. RIPv2-protokolla tukee myös 16-bittistä selväkielistä salausta tarvittaessa autentikoitujen reittien päivityksessä. RIPv2-protokolla kuormittaa vähemmän isoja verkkoja, koska päivityssanomat lähetetään Multicast lähetyksinä. (Internet Engineering Task Force 1997a.)

RIPv2–protokolla voidaan ottaa käyttöön Ciscon reitittimissä komennolla *router rip*. Käsky annetaan Global-config tilassa. Komennon jälkeen reititin siirtyy reitittimen konfiguraatiotilaaan (config-router). Tämän jälkeen RIP–protokolla määritellään käyttämään protokollan versiota kaksi käskyllä *version 2*. RIPv2-protokollan mainostamat verkot määritellään seuraavaksi. Haluttu verkko saadaan mainostukseen komennolla *network,* johon lisätään haluttu verkko-osoite ilman aliverkkomaskia. Esimerkiksi käsky *network 10.0.0.0.* lisää verkon 10.0.0.0. mainostukseen.

RIP–protokollan toimintaa voidaan seurata reititystaulun informaation perusteella. Käskyllä *show ip route rip* reititin listaa reititystaulusta RIP–protokollan tuntemat reitit. Käskyllä *show ip protocols* voidaan tutkia RIP–protokollan konfiguraatiotietoja sekä naapurireitittimien IP-osoitteita, joilta reititin on oppinut reittejä. Kaikki käskyt annetaan pääkäyttäjätilassa. (Cisco Systems 2007b, 459-460,462-463; Hakala & Vainio 2005, 280.)

9.13 EIGRP (Enchanced Interior Gateway Protocol) -reititysprotokolla

Cisco Systemsin teos CCNA/ICND 2 sekä Hakala & Vainion teos Tietoverkon rakentaminen käsittelevät EIGRP-protokollan toimintaa. EIGRP–protokollaa voidaan pitää kehittyneenä etäisyysvektoriprotokollana, mutta sille on määritelty myös oma kategoria hybridi reititysprotokolla, joka määräytyy erityisesti sen toiminnan perusteella. EIGRP on suosituin dynaaminen reititysprotokolla suurissa verkoissa. Se käyttää reitityksen perusteena suorituskykyyn perustuvia mittalukuja. Suorituskyvyn mittaluvun laskemiseen käytetään useita

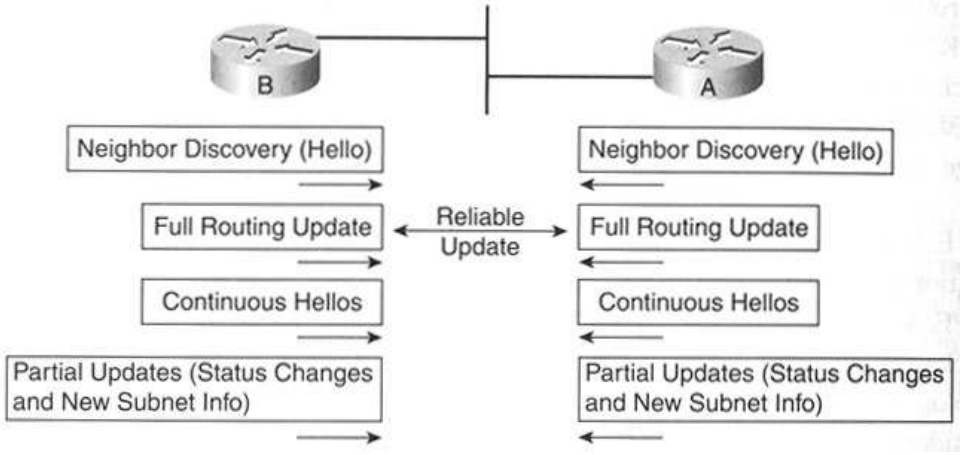
muuttujia painotuskertoimen perusteella. Painotuskertoimena voidaan korostaa tiettyjä asioita, joita verkon ylläpitäjä voi määritellä. Painotuskertoimeksi voidaan määritellä esimerkiksi yhteyden nopeus, kuormitus tai luotettavuus.

EIGRP–protokolla lähettää Hello-viestejä, joiden perusteella naapurussuhteet muodostetaan, Hello-viestejä lähetetään viiden sekunnin välein tai minuutin välein riippuen verkon nopeudesta. Hello-viestien avulla varmistetaan yhteyden toimivuus, jos Hello–viestiin ei kuulu vastausta reititin odottaa Hold Time-asetuksella määritetyn ajan, jonka jälkeen yhteys määritellään katkenneeksi. Normaalitilanteessa reititin määrittää Hold Time-viestien viiveeksi kolme kertaa Hello-viestien lähetykseen kulutetun ajan.

EIGRP–protokollan toiminta perustuu kolmeen tärkeään seikkaan naapuristosuhteiden ylläpitämiseen Hello–viestien avulla, verkkotopologiaa koskevaan tietojen vaihtoon päivitysviestien avulla sekä reitityksen tekemiseen suorituskyvyn perusteella. Näiden kolmen tehtävän perusteella EIGRP–protokolla muodostaa reititystaulut. Reititin kirjaa reititystauluun kaikki reitit omiin naapureihinsa ja topologiatauluun puolestaan kirjataan kaikki naapurireitittimien alaisten verkkojen topologiatiedot.

EIGRP–protokolla käyttää naapurissuhteiden tunnistamisessa järjestelmä numero (ASN, Autonomous System Number) -parametria, joka on täsmättävä reittimissä, joiden kesken naapuristosuhteet muodostetaan. Toisena ehtona reitittimen käyttämän IP–osoitteen pitää täsmätä naapurireitittimen sallimien IP–osoitteiden kanssa. Ehtojen täytyttyä reititin voi aloittaa verkkotopologiakohtaisen tiedon välittämisen.

Topologiatietoa välitetään päivitysviestien avulla, jotka lähetetään Unicast–viestillä jos kohteena on yksittäisen verkon reittipäivitys tai Multicast-viestillä. Jos tarkoituksena on päivittää useampia reittejä yhtäaikaisesti. Päivitysviestit lähetetään joko täydellisinä päivityksinä, jotka pitävät sisällään reitittimen kaikki tiedossa olevat reitit tai osittaisina päivityksinä, jolloin viestissä mainitaan ainoastaan muuttunut verkon reitti. Täydellisiä päivityksiä lähetetään ainoastaan verkon muodostamisen yhteydessä, jolloin kaikki reitittimet muodostavat omat taulunsa. EIGRP-reititysprotokollan lähettämät päivitysviestit on esitetty kuvassa 6. (Cisco Systems 2007b, 380-382;Hakala & Vainio 2005, 286-287.)



Kuva 5: EIGRP-protokollan toiminta (Cisco Systems 2007b, 382).

Topologiataulu sisältää tiedot kohdeverkoista ja niihin johtavista reiteistä, reittitiedon lisäksi topologiataulussa on tieto suorituskykytiedoista kyseiseen verkkoon. Suorituskykytietoa käytetään hyväksi mittaluvun (cost) laskemisessa. Mittaluvun perusteella valitaan paras reitti jokaiseen verkkon, parhaasta reitistä käytetään nimitystä (feasible path). Parhaalle reitille valitaan myös varareitti (feasible successor), jonka kokonaiskustannus on toiseksi paras kuhunkin verkkoon. Yhteydelle määritellään myös kokonaiskustannus (reported distance), joka ilmoittaa kustannuksen, jonka naapurireititin on yhteydelle ilmoittanut.

EIGRP–protokolla pitää yllä tietoja ainoastaan kaikista seuraavan hypyn reitittimille vaihtoehtoisista reiteistä, eikä välitä sitä kauemmista reiteistä. Reitin valitsee vaihtoehtoisista reiteistä parhaan ja toiseksi parhaan reitin joita käytetään reitityksessä varareittinä. Tämä mahdollistaa hyvän vikasietoisuuden ja nopean konfergenssi ajan vikatilanteissa. Reititin valitsee vaihtoehtoisen reitin, katkennen reitin tilalle noin 2 sekunnissa.

EIGRP–protokolla käyttää DUAL (Diffusing Update Algorithm) -algoritmia tapauksessa, jossa reitittimen reitti katkeaa eikä varareittiä ole määritelty. DUAL–prosessi käyttää kysely viestejä (query messages) hyväkseen ja tarkistaa niiden avulla, ettei uusi valittu reitti muodosta looppia reitityksessä. Uusi reitti otetaan käyttöön, kun se on todettu looppi vapaaksi reitiksi. DUAL–algoritmin käyttö vie aikaa maksimissaan noin 10 sekunnin verran. (Cisco Systems 2007b, 386-388;Hakala & Vainio 2005, 287.)

EIGRP–protokolla käynnistetään reitittimessä käyttämällä käskyä *router eigrp (+) prosessin numero* globaalissa konfigurointitilassa. Prosessitunnuksella erotellaan reitittimessä toimivat EIGRP prosessit toisistaan. Prosessitunniste numeroa käytetään samalla myös autonomisen järjestelmän tunnuksena. EIGRP-reititysprosesseja voidaan ajaa reitittimessä yhtäaikaisesti

useita, mutta prosessit eivät vaihda keskenään reititystietoa. Reitittimet, joiden kesken reititystä tehdään, on konfiguroitava käyttämään samaa prosessinumeroa. Router eigrp käskyn jälkeen reititin siirtyy reitittimen konfigurointi tilaan, jossa voidaan määritellän EIGRP-protokollan verkot, joita käytetään mainostuksessa. Verkot määritellään luokallisina osoitteina käyttämällä käänteistä maskia esimerkiksi käskyllä *network 10.100.10.0 0.0.0.255* EIGRP-protokolla mainostaa verkkoa 10.100.10.0 muille reitittimille.

EIGRP-protokollan toimintaa voidaan seurata monella tavoin, pääkäyttäjätilassa annetuilla käskyillä. Käskyllä *show ip route eigrp* saadaan selville kaikki reitittimen reititystaulussa olevat EIGRP-reitit. Käsky *show ip eigrp neighbors* näyttää kaikki reitittimen naapurireitittimet, joiden kanssa on luotu naapurussuhteet. Reitittimen EIGRP-topologia taulua voidaan tarkastella käskyllä *show ip eigrp topology* ja reitittimien välistä EIGRP-protokollien välistä liikennettä käskyllä *show ip eigrp traffic*. Reaaliaikaisesti EIGRP-protokollassa tapahtuvaa pakettien kulkua reitittimessä voi seurata käskyllä *debug ip eigrpf packet*. (Cisco Systems 2007b, 396-397;Hakala & Vainio 2005, 288,291,293.)

9.14 Linkkitilaprotokolla

Linkkitilareititys perustuu monimutkaiseen topologiatietokantaan, jolla linkkitila-algoritmi pitää yllä tietoa kauemmista reitittimistä ja niiden keskinäisistä yhteyksistä. Linkkitilareititys käyttää hyväkseen linkkitilapaketteja (link state packets), topologiatietokantaa, SPF (shortest path first) -algoritmia ja sen muodostamaa puurakennetta olemassa olevasta verkon yhteyksistä.

Yhteystilaprotokollat keräävät verkosta linkkitilatietokantaa, joiden perusteella reititystaulut muodostetaan. Tämän jälkeen SPF-algoritmin avulla muodostetaan lyhin mahdollinen yhteys linkkien välillä. Linkkitilareitityksessä verkon kaikki reitittimet jakavat saman kuvan verkosta. Tämä menetelmä nopeuttaa virheistä toipumisaikaa. Linkkitilaprotokollista yleisin käytössä oleva protokolla on OSPF (Open Shortest Path First). (Chappell 2002, 98;Kaario 2002, 92-94.)

9.15 OSPFv2 (Open Shortest Path First) -reititysprotokolla

Yleisimpänä yhteystilaprotokollana IP-verkoissa käytetään OSPFv2-protokollaa. OSPF-protokollan toiminta perustuu yhteystilatietokannan ylläpitämiseen. OSPF-protokollan nykyisin käytössä olevan version 2 toiminta määritellään RFC dokumentissa 2328. Yhteystilatietokanta on tietokanta, johon kerätään tietoja verkon reitittimien yhteystilatiedoista. OSPF-protokolla käyttää verkon reitittimien väliseen reitin selvitykseen yhteystila algoritmia ns. Dijkstran algoritmia. Tämä algoritmi muodostaa reitittimien välisen

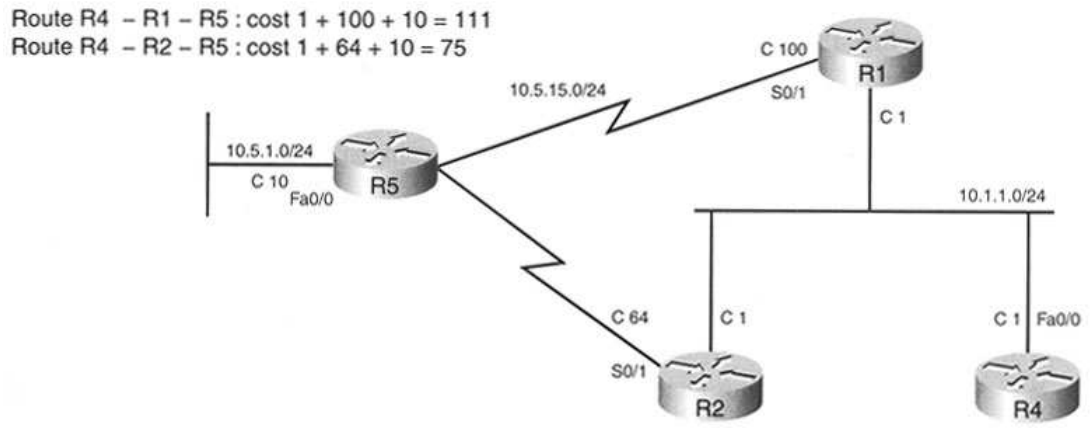
reitin tietyillä perusteilla. OSPF-protokollassa algoritmi käyttää reitin määritykseen lyhintä mahdollista reittiä. Algoritmin toimintaa perustuu kahteen päävaiheeseen:

1 Ensimmäisessä vaiheessa reititin mainostaa omia reittejään verkkoon käyttäen yhteystilamainostus viestiä (link state advertisement, LSA). Viesti lähetetään tilanteessa, jossa verkon tilanteeseen tapahtuu muutos. Viesti sisältää tiedot uudesta verkon tilanteessa ja se lähetetään kaikille verkossa oleville reitittimille. Verkkoalueen reitittimet vastaanottavat LSA-viestin ja kopioivat sen eteenpäin verkossa.

2 Toisessa vaiheessa reitittimien saatua tiedon verkon uudesta tilanteesta, jokainen reititin laskee algoritmia käyttämällä lyhimmät yhteydet verkon kaikkiin laitteisiin. Algoritmi mahdollistaa reitityksen ilman reitityssilmukoiden syntymistä. Algoritmin suorittamisen jälkeen reitittimet päivittävät reititystaulunsa uusilla reititystiedoilla.

(Internet Engineering Task Force 1998a.)

OSPF-protokollan reitinvalitsemisprosessi esitetään kuvassa 7. Kuvan tilanteessa reitittimeltä R4 on mahdollista kuljettaa paketteja reitittimelle R5 kahta vaihtoehtoista reittiä pitkin. Reitittimen R1 kautta reitin hinnaksi muodostuu arvo 111 ja reitittimen R2 kautta arvo 75. Reititin valitsee tämän jälkeen näistä kahdesta reitistä paremman mahdollisen reitin, joka tässä tapauksessa kulkee reitittimen R2 kautta.



Kuva 6: Reitin valitsemisprosessi OSPF-reitityksessä (Cisco Systems 2007b, 357).

9.15.1 OSPF-protokollan naapurussuhteet

Ciscon teoksessa CCNA/ICND2 sekä K,Kaarion teoksessa TCP/IP-verkot esitetään miten OSPF-protokollan naapurisuhteet luodaan. Reitittimet jatkavat toimintaan yllä kuvatulla tavalla aina verkon tilanteen muuttuessa. Tämän lisäksi reitittimet lähettävät sanomia keskenään,

joiden avulla verkon toimintakuntoa tarkkaillaan. Näihin viesteihin kuuluvat Hello-viestit, joiden avulla reitittimet viestivät toisilleen toimintakunnossa olostaan. Hello interval sanoman arvo kertoo reitittimelle, kuinka usein Hello-viestejä lähetetään. Router dead interval sanomalla puolestaan todetaan reititin epäkuntoiseksi.

OSPF-verkko toipuu virheistä nopeasti, normaalitilanteessa siihen kuluu aikaa noin 40 sekuntia. Tämä aika muodostuu oletusasetuksilla router dead interval sanoman 10 sekunnin viiveestä, johon lisätään router dead interval sanoman nelinkertainen aika verrattuna edelliseen viestiin.

Isommissa verkoissa naapurisuhteita ei luoda yleensä kaikkien reitittimien kesken, mistä aiheutuu paljon liikennettä. Ylläpitäjä voi halutessaan määritellä verkkoon määritellyn reitittimen (designated router, DR). Tämä reititin toimii verkossa kaikkien muiden reitittimien naapurina. Reitittimen avulla saadaan tieto kaikkien sen alueella olevien muiden reitittimen tilasta. Tälle reitittimelle valitaan yleisesti myös vara reititin (Backup Designater Router, BDR), joka toimii DR-reitittimenä tilanteessa, jossa alkuperäiseen DR-reitittimeen tulee vikatilanne.

DR-reititin valitaan alueelle käyttäen DR-reitittimen valintamenettelyä hyväksi. Tässä menettelyssä reitittimien kesken valitaan reititin, joka toimii jatkossa DR-reitittimenä tietyin valintaperustein. Alla on esitelty valintaperusteet reitittimen valinnalle.

1 Reititin, jonka Hello viesti pitää sisällään korkeimman OSPF-prioriteetin valitaan DR-reitittimeksi.
2 Jos OSPF-prioriteetti on tasan, DR-reitittimeksi valitaan reititin, jonka Hello-viestin ID-kentän arvo on korkein.
3 BDR-reitittimeksi valitaan normaalitilanteessa reititin, jonka OSPF-prioriteetti on toiseksi korkein.
4 OSPF-prioriteetin arvon ollessa 0 reititintä ei voida valita.
5 Myöhemmin lisätty reititin, joka voittaisi valintaperusteluissa aiemman DR tai BDR-reitittimen ei korvaa aiemmin valittuja reitittimiä.

DR-reitittimen valintaan vaikuttaa oleellisesti laitteiden käynnistysjärjestys ja kohdan 5 mukaan uusi laite ei korvaa vanhaa reititintä. Tästä voi aiheutua ongelmia verkossa esimerkiksi tapauksessa, jossa uusi nopea reititin on tarkoitus lisätä DR-reitittimeksi verkkoon. Tästä syystä hitaiden reitittimien prioriteetti arvo on syytä muuttaa käsin tarpeeksi alhaiseksi tai arvoon 0. (Cisco Systems 2007b, 350,354;Kaario 2002, 94-95,99-100.)

9.15.2 OSPF-alueet

Isoissa verkoissa, jotka pitävät sisällään yli 10 reitintä OSPF-protokollan reitittimet jaetaan alueisiin. Alueet numeroidaan nollasta ylöspäin. Numerointi on vapaata alueesta 1 ylöspäin, aluetta 0 käytetään ns. backbone alueena, joihin kaikki muut alueet yhdistetään. Tällä tavoin verkon kapasiteettia voidaan jakaa pienempiin osiin ja alueiden sisäisten reitittimien (Internal Router), käsittelemän tiedon määrä pysyy suhteellisena.

Aluejaon seurauksena reitittimet määritellään eri rooleilla. ABR (Area Border Router) -reititin vastaa kyseisen alueen yhteyksistä ulkopuolella. Tässä reitittimessä on tiedot kaikista alueista, joihin reitittimen oma alue on yhdistetty. ABR-reititin sijaitsee kahden alueen välisellä rajalla. ABR-reitittimeksi valitaan yleisesti verkon tehokkaimmat reitittimet, koska ne käsittelevät useimpien alueiden tietoja. ASBR (Autunomous System Border Router) -reititin sijoitetaan kahden alueen välille, jotka käyttävät toisena reititysprotokollana muuta kuin OSPF-protokollaa. ASBR-reitittimien avulla liikenne mahdollistetaan eri protokollien välillä. (Cisco Systems 2007b, 358-359;Kaario 2002, 94,98.)

9.15.3 OSPF–protokollan konfigurointi

OSPF–protokollassa samoin kuin EIGRP–protokollassa voidaan käyttää monia rinnakkaisia prosesseja yhtäaikaisesti. Prosessit erotellaan toisistaan käyttämällä prosessinumeroa. Prosessien erottelemiseksi toisistaan, yhdessä reitittimessä ei voi olla kahta samaa numeroa, mutta muiden reitittimien kohdalla numerolla ei ole väliä, numeron ollessa kokonaisluku väliltä 1-65535.

OSPF–protokolla käynnistetään reitittimessä käskyllä *router ospf (+) prosessinumero* globaalissa konfiguraatiotilassa. Reititin siirtyy tämän jälkeen reititysprotokollan konfigurointi tilaan, jossa määritellään OSPF–protokollan mainostuksessa käyttettävät verkot. Esimerkiksi käskyllä network 10.100.10.1 0.0.0.255 area 0, konfiguroidaan OSPF–protokolla mainostamaan verkkoa 10.100.10.0 alueelle 0. Alue määritys kertoo, sen missä alueessa reititin halutaan toimimaan, reitittimet joiden halutaan liikennöivän keskenään, on sijoitettava saman alueen sisälle. Poikkeuksen tähän tekevät ABR (Area Border Router) -reitittimet, joiden tarkoitus on toimia kahden alueen välissä. Käskyssä käytetään käänteistä maskia jossa maskin merkintätapa 0.0.0.255 tarkoitta, että osoitteen viimeisen oktetin tilalla voi esiintyä mikä tahansa bitti.

OSPF–protokollan toimintaa voidaan seurata käskyllä *shop ip route ospf*, jolla reititin listaa kaikki OSPF–protokollan oppimat reitit reititystaulusta. Käsky *show ip ospf neighbor* listaa

reitittimen käyttämän alueen numeron liitäntäkohtaisesti ja alueella toimivat muut reitittimet, joiden kanssa tapahtuu liikennöintiä. Reaaliaikaisesti OSPF–protokollassa tapahtuvaa pakettien kulkua reitittimessä voidaan seurata käskyllä *debug ip ospf packet*. (Cisco Systems 2007b, 363,366-367,375;Hakala & Vainio, 2005, 285.)

9.16 Pääsylistat (Access List, ACL)

Ciscon teoksessa Cisco Verkkoakatemia sekä Laurea Chappelin teoksessa Cisco reititimet kerrotaan pääsylistojen käyttötavoista. Pääsylistat tarjoavat tehokkaantyökalun verkon hallinnassa ja tietoturvan ylläpidossa. Niillä voidaan hallita lähiverkon tietoturvaa joustavasti ja tarkasti, poikkeuksena muista tietoturva menetelmistä kuten salasanoista tai fyysisistä tietoturva ratkaisuista. Pääsylistat rajaavat verkkoliikenteen pakettikohtaisiin kategorioihin, jotka sallivat tai kieltävät liikennettä eri ominaisuuksien perusteella. Pääsylistoja käytetään yleisesti seuraavissa tarkoituksissa:

1 Pakettien priorisoinnissa ja mukautetussa jonotuksessa. Priorisoinnin avulla mahdollistetaan pakettien käsittely reitittimessä protokollan perusteella, ennen muun liikenteen käsittelyä.

2 Reitityspäivitysten rajoittamisessa ja vähentämisessä. Näiden rajoitusten avulla voidaan estää tietystä verkosta saapuvien päivitysten ja informaation leviäminen verkon läpi.

3 Dial-on-demand reititysyhteyksiä vaativien pakettien tunnistamisessa. Tämän tunnistusmenetelmän avulla voidaan estää turhien WAN-linkkien muodostuminen verkon ulkopuolelle.

4 Perustason tietoturvan tarjoamisessa verkkoon. Pääsylistojen avulla mahdollistetaan koneen pääsy verkon yksittäiseen osaan ja samanaikaisesti voidaan kieltää toisen koneen pääsy samaan verkko-osaan.

5 Verkkoliikenteen sallimisessa ja estämisessä liikennetyypin perusteella. Pääsylistoilla voidaan estää esimerkiksi sähköposti tai internet liikenne, mutta sallia samoilta koneilta Telnet-muotoinen liikenne.

Pääsylistojen tekemään pakettien prosessointia voidaan käyttää myös muista syistä, joita ovat:

1 IP-liikenteen dynaaminen hallinta ns. lukko ja avain ominaisuuden avulla, jolla mahdollistetaan laajennettu käyttäjähallinta.

2 Pakettien identifioimisessa kryptausta varten.

3 Pakettien identifioimisessa sallittujen Telnet-yhteyksien muodostamista varten reitittimen virtuaalipäätteille.

(Chappell 1999, 308:Cisco Systems 2002, 151.)

9.16.1 Pääsylistan toiminta

Cisco Systemsin teoksessa Cisco Reitittimet sekä Hakala & Vainion teoksessa Tietoverkon rakentaminen käsitellään pääsylistojen toimintaa. Pääsylistoja käytetään lähiverkkoreitittimissä ja palomuurilaitteissa. Niiden avulla määritellään käyttöoikeuksia lähiverkkoon ja verkkolaitteisiin rajoittamalla verkkoliikenteen ja päivitystietojen kulkua. Pääsylistat jaetaan kahteen ryhmään niiden ominaisuuksien perusteella vakiolistoihin (Standard list) ja laajennettuihin listoihin (Extended list).

Pääsylistat kiinnitetään reitittimen porttiin, jossa pääsylistaa kertoo reitittimelle, millaista tietoa sisältämä paketti päästetään portista läpi ja mikä tieto hylätään. Liikenteen rajoittamista voidaan tehdä paketin lähdeosoitteen, kohdeosoitteen tai porttinumeron mukaan. Pääsylistan toiminta perustuu näiden ehtojen perusteella tehtävään liikenteen rajoittamiseen. Pääsylista toimii reitittimessä tarkkailemalla kaikkea reitittimeen portteihin saapuvaa liikennettä ja soveltamalla pääsylistan ehtoja liikenteeseen. Reititin tutkii liikennettä yksittäinen paketti kerrallaan ja päättää prosessin jälkeen täyttääkö paketti pääsylistan ehdot. Ehdot täyttävä paketti reititetään portista eteenpäin, muussa tapauksessa paketti hylätään. Pääsylistoja luodaan kaikelle liikenteelle reititysprotokollasta riippumatta. Protokollakohtaista reititystä tehtäessä vaaditaan yksittäiset asetukset kaikille protokollille. Käytännössä tämä tarkoittaa erillisten pääsylistojen tekemistä jokaiselle protokollalle.

Pääsylistoja voidaan asettaa yhteen tai useampaan liitäntään ja ne voidaan konfiguroida suodattamaan ulos menevää liikennettä sekä sisäänpäin tulevaa liikennettä. Ulospäin menevän liikenteen suodatus on tehokkaampaa, koska sisäänpäin tulevan liikenteen pääsylista käy läpi kaikki paketit ennen niiden kytkemistä ulosmenevään liitäntään. Pääsylistoissa käytetään numerointia, joka jakautuu protokollien perusteella sarjoihin, esimerkiksi IP-

protokolla käyttää peruslistoissa numeroita väliltä 1-99 ja IP-protokollan laajennetut listat käyttävät numeroita väliltä 100–199. (Cisco Systems 2002, 150,156;Hakala & Vainio, 2005, 348.)

9.16.2 Standardi pääsylista (standard access-list)

Vakiolistoja käytetään tilanteessa, jossa kaikki liikenne halutaan estää tietystä verkosta, isäntä koneelta tai protokollasta tai sallia liikenne tietystä verkosta. Standardi pääsylista käy läpi pakettien lähdeosoitteet, jonka perusteella reititystoiminta tehdään. Reititys koskee tällöin koko protokollaperhettä, joka voidaan kieltää verkon, aliverkon tai osoitteen perusteella. (Cisco Systems 2002, 161.)

9.16.3 Standardin pääsylistan konfigurointi

Standardit pääsylistat käyttävät numerointia 1-99 ja niiden luomiseksi käytetään komentoa access list. Täydellinen komennon syntaksi on seuraavanlainen *access list (pääsylistan numero) permit / deny lähdeosoite (lähdejokerimaski) log*. Permit ja deny komennot määrittävät sen onko lista kieltävä vai salliva lista. Esimerkki kieltävästä listasta on seuraava, komennolla access list 1 deny 192.168.1.0 0.0.0.255 estetään liikenne 192.168.1.0 verkon osoitteista. Permit -komennolla voidaan vastaavasti sallia kaikki liikenne kyseisestä verkosta. Log-komennolla voidaan käynnistää kirjaus toiminto, jolloin reititin kertoo viiden minuutin välein, reitittimen läpi kulkeneiden sallittujen ja kiellettyjen pakettien määrän. Listojen tekemisessä tärkeää on muistaa, että lista ehtojen jälkeen kaikki listat sisältävät aina näkymättömän kieltolauseen (implicit deny), jolla kielletään kaikki muu liikenne, jota ei ole erikseen määritelty. Tällöin lista, joka ei sisällä yhtään ainuttakaan riviä määrityksiä, kieltää aina kaiken läpikulkevan liikenteen.

Pääsylistaa koskevien määrityksen asettamisen jälkeen pääsylista kiinnitetään haluttuun liitäntään. Pääsylista kiinnitetään liitäntään käyttämällä komentoa *ip access-group (pääsylistan numero) in / out*. IP access-group-käskyn avulla pääsylista kiinnittyy haluttuun liitäntään, määritykset in / out kertovat sen, kumpaan suuntaan menevää liikennettä halutaan estää. In määritys estää liitännästä ulos menevää liikennettä ja out määritys liitännästä sisään tulevaa liikennettä. Komennolla *ip access group 1 out* standardi pääsylista 1 voidaan kiinnittää haluttuun liitäntään ulosmenevälle liikenteelle. Pääsylista voidaan poistaa käytöstä käyttämällä komentoa *no access-list (pääsylistan numero)*. Yksittäinen listan rivi poistetaan puolestaan komennolla *no (pääsylista rivi täydellisenä)*. Kaikki listat voidaan tulostaa näkyviin komennolla *show acces-list* ja yksittäinen lista tulostetaan käyttämällä komentoa *show access-list (pääsylistan numero)*. (Cisco Systems 2002, 162-163;Hakala & Vainio, 2005, 353.)

9.16.4 Laajennettu pääsylista (extended access –list)

Laajennetut pääsylistat tarjoavat laajemmat kontrollointimahdollisuudet kuin standardit pääsylistat. Niiden avulla voidaan kontrolloida niin lähde kuin kohdeosoitteita, porttinumeroita, protokollatietoja tai muita muuttujia. Paketteja voidaan suodattaa niiden lähdeverkon tai kohdeverkon perusteella. Yksittäiseen pääsylistaan voidaan määritellä useita ehtolauseita. Lauseiden on viitattava samaan tunnistenimeen tai pääsylistanumeroon, jotta ne voidaan identifioida. Ehtolauseita voi olla määriteltynä niin paljon kuin reitittimen muistiin saadaan tallennettua, mutta niiden käsittely ja hallinta monimutkaistuu, mitä enemmän ehtoja on käytössä samassa pääsylistassa.

Laajennetuilla pääsylistoilla on mahdollista tehdä liikenteen tarkempaa suodatusta. Liikenne voi olla esimerkiksi sisäänpäin ja ulostulevan liikenteen erottelemista toisistaan tai liikenteen suodatusta protokollien porttinumeroiden perusteella. Kieltomääritys tehdään laajennetuissa pääsylistoissa lisäämällä protokollamäärityksen jälkeen lauseen loppuun protokollan käyttämä porttinumero. Yleisimpiä porttinumeroita, joita käytetään laajennetuissa pääsylistoissa, ovat mm. FTP-protokollan käyttämä portti 20, Telnet-liikenteen käyttämä portti 23 ja TFTP-protokollan käyttämä portti 69. (Cisco Systems 2002, 167-169.)

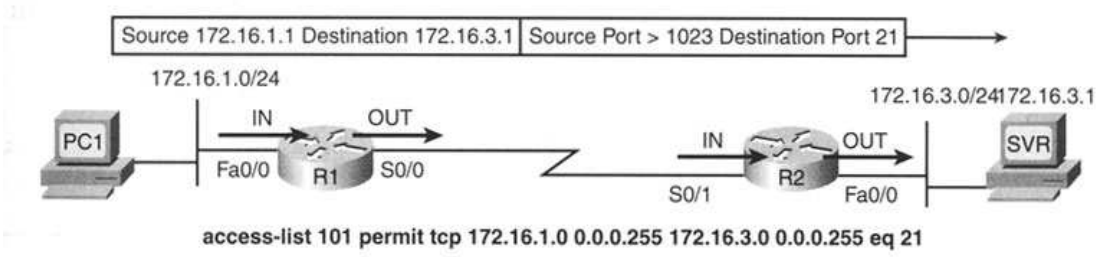
9.16.5 Laajennetun pääsylistan konfigurointi

Laajennetun pääsylistan asetukset määritellään seuraavasti. Laajennettu pääsylista käyttää standardin listan tavoin komentoa *access-list*. Laajennetut pääsylistat identifioidaan numerolla 100–199 tai 200-2699, jonka jälkeen määritellään halutut ehdot numeroidulle listalle seuraavaan syntaksiin perustuen *access-list (pääsylistan numero) deny / permit (+) protokolla (+) lähdeosoite(+) lähdeosoitteen maski (+) kohdeosoite (+) kohdeosoitteen maski (+) operaattori log*. Protokolla komennolla määritellään protokollatyyppi, joka halutaan sallia tai kieltää näitä ovat esimerkiksi TCP ja UDP-protokollat. Operaattori komennolla voidaan määrittää porttinumero, nimi tai portti alue sallituksi tai kielletyksi.

FTP-liikenteen kieltäminen verkosta 192.168.1.0 verkkoon 10.100.10.1 voidaan tehdä laajennetun pääsylistan avulla seuraavilla komennoilla *access-list 101 deny tcp 192.168.1.0 0.0.0.255 10.100.10.1 0.0.0.255 eq 21*. Komennon lopussa oleva määritys eq 21 kertoo kohteena olevan portin, joka on tässä tapauksessa portti 21 eli FTP -liikenteen käyttämä portti. Pääsylistaan tehdään tämän jälkeen salliva ehto, koska muuten lista kieltäisi kaiken liikenteen verkkojen välillä. Ehto määritellään seuraavasti *access-list 101 permit ip 192.168.1.0 0.0.0.255 10.100.10.1 0.0.0.255*. Tämän määrityksen avulla lista sallii kaiken muun liikenteen verkkojen välillä.

Laajennettu lista kiinnitetään lopuksi haluttuun liitäntään ja haluttuun suuntaan standardin pääsylistan tavoin. Syntaksi komennolle on seuraava *ip access-group (pääsylistan numero) in / out*. Aiempi tehty laajennettu pääsylista numerolla 101 voidaan kiinnittää esimerkiksi reitittimen liitäntään Fast Ethernet 0/0 seuraavalla komennolla. *ip access-group 101 out*. Komento annetaan liitännän Fast Ethernet 0/0 konfigurointi tilassa.

Kuvassa 8 on esitetty malli, miten laajennetulla pääsylistalla sallitaan FTP-protokollan liikenne tietokoneelta PC1 palvelimen SVR porttiin 21, reitittimien R1 ja R2 kautta. Pääsylista asennetaan tässä tapauksessa reitittimen R1 sisäänpäin menevään porttiin FA 0/0. (Cisco Systems 2002, 168,170;Hakala & Vainio, 2005, 354.)



Kuva 7: Liikenteen rajoittaminen pääsylistan avulla (Cisco Systems 2007b, 247).

Pääsylistat voivat toimia myös numeron sijasta nimettyinä listoina. Nimettyjen listojen käyttö on perustelua, jos reitittimessä on käytössä useita monimutkaisia listoja. Nimetyille listoille määritellään ensimmäisenä listan tyyppi, jonka jälkeen listalle määritellään siihen kuuluvat permit ja deny komennot. Nimettyjen listojen käyttöä ei kuitenkaan suositella, koska ne eivät ole yhteensopivia kaikkien IOS-komentojen kanssa. Nimetyn listan syntaksi on seuraava *ip access-list (standard / extended) nimi*. Komennon antamisen jälkeen lista kytketään vielä liitäntään samoin kuin numeroita lista, mutta käytetään listan nimeä määrityksessä seuraavasti *ip access-group (pääsylistan nimi) in /out*.

Reitittimen pääsylistan käsittelyssä oleellista on se, että reititin lukee pääsylistan tiedot ylhäältä alaspäin ja lopettaa listan lukemisen välittömästi kun tarkasteltava ehto täyttyy. Tästä syystä listalla olevat ehdot on järjesteltävä tärkeysjärjestyksessä. Peruslistoissa täsmälliset määritykset tulevat listan alkuun. Ensimmäisenä listalle määritellään koneet, sitten aliverkot, normaalit verkot ja lopuksi muut osoitteet. Laajennettujen listojen lisämääritykset käyttävät samaa periaatetta, ensimmäiseksi määritellään protokollat tai portit, sitten porttialueet ja lopuksi määrittämättömät portit tai vastaavasti koko IP-liikenne. Listoissa käytetään käänteistä maskia ns. jokerimaskia (wildcard mask), joka koostuu ns. jokerimaski biteistä (wildcard bits). Biteillä määritellään verkko-osoitteesta ne bitit, jotka

voivat muuttua. Bitin ollessa yksi osoitteen vastaava bitti on joko nolla tai ykkös bitti. Desimaaliluku nolla kertoo sen, että osoitteen on vastattava listassa olevaa osoitetta, vastaavasti luku 255 kertoo sen, että vastaava verkko-osoite voi olla mikä tahansa binääriluku.

Jokerimaskibittien kanssa työskentely on hankalaa ja asioiden helpottamiseksi niiden sijasta voidaan käyttää lyhenteitä. Yhtenä näistä lyhenteistä käytetään any-lyhennettä, jonka avulla voidaan korvata kohde tai lähdeosoitteen kaikki mahdolliset osoitteet. Host-lyhennettä käytetään tilanteessa, jossa halutaan pääsylistan koskevan yksittäistä päätettä, Host-lyhenteellä voidaan korvata IP-osoitteen ja maskin kirjoittaminen.

Järjestysnumeroiden käyttö pääsylistoissa on mahdollista IOS-version 12.2 jälkeen. Vanhemmissa versioissa pääsylistaa ei voitu muokata sen luomisen jälkeen vaan koko lista jouduttiin poistamaan ja tekemään uusi lista asetusten muuttuessa. Järjestysnumeroiduissa pääsylistoissa jokainen pääsylistan komento saa oman järjestysnumeronsa. Tämän järjestysnumeron perusteella pääsylistan käskyt voidaan eritellä toisistaan. Tämä mahdollistaa samalla käskyn poistamisen yksittäin listalta. Pääsylistan käskyt numeroidaan menetelmällä 10,20,30,40, jolloin esimerkiksi 24 numerolla olevan pääsylistan käsky 20 voidaan poistaa listasta yksittäin käyttämällä käskyä *no 20*. Järjestysnumeroa käyttävään listoihin voidaan myös lisätä uusi ehto esimerkiksi käsky *5 deny 192.168.1.0*, joka lisää kyseisen ehdon listalle ylimmäiseksi, koska se käyttää järjestysnumeroa 5. Perus pääsylista komentoa käyttämällä esimerkiksi *access list 24 permit 192.168.2.0* lause lisää pääsylistaan 24 uuden ehdon uudella järjestysnumerolla 50, jolloin pääsylistan uusi ehto tulee pääsylistan käskyistä alimmaiseksi. (Cisco Systems 2002, 159-160;Cisco Systems 2007b, 256-258;Hakala & Vainio 2005, 353-354,348-349.)

9.16.6 Pääsylistojen sijoittelu

Pääsylistojen sijoittelu on tärkeää verkon toiminnan kannalta. Tarpeetonta liikennettä voidaan vähentää sen mukaan minne pääsylista sijoitetaan, jos paketti kielletään liian myöhäisessä vaiheessa se aiheuttaa turhaa verkon kuormitusta. Liikennettä kiellettäessä laajennetulla pääsylistalla lista sijoitetaan mahdollisimman lähellä kielletyn liikenteen lähdettä, tällä tavoin menettelemällä kielletty liikenne ei pääse kulkemaan turhaan verkossa. Standardit pääsylistat eivät määrittele kohdeverkkoa, joten ne sijoitetaan mahdollisimman lähelle kohdeverkkoa.

Pääsylistoja suositellaan käytettäväksi palomuurina toimivissa reitittimissä, jotka sijaitsevat sisäisen verkon ja ulkoisen verkon välissä. Pääsylistat rajoittavat tällöin määrätyn verkko-osan sisään ja ulospäin kulkevaa liikennettä. Tietoturvan takaamiseksi verkossa, pääsylistat tulee

olla aseteltuna verkon reunareitittimissä. Reunareitittimissä pääsylistat asetetaan jokaista reitittimen käyttämää protokollaa kohden erikseen. Pääsylistoilla voidaan eristää reunareitittimien sisäänpäin tuleva liikenne, ulosmenevä liikenne tai molemmat liikenteet haluttaessa. Pääsylistojen avulla verkon vähemmän valvottu osa ja yksityisempi osa voidaan erottaa toisistaan ja taata näin perustason tietoturva verkkossa. (Cisco Systems 2002, 176-177.)

9.16.7 Muita pääsylistamuotoja

Pääsylistoista on myös kehitelty uusia muotoja, jotka tulevat mukana osassa kehittyneimmistä tietoturvaratkaisuista, näitä ovat mm. refleksiiviset pääsylistat, dynaamiset pääsylistat sekä aikaan perustuvat pääsylistat.

Refleksiivisen pääsylistan avulla esimerkiksi ulkopuolelta tuleva hyökkäys sallittuun HTTP-protokollan käyttämään porttiin 80 voidaan estää, siten että pääsylista tarkkailee mistä kohteesta liikenne tulee ja sallitusta kohteesta tuleva liikenne sallitaan. Ainoastaan tapauksessa jossa paketin osoite tiedot ja porttitiedot vastaavat alkuperäistä sallittua lähettäjä konetta. Kaikki muu ulkopuolinen liikenne voidaan estää porttiin 80. Refleksiiviset pääsylistat vaativat lisäasetusten tekemistä reitittimeen sekä nimettyjen laajennettujen listojen käyttöä.

Dynaamiset pääsylistat käyttävät ominaisuutta nimeltä Lock and Key Security, jossa käytetään apuna avaimeen perustuvaa autentikointia. Dynaamisella pääsylistalla konfiguroituun verkkoon pääsemiseksi. Käyttäjältä pyydetään aluksi Telnet-yhteyden ottamista verkon palvelimelle, jossa häneltä vaaditaan käyttäjätunnusta sekä salasanaa. Näiden tietojen perusteella käyttäjä voidaan tunnistaa. Reititin vertaa käyttäjän tietoja käyttäjätietokantaan. Jos käyttäjän tiedot löytyvät tietokannasta, reititin lisää päästylistalle tiedon käyttäjän koneesta. Tämän toiminnon jälkeen liikenne mahdollistuu käyttäjän ja verkon välillä.

Aikaan perustuvat pääsylistat toimivat normaalien pääsylistojen tavoin, mutta sisältävät aikamäärityksen ehtojen voimassa olosta. Pääsylistan määrittelyssä päästylistan ehdoille annetaan aikamääritys, joka määrittää ajan millä aikajaksolla pääsylistan ehto on voimassa. Pääsylistan ehdot voivat toimia eriaikaan esimerkiksi pääsylista voi sisältää ehdot, jotka ovat voimassa yö aikaan ja ehdot jotka ovat voimassa päivisin. (Cisco Systems 2007b, 262-264.)

9.17 Network Address translation (NAT)

NAT (Network Address Translation, NAT)-osoitemuunnospalvelua käytetään hyväksi suurissa yritysverkoissa, jotka sisältävät useita sisäisiä IP4-verkon osoitteita. NAT-protokollan käytöstä tuli tarpeellista, koska internetin vapaiden IPv4-osoitteiden määrä alkoi vähentyä. Suurien organisaatioiden oli käytännössä mahdotonta hankkia vapaita B ja C luokan osoitteita omiin tarpeisiinsa. NAT-palvelua käyttävä yritys käyttää omassa intranetissä sisäisiä rekisteröimättömiä osoitteita. NAT-palvelun avulla yrityksen intranet osoitteet muunnetaan internetin käyttämiin julkisiin osoitteisiin.

Normaalisti NAT-prosessi tehdään yksittäisesti kaikkiin intranet koneisiin, joilta halutaan yhteys ulkoverkkoon. Tässä tapauksessa jokaiseen yrityksen intranet koneeseen määritellään oma julkinen IP-osoite. Toinen tapa tehdä osoitemuutos on käyttää hyödyksi sovelluksien käyttämiä porttinumeroita. Tällä menetelmällä on mahdollista luoda useampia samanaikaisia yhteyksiä yhden IP-osoitteen perusteella. (Hakala & Vainio 2005, 212-213.)

NAT-palvelun toiminta määritellään RFC-dokumentisssa 3022. NAT-palvelussa tapahtuvat osoitemuutokset tehdään yrityksen reitittimessä, joka sijaitsee yritysveron ja ulkoverkon välisellä rajalla. Reititin pitää tietokantaa intranet osoitteista ja niiden vastaavista julkisista osoitteista ja muodostaa näistä osoitepareja, joiden perusteella NAT-prosessi tapahtuu. Tällä menetelmällä yrityksen verkon topologia ja tiedot voidaan salata ulkopuolelta, koska ulospäin menevä osoite ei kuulu mihinkään yrityksen koneelle vaan tulee reitittimestä, joka toimii NAT-prosessissa mukana. NAT-prosessissa käytetään, joko yhtä osoitetta hyväksi tai reititin valitsee osoitteet erityisesti sitä varten luodusta osoiteavaruudesta (address pool). Cisco määrittelee osoitteiden nimet seuraavasti, sisäinen alkuperäinen lähdeosoite määritellään nimellä inside local ja ulospäin näkyvä osoite nimellä outside local. Vastaavasti ulkoverkon osoitteet saavat nimet outside local ja outside global. Local-osoitteet näkyvät sisäverkkoon päin ja global-osoitteet ulkoverkon eli internetin suuntaan.

Osoite käännös voidaan toteuttaa kaksisuuntaisena (bi-directional translation) tai yksinkertaisena osoitekäännöksenä (simple translation entry). Kaksisuuntaisessa käännöksessä osoite muunnetaan sekä ulkopuolelta sisäverkkoon että sisäverkosta ulkoverkkoon. Tällöin kaikki liikenne sisältäpäin kuljetetaan reitittimen jakaman osoite alueen osoitteesta ulos ja ulkopuolinen liikenne kuljetetaan vastaavasti määritetystä osoite alueen osoitteesta sisään. Yksinkertaisessa käännöksessä IP-osoite vaihdetaan toiseen osoitteeseen, joko suoraan tai porttinumeron perusteella. Muutos voidaan tehdä staattisesti (static address translation), jossa osoitepari ovat ennalta määrättyjä tai dynaamisesti, jolloin osoiteparit muodostetaan

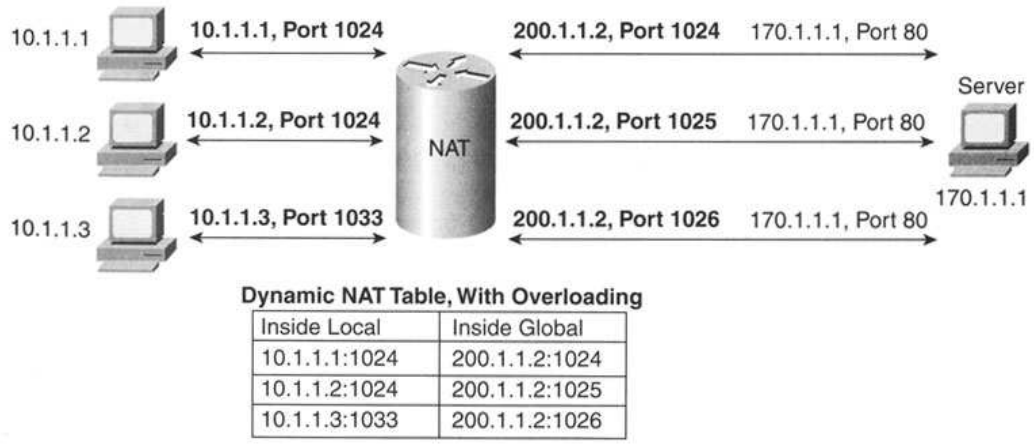
osoitealueiden sisältä valitsemalla osoite automaattisesti. (Internet Engineering Task Force 2001.)

9.18 Port Address translation (PAT)

Porttinumeroihin perustuvaa osoitteiden muutosta kutsutaan nimellä (Port Address translation, PAT), tässä tapauksessa osoitemuutoksiin käytetään sovelluksien käyttämiä porttinumeroita hyväksi. Muutos tehdään siten, että yhtä julkista IP-osoitetta kohden voidaan mahdollistaa useamman intranetin koneen liikennöinti yrityksen verkosta ulkoverkkoon. Tekniikan avulla pyritään käyttämään mahdollisimman vähän ulkopuolisia julkisia osoitteita. PAT-prosessin avulla on mahdollista käyttää kaikki vapaat porttinumerot hyödyksi ennen seuraavaan julkisen IP-osoitteen varaamista. Tekniikasta käytetään yleisesti myös nimeä (Network Address and Port Translation, NAPT). (Hakala & Vainio 2005, 214,248.)

PAT-palvelua käytetään reitittimessä, joka toimii yrityksen yhdyskäytävänä ulkoverkkoon, reititin muuttaa sisäverkon osoitteen ulkoverkon julkiseksi osoitteeksi ja muuttaa sovelluksen käyttämän porttinumeron käyttäen vapaita porttinumeroita hyväkseen. Reititin käyttää muutoksessa ns. socketteja, joiden avulla se muodostaa tietokannan, osoitteiden ja porttinumeroiden perusteella. Tietokanta koostuu alkuperäisestä intranet osoitteesta ja portista sekä muutetusta portista ja reitittimen osoitteesta. Reitittimen oma osoite toimii ainoana näkyvänä osoitteena ulkoverkkoon. Kun reititin vastaanottaa ulkoverkosta tähän osoitteeseen tulevan paketin se tutkii tietokannasta löytyykö vastaavalla porttinumerolla intranetin osoitetta. Jos osoite löytyy tietokannasta reititin korvaa porttinumeron ja osoitteen tietokannasta löytyvillä tiedoilla ja lähettää paketin sisäverkon koneelle. (Hakala & Vainio 2005, 214.)

Kuvassa 10 esitellään tilanne, jossa reitittimeen on konfiguroitu PAT-ominaisuus, jonka kautta liikennettä ohjataan työasemilta palvelimelle. PAT-ominaisuus tekee IP-liikenteen ohjauksen porttien kautta. Liikenteen ohjaus voidaan tehdä samojen porttien tai eri porttien kautta kuten kuvasta voidaan huomata. Reititin pitää yllä dynaamista PAT-taulua, johon läpikulkeva liikenne tallentuu.



Dynamic NAT Table, With Overloading

Inside Local	Inside Global
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

Kuva 8: Porttikohtainen osoitteenmuutos (Cisco Systems 2007b, 559).

10 IPv6 (Internet protocol version 6)

IPV4-protokolla on lähiverkkojen yleisin protokolla, jonka kehitystyö jatkuu edelleen. Suurin ongelma IPV4-protokollassa on sen 32-bittinen verkko-osoitteille varattu osoiteavaruus. IPV4-verkon vapaiden osoitteiden on ennustettu loppuvan seuraavan kahden vuoden aikana, viimeistään vuonna 2010. NAT-osoitemuunnoksien avulla tilannetta pystyttiin korjaamaan väliaikaisesti, mutta IPV6-verkkoihin siirtyminen tulee olemaan välttämätöntä seuraavien vuosien aikana. Vuonna 2008 IPv6-osoitteisiin siirtyminen tulee olemaan vilkasta, esimerkiksi USA:ssa kaikki hallintolaitoksien ydinverkot siirtyvät tukemaan IPv6-osoitteita vuonna 2008. (Kaario 2002, 108; Cisco Systems 2007b, 580.)

IPv6-standardi julkaistiin vuonna 1998, tekniikan suurimpana etuna voidaan pitää sen 128-bittistä osoiteavaruutta, joka mahdollistaa kaksi potenssiin 128 kappaletta osoitteita. Tämä osoitemäärä tulee riittämään tekniikan käyttöön pitkäksi ajaksi. IPv6-protokolla perustuu 64-bittiseen arkkitehtuuriin, jolloin kehyksien otsikot ovat aina 64-bitin monikertoja. Tästä johtuen niiden käsittely tapahtuu optimoidusti 64-bittisissä ympäristöissä. IPv6-protokollan toiminta määritellään RFC-dokumentissa 2460. IPv6-protokolla sisältää kahdeksan otsikkokenttää vanhan IPv4 12-kentän sijasta, mutta IPv6-protokollassa otsikoita voidaan ketjuttaa peräkkäin tarpeen vaatiessa. IPv6 ei sisällä tarkistussummia IP-kerroksessa, mutta ylempien kerroksien protokollissa tarkistus summan käyttö on pakollista. IPv6-protokolla ei myöskään salli pakettien pilkkomista verkosta vaan kaikki paketteihin kohdistuvat muutokset täytyy tehdä jo lähettäjän toimesta. Tällä vähennetään reitittimien kuormitusta ja mahdollistetaan nopeat kytkentä mekanismit kuten MPLS (Multiprotocol Label Switching). IPV6-verkoissa yhden linkin pitää pystyä välittämään vähintään 1280-tavun mittaisia IP-paketteja IPv4 68 tavun sijasta. (Internet Engineering Task Force 1998b.)

Osoitteiden lisäämisen ohella IPv6-protokolla mahdollistaa paremmat tietoturvaominaisuudet sekä palvelun laatuun liittyviä parannuksia. IPV6-protokolla on otettu huomioon jo suunnitteluvaiheessa lisäämällä tietoturvaan liittyviä otsikoita. Palvelun laatua varten IPv6 sisältää vuontunnistukseen liittyvän kentän, jolla IP-osoitteet voidaan tunnistaa loogisen yhteyden perusteella. IPv6 osoitteen luokkakenttä tarjoaa vastaavasti mahdollisuuden jakaa paketit eri luokkiin.

Cisco Systemin teoksessa CCNA/ICND2 luetellaan suurimpia IPv6-protokollan tuomia uudistuksia:

1 Osoitteiden luovutukseen liittyviä ominaisuuksia, jolla tarkoitetaan kannettavien mobiili laitteiden sekä kannettavien tietokoneiden liikuteltavuutta saman IP-osoitteen perusteella.

2 Verkko-osoitteiden kasausta, joka tarkoittaa internetin osoitteiden yhdistämistä perustuen IPv6-protokollaan suureen osoiteavaruuteen.

3 NAT/PAT-protokollien tarpeettomuutta, IPv6-protokollassa ei tarvitse tehdä osoitteille kohdistuvaa NAT tai PAT muutosta.

4 IPsec-tietoturva ominaisuudet ovat pakollisia IPV6-verkkojen päätelaitteissa, näillä mahdollistetaan luotettavasti VPN-tunneloinnin teko.

5 IPv6-osoitteiden otsikoinnissa tapahtuneet parannukset vähentävät reitittimien kuormitusta tarkistussumman tarkistamisen jäädessä pois ja lisäksi ne mahdollistavat vuon ohjaukseen liittyvät tunnistamismenetelmät.

6 Uudet lisätyökalut, joilla mahdollistetaan uusia lisäominaisuuksia laitteiden hallinnassa.

(Cisco Systems 2007b, 580-581.)

10.1 IPv6-protokollan osoitteiden rakenne

IPv6-osoitteen rakenne koostuu kahdeksasta 16-bittisestä heksadesimaaliluvusta esimerkiksi osoite *2340:BA12:4563:3456:FFCB:F453:2334:0001* edustaa normaalia IPv6-osoitetta. IPv6-osoitteita voidaan lyhentää niiden muistamisen helpottamiseksi seuraavalla tavalla, määrittämätön osoite sarja 0:0:0:0 voidaan lyhentää käyttämällä kahta peräkkäistä kaksoispistettä esimerkiksi seuraavasti, osoite *1111:2222:3333:0000:0000:4444:5555:FFFF* voidaan lyhentää muotoon *1111:2222:3333::4444:5555:FFFF* kahdella kaksoispisteellä.

Lyhennystapaa voidaan käyttää kuitenkin vain yhden kerran IPv6-osoitetta kohden. (Kaario 2002, 111-112.)

10.2 IPv6-protokollan lähetys ja osoiteluokat

Cisco Systemsin teoksessa CCNA/ICND2 sekä K, Kaarion teoksessa TCP/IP-verkot kuvataan IPv6-protokollan käyttämiä osoite ja lähetys luokkia. IPv6-osoitteet jaetaan kolmeen eri lähetysluokkaan, Unicast, Multicast sekä Anycast-osoitteisiin. Unicast-osoitteet sopivat liitäntöihin, johon kytketään ainoastaan yksi laite datan lähettämistä ja vastaanottoa varten. Multicast-osoitteet sijoitetaan laitteisiin, jotka edustavat ryhmää laitteita, joille dataa lähetetään yhtäaikaisesti. Multicast-osoitteet sisältävät myös kattavan tuen loppukäyttäjien ohjelmistoille. Anycast-osoitteet tukevat parhaiten palvelimia, joiden kaikki palvelut käyttävät samoja Unicast-osoitteita. Asiakaskoneiden lähettämät paketit voidaan tällöin ohjata tasaisesti eri palvelimien välillä, jolla voidaan taasta kuormitusta.

IPv6-Unicast-osoitteet jaetaan kolmeen eri osoiteluokkaan globaaleiksi osoitteiksi (global), aluekohtaisiksi osoitteiksi (site local) tai nykyisin kutsutuksi (unique local) sekä linkkikohtaisiksi osoitteiksi (link local). Linkkikohtaisia osoitteita on mahdollista käyttää vain yhdellä linkillä, eivätkä muut reitittimet voi ohjata osoitteita kuin kyseiselle linkille. Linkkikohtaisilla osoitteilla voidaan hoitaa esimerkiksi laitteen automaattinen konfigurointi. Linkkikohtainen osoite on rakenteeltaan seuraavanlainen:
(1111111010 + 54 nollabittiä) + (vastaan ottajan ID 64 bittiä)

Aluekohtaisia osoitteita käytetään tietyn rajatun alueen sisällä, joiden laitteet ovat yhteydessä keskenään aina yhden toimiston muutamasta koneesta pienen yrityksen koko sisäverkkoon. Aluekohtainen osoite on rakenteeltaan seuraavanlainen:
(11111101 + 40 nollabittiä + 16 bittinen aluetunnus) + (vastaanottajan ID 64 bittiä)

Globaalit osoitteet ovat yleisimpiä IPv6-verkon osoitteita. Ne muodostuvat kolmesta osasta, joita ovat yleinen osa, alueellinen osa sekä vastaanottajan tunnistava osa. Yleistä osaa osoitteesta käyttävät palveluntarjoajat, jotka tarjoavat palveluja alemmille tahoille. Osoite muodostuu 48-bitistä, joilla määritellään miten korkea taho jakaa kyseistä osoitetta. Osoitteen aluekohtaista osaa käyttää paikallinen palveluntarjoaja esimerkiksi Sonera tai Elisa suomessa. Vastaanottajan tunniste on osoitteen viimeinen kolmas osa, joka muodostetaan 64-bitistä.

Multicast-osoitteen rakenne poikkeaa hieman Unicast-osoitteiden rakenteesta. Multicast-osoite alkaa aina kahdeksalla 1 bitillä, jota seuraa neljä lippubittiä. Lippubittien tehtävänä on kertoa onko osoite pysyvä vai väliaikainen osoite. Tarkennin osan neljän bitin tehtävänä on

kertoa osoitteen luonteesta ja tarkoituksesta lisätietoja. Multicast-osoitteen rakenne on seuraavanlainen:
(11111111 + 4 lippubittiä +4 bitin tarkennin osa) + (64 bitin ryhmätunniste)

Anycast-osoitteet käyttävät samaa rakennetta kuin Unicast-osoitteet, poikkeuksena Anycast-osoite ryhmän jäsenen täytyy tietää oma osoitteensa ja toimia ryhmänsä mukaisesti. Anycast-osoitteita ei käytetä yleensä palvelimien väliseen kommunikointiin vaan niitä käyttävät palveluita käyttävät asiakkaat. Anycast-ryhmässä toimivan palvelin voi ohjata asiakkaalta tulevan kyselyn lähimmälle palvelimelle, jolloin asiakas voi hoitaa palvelun käytön yhden IP-osoitteen avulla. Anycast-lähetykset sopivat parhaiten juuri kannettaville päätelaitteille. Anycast-lähetyksien suurin ongelma on se, että niitä ei voida sijoittaa IPv6-pakettien lähdeosoitteiksi, jolloin käyttö TCP-protokollan kanssa on hankalaa, mutta UDP-protokollan kanssa toimivia sovelluksia on sille helpompi kehittää. (Cisco Systems 2007b, 600-601;Kaario 2002, 112-114,122-123.)

10.3 IPv6 ja IPv4-verkkojen yhdistäminen

IPv6-verkkojen yleistymisen myötä IPv6-verkkojen määrä alkaa olla jo maailmalla suuri varsinkin Aasian mantereella. Tästä johtuen IPv4 ja IPv6-verkkojen liikenne pitää saada toimimaan keskenään, tähän on olemassa monia ratkaisuja, joista IPv4/IPv6 dual stack on yksi. Termi tarkoittaa päätelaitetta, joka ohjaa yhtäaikaisesti IPv4 ja IPv6-liikennettä. Päätelaitteella täytyy tässä tapauksessa olla konfiguroituna IPv4-reititysprotokolla sekä IPv4-verkon reititysprotokolla yhtäaikaisesti. Tätä menetelmää käyttäen yrityksen verkko saadaan muutettua IPv6-ympäristöä tukevaksi muutamilla ohjelmisto päivityksillä tai laitteisto hankinnoilla, jolloin aikaa jää myös henkilökunnan koulutukselle.

IPv6-tunnelointi on toinen tapa tehdä IPv4 ja IPv6-verkon yhdistämistä. IPv6-tunnelointi tarkoittaa IPv6-pakettien reititystä IPv4-verkon läpi. Tunneloinnissa IPv6-paketti paketoidaan IPv4-paketin sisälle, josta se saavuttaessa kohdeverkon voidaan purkaa kohdeverkon reitittimessä, joka tukee IPv6-protokollaa. Tunnelointi tapoja on useita manuaaliset tunnelit konfiguroidaan manuaalisesti laitteisiin, joista IPv6-tunnelointia halutaan tehdä. Laitteisiin tehdään tällöin virtuaaliset liitännät joiden kautta tunnelointi tapahtuu.

Dynaamisessa 6to4 tunneloinnissa tunneloinnin tekeminen tapahtuu automaattisesti kohdeosoitteen perusteella tunnelin päätepisteen reitittimellä, jolloin IPv6-verkon kohdeosoite saadaan purettua IPv4-verkko-osoitteesta. ISATAP-tunneloinnin tekniikka perustuu dynaamiseen 6to4 tunnelointiin, mutta tunnelointi tapahtuu yritysverkon sisällä. Tämä voidaan varmistaa siten, että tunnelointimekanismi ei kulje IPv4 protokollaan perustuvan NAT-osoitemuutoksen läpi. Teredo-tunnelointi perustuu dual stack-tekniikkaan,

jossa dual stack päätelaite itse pystyy sekä luomaan että purkamaan IPv6 paketin IPv4 paketin sisältä. Teredo-tunnelointia käytetään yleisesti juuri päätelaitteiden välisessä kommunikoinnissa. (Cisco Systems 2007b, 609-612.)

11 Verkkoharjoitusten sisältö

11.1 1. Harjoitus / Kytkimen IOS–perusteet

Ensimmäisen viikon harjoituksen tavoitteena on antaa opiskelijalle peruskäsitys siitä, miten IOS CLI -käyttöjärjestelmä toimii, mitkä ovat käyttöliittymän perustilat ja miten eri tilojen välillä liikutaan. Harjoituksessa käydään läpi myös IOS-käyttöliittymän aputoimintoja ja tutkitaan, mitä tietoja kytkimestä voidaan saada eri käskyjen avulla. Tietoturvallisuuteen liittyvät seikat sekä salasanojen asettelu virtuaalilinjoille ovat viimeisenä osana harjoitusta.

Harjoitus jakautuu kolmeen osa-alueeseen, joista ensimmäinen käsittelee yhteyden muodostamista kytkimeen. Toinen vaihe käsittelee kytkimeen liittyvien tietojen tulostamista ja kolmas vaihe käsittelee virtuaalilinjakohtaisten salasanojen asettamista sekä tietojen tallentamista.

11.1.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, jossa on mukana kuusi kytkintä sekä terminaalipalvelin. Kytkimet toimivat harjoituksessa työryhmäkytkiminä, joihin muodostetaan yhteys Telnet-ohjelmistolla, terminaalipalvelimen konsoliporttia käyttäen. Harjoituksessa käytetään yhtä tietokonetta ryhmää kohden, tietokoneen avulla konfiguroidaan yhtä työryhmäkytkintä. Maksimissaan kuusi ryhmää voi tehdä harjoitusta yhtäaikaisesti.

11.1.2 Osio 1 Yhteyden muodostaminen ja konfiguraatiotilat

Harjoituksen ensimmäisessä vaiheessa opiskelijat muodostavat yhteyden kytkimeen terminaalipalvelimen kautta. Yhteys muodostetaan käskyllä *telnet 10.8.4.2 20??*, jossa laitteen porttinumero määräytyy ryhmän numeron mukaan. Yhteyden saamisen jälkeen harjoituksessa käsittellään ”?”-merkin käyttöä, jota käytetään IOS-käyttöjärjestelmässä vaihtoehtoisten käskyjen listaukseen komentotilassa. Kysymysmerkin oikeanlainen käyttö on tärkeää, koska sen avulla on mahdollista löytää käsky, joka toimii halutussa konfiguraatiotilassa. Kysymysmerkkiä voidaan käyttää käskyn alussa, keskellä tai käskyjen välissä. ”Tab”-näppäimen oikeanlainen käyttö helpottaa paljon turhaa kirjoitustyötä, sen avulla käsky voidaan tulostaa kokonaisena, jo muutaman kirjaimen kirjoittamisen jälkeen. Tätä harjoitellaan myös ensimmäisessä osiossa muutaman muun helpottavan

näppäinkomennon kanssa esim. ”return”, ja ”space bar” -näppäimet jotka vaikuttavat siihen, miten IOS listaa tietoa ruudulle.

Konfiguraatiotilojen välinen liikkuminen on yhtenä osana ensimmäistä osiota, opiskelijan on tunnistettava IOS-käyttöliittymässä olevat konfiguraatiotilat toisistaan sekä osattava liikkua tilojen välillä. Konfiguraatiotilat erottaa toisistaan tunnuksesta, joka näytetään rivillä ennen käskyn antamista. Käyttäjätilan tunnuksena käytetään ”>” merkkiä, pääkäyttäjätilassa tunnuksena on ”#” merkki ja globaalissa konfiguraatiotilassa käytetään ”<config>#” tunnusta. Tilojen välillä tapahtuva liikkuminen IOS-järjestelmässä eteenpäin tapahtuu käskyillä *enable* sekä *configure terminal* ja taaksepäin käskyillä *disable*, *end* sekä *exit*.

11.1.3 Osio 2 Kytkimen tietojen tulostaminen

Harjoituksen toinen osio käsittelee kytkimen tietojen tulostamista ja yksittäisten tietojen hakua tulostuksesta. Pääkäyttäjätilassa tehdyt käskyt *show version* sekä *show running-configuration* ovat peruskäskyjä, joita käytetään tulostamaan tietoa, joka liittyy kytkimen järjestelmän konfiguraatiotiedostojen sekä IOS-versiokohtaisen tiedon hakemiseen. Opiskelijoiden on tässä osiossa haettava edellä mainittuja käskyjä käyttäen IOS-version ja kytkimen perustietoja esim. versio numeroon, käyttöjärjestelmän päälläoloaikaan tai järjestelmän käyttämään image-tiedostoon liittyviä tietoja sekä tietoja kytkimen käyttämän nvram muistin määrästä. Seuraavissa tehtävässä määritellään terminaalin käskyhistoriaksi 50 riviä ja tutkitaan kytkimen historia lokia. Terminaalin historiaa voidaan säätää käskyllä *terminal history size* ja sen sisältöä tutkia käskyllä *show history*. Terminaaliin määritetyt asetukset voidaan tarkistaa käskyllä *show terminal*.

11.1.4 Osio 3 Salasanojen asettaminen ja konfiguraatiotietojen tallennus

Harjoituksen kolmas osio käsittelee virtuaaliliitäntään liittyviä asetuksia ja konfiguraatioiden tallennusta. Osiossa määritellään virtuaaliliitäntään kirjautumistunnukset käyttäjätunnusta ja salasanaa käyttäen. Kirjautuminen käyttäjätunnuksen avulla määritellään virtuaalilinjakohtaisessa konfiguraatiotilassa käskyllä *login local* ja käyttäjätunnus ja salasana käskyillä *username* ja *password*. Virtuaalilinjakohtaiseen konfiguraatiotilaan päästään komennolla *line vty* sekä syöttämällä haluttu linjaväli, joka halutaan ottaa mukaan konfigurointiin. Virtuaalilinjan alla tehdään lisäksi muita määrityksiä määrittämällä linjan varausaika äärettömään käskyllä *exec-timeout 0 0* sekä viestien synkronointia koskeva asetus käskyllä *logging syncronous*. Harjoituksen viimeisenä tehtävänä kytkimeen tehdyt asetukset kopioidaan kytkimen nvram muistiin startup-configuration tiedostoon. Kopiointi suoritetaan käskyllä *copy running-config startup-config*.

11.2 2. Harjoitus / IOS-salasanat ja konfiguraatiotiedostojen käsittely kytkimessä

Toisen viikon harjoituksen tarkoituksena on konfiguroida kytkin käyttämällä automaattista Setup-toimintoa. Opiskelijoiden tarkoitus on harjoituksen avulla oppia suojaamaan virtuaaliset linjat salasanojen avulla, määrittämään kuvauksia käytetyille liitännöille sekä luomaan banneri muotoisia ilmoituksia kytkimeen kirjauduttaessa. Harjoitus käsittelee myös liitäntäkohtaisia asetuksia mm. porttikohtaisen IP-osoitteen määrittämistä sekä TFTP-palvelimen käyttöä.

Harjoitus jakautuu viiteen osa-alueeseen, joista ensimmäinen osio käsittelee automaattisen Setup-toiminnon vaiheita sekä salasanojen asettamista. Toisessa osiossa luodaan kytkimeen liitäntäkohtaisia kuvauksia sekä kirjautumis banneri. Kolmannessa vaiheessa tutkitaan kytkimen Image-tiedoston ominaisuuksia. Neljännessä vaiheessa määritetään kytkimeen porttiin IP-osoite ja aliverkkomaski. Viimeisessä vaiheessa kytkimeen tehty konfiguraatiotiedosto tallennetaan ulkopuoliselle TFTP-palvelimelle.

11.2.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, joka sisältää kuusi työryhmäkytkintä, terminaali palvelimen, Corekytkimen ja TFTP-palvelimen. Työryhmäkytkimiin muodostetaan yhteys käyttäen terminaalipalvelimen konsoliporttia. Työryhmäkytkimet on kytketty runko porttien kautta Corekytkimeen. Corekytkimen kautta muodostetaan yhteys hallinta VLAN 8 verkkoon ja TFTP-palvelimelle. Opiskelijat käyttävät yhtä tietokonetta, jonka avulla opiskelijaryhmä konfiguroi yhtä työryhmä-kytkimistä, harjoituksen lopussa opiskelijat tallentavat kytkimen konfiguraation TFTP-palvelimelle. Maksimissaan kuusi ryhmää voi tehdä harjoitusta yhtäaikaisesti.

11.2.2 Osio 1 Setup-toiminnon käyttäminen kytkimessä

Harjoituksen alussa opiskelijat muodostavat yhteyden kytkimeen terminaalipalvelimen avulla. Kytkimen peruskonfiguraatio tehdään harjoituksessa käyttäen automaattista Setup-toimintoa, jonka avulla kytkimelle syötetään perusasetukset kuten IP-osoite, oletussalasanat virtuaalilinjoille sekä kytkimen nimi. Kytkimen automaattinen konfigurointi käynnistetään komennolla *setup* pääkäyttäjätilass*a*. Konfiguraatio tallennetaan asetusten teon jälkeen kytkimen NVRAM-muistiin. Tallennetut asetukset tarkastetaan tämän jälkeen kytkimen ajonaikaisesta konfiguraatiosta. Osion loppuosa käsittelee salasanojen merkitystä ja niiden eroavaisuuksia.

11.2.3 Osio 2 Bannereiden teko ja liitäntäkohtaiset kuvaukset

Harjoituksen toisessa osiossa opiskelijat luovat kytkimelle bannerin, joka näytetään kirjautumisen yhteydessä. Banneri luodaan käskyllä *banner motd* globaalissa konfiguraatiotilassa, jonka jälkeen syötetään banneriin kuuluva lopetusmerkki. Tämän jälkeen painetaan ”enter”-näppäintä ja kirjoitetaan banneriin kuuluva tekstiosuus. Bannerin tekstiosuus saadaan lopetettua käyttämällä erottelumerkkiä. Bannerin teon lisäksi kytkimelle määritellään liitäntäkohtaiset kuvaukset. Kuvaus voidaan määrittää liitäntään *description* käskyllä liitännän alaisessa konfiguraatiotilassa, jonka jälkeen syötetään kuvaukseen käytettävä tekstiosuus. Osion viimeinen vaihe käsittelee salasanatietojen ja kuvausten hakemista kytkimen konfiguraatiotiedoista. Step 5 kohdassa halutaan tietää kytkimen MAC-osoite taulussa olevat MAC-osoitteet, MAC-osoitteet voidaan selvittää pääkäyttäjätilan käskyllä *show mac-address table*.

11.2.4 Osio 3 Image-tiedoston tutkiminen

Harjoituksen kolmas osio on tarkoitettu IOS-image-tiedostoon liittyvän tulostuksen tutkimiseen. Käskyllä *show version* voidaan tulostaa kytkimen IOS-versioon liittyviä tietoja. Oppilaiden on tarkoitus löytää tulostuksesta kytkimen käyttämä IOS-versio sekä IOS–image-tiedostoa koskevia tietoja mm. IOS järjestelmän tukemat ominaisuudet, tiedoston tiedostopääte ja versio numero.

11.2.5 Osio 4 Kytkimen liitännän konfigurointi ja hallinta VLAN asetukset

Harjoituksen neljännessä osiossa konfiguroidaan kytkimen liitäntää Fast Ethernet 0/1 ja määritellään kytkimelle hallinta virtuaalilähiverkko. Opiskelijat määrittävät liitännän FA 0/1 aktiiviseksi ja tutkivat sen jälkeen kytkimen liitäntäkohtaisia asetuksia. Tämän jälkeen opiskelijat poistavat kytkimen hallinnan ja IP-osoitteen VLAN verkosta yksi ja siirtävät hallinnan VLAN verkkoon kahdeksan. Kytkimessä liitäntäkohtaiseen konfiguraatiotilaan päästään kirjoittamalla globaalissa konfiguraatiotilassa komento *interface fastethernet* sekä halutun liitännän tunnus. Kytkimen VLAN–konfiguraatiotilaan päästään puolestaan kirjoittamalla komento *interface vlan* ja halutun VLAN–verkon numero. Kytkimessä portti määritellään aktiiviseksi käskyllä *no shutdown*. Käsky annetaan portin konfiguraatiotilassa. Kytkimen IP-osoite määritellään käskyllä *ip address* ja poistetaan käskyllä *no ip address*. Kytkimen hallinta VLAN määritellään käskyllä *management*, käsky tehdään VLANin konfigurointitilassa, jolloin kyseinen VLAN muuttuu kytkimen virtuaaliseksi hallinta lähiverkoksi.

11.2.6 Osio 5 TFTP–palvelimen toiminta

Harjoituksen viimeinen osio käsittelee kytkimen konfiguraation tallentamista ulkoiselle TFTP-palvelimelle. TFTP–palvelinta käytetään harjoituksissa konfiguraatioiden tallennuspaikkana. TFTP–palvelimen avulla kytkimiin ja reitittimiin tehdyt konfiguraatiot voidaan tallentaa ”.bin” muotoiseen binääritiedostoon. TFTP–palvelimelta voidaan myös hakea konfiguraatio, joka voi toimia esimerkiksi harjoituksessa aloituskonfiguraationa. Yhteyden muodostamiseksi TFTP–palvelimelle vaaditaan, että TFTP–palvelin on kytketty samaan verkkoon laitteen kanssa. TFTP–palvelimelle konfiguraatiotiedoston kopiointi tapahtuu pääkäyttäjätilassa käskyllä copy running-config tftp, jonka jälkeen annetaan TFTP–palvelimen IP-osoite sekä haluttu nimi tiedostolle. Tämän jälkeen kopioinnin suoritus varmennetaan. Kopiointi prosessin jälkeen IOS kertoo kopioinnin onnistumisesta ilmoituksella.

11.3 3. Harjoitus / IOS–perusteet ja CDP–protokollan toiminta reitittimessä

Harjoitus kolme käsittelee reitittimen perusasetuksia sekä CDP-protokollan toimintaa ja siihen pohjautuvaa tiedonhakua lähiverkossa. Harjoituksen avulla oppilaat muodostavat käsityksen siitä miten reititin toimii ja miten se eroaa kytkimen toiminnasta. CDP–protokollan avulla oppilaat hahmottavat sen miten harjoituksen topologiaa on mahdollista tutkia käyttöjärjestelmän avulla ja miten laitteiden välillä voidaan liikkua yhteyttä katkaisematta.

Harjoitus jakautuu viiteen osioon, joista ensimmäisessä muodostetaan yhteys reitittimelle ja tutkitaan reitittimen konfigurointitiloja ja asetuksia. Toisessa osiossa tutkitaan reitittimen liitäntöjä ja määritellään IP-osoitekohtaisia asetuksia. Kolmannessa osiossa tutustutaan CDP-protokollan toimintaan sekä tutkitaan mitä tietoa sen avulla on reitittimestä mahdollista saada. Neljännessä osiossa harjoitellaan Telnet-yhteyksien ottamista kytkimen ja reitittimen välillä. Viimeinen osio keskittyy konfiguraatiotiedostojen käsittelyyn reitittimessä.

11.3.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, jossa on mukana 6 työryhmäreititintä, kuusi työryhmäkytkintä, Core-kytkin, TFTP-palvelin ja Terminaalipalvelin. Kytkimet, reitittimet ja TFTP-palvelin on kytketty Core-kytkimeen harjoituksen alussa. Harjoituksen työryhmäkytkimiin on asetettu valmis kokoonpano Telnet-yhteyden testaamista varten. Harjoituksen neljännessä osuudessa yhteyttä reitittimistä kytkimiin testataan Core-kytkimen kautta. Opiskelijat muodostavat yhteyden reitittimiin Terminaalipalvelimen kautta. Harjoituksen lopussa reitittimiin haetaan uusi konfiguraatio TFTP-palvelimelta. Harjoitus toteutetaan siten, että jokaiselle opiskelijaryhmälle on varattu yksi työryhmäkytkin sekä yksi reititin, maksimissaan kuusi ryhmää voi tehdä harjoitusta yhtäaikaisesti.

11.3.2 Osio 1 Reitittimen konfigurointilat ja salasana asetukset

Harjoituksen ensimmäisessä vaiheessa opiskelijat muodostavat yhteyden reitittimeen Terminaali-palvelimen kautta. Yhteyden muodostamisen jälkeen opiskelijat tutkivat reitittimen ajonaikaista konfiguraatiota sekä reitittimen eri tiloja ja vertaavat niiden toimintaa kytkimen vastaaviin tiloihin. Opiskelijat luovat tämän jälkeen reitittimeen käyttäjätunnuksen sekä salasanan, jotka suojaavat reititintä virtuaalilinjojen kautta tulevilta yhteys yrityksiltä. Tämän jälkeen opiskelijat testaava salasanan ja käyttäjätunnuksen toimivuutta ottamalla uuden yhteyden laitteeseen virtuaalilinjan kautta ja syöttävät määritellyn käyttäjänimen ”cisco” sekä salasanan ”cisco”.

11.3.3 Osio 2 Reitittimen liitännät ja IP-kohtaiset asetukset

Harjoituksen toisessa osiossa käsitellään reitittimen liitäntäkohtaisia asetuksia. Opiskelijat määrittävät reitittimen porttiin Fast Ethernet 0/0 IP-osoitteen ja muuttavat portin tilan aktiiviseksi sekä tarkastavat tehdyt konfiguraatiot listaamalla reitittimen asetukset. Osion viimeinen vaihe käsittelee reitittimen IOS-versiokohtaisia tietoja ja niiden hakemista. Opiskelijat hakevat kysymyksiä vastaavia tietoja IOS-käyttöjärjestelmästä. Kysymykset koskevat mm. järjestelmän muistien määriä, konfiguraatiorekisterin arvoa ja versionumeroa.

11.3.4 Osio 3 CDP-protokolla

Harjoituksen kolmannessa osiossa käsitellään CDP-protokollaa ja sen toimintaa. Opiskelijoiden on tarkoitus tutkia CDP-protokollan avulla mitä naapurilaitteita on kytkettyinä ryhmän reitittimeen. Opiskelijat käyttävät komentoa *show cdp neigbourhood* ja hakevat tulostuksesta vastauksia kysymyksiin, jotka liittyvät esim. laite tunnuksen, paikallisen liitännän, paikallisen portin sekä laitteen ominaisuuksien hakuun. Vastaukset löytyvät edellä mainitun komennon avulla. Opiskelijoiden on tarkoitus löytää käskyn avulla saadusta tulostuksesta oikeat tiedot. Viimeisenä vaiheena osiossa on CDP–protokollan käyttämän liikenteen tutkiminen laitteiden välillä. Liikennettä tutkitaan käyttämällä komentoa *show cdp traffic* ja selvittämällä tulostuksesta kulkeeko liikennettä laitteiden välillä vai ei.

11.3.5 Osio 4 Telnet-yhteydet laitteiden välillä

Harjoituksen neljännessä osuudessa testaan Telnet-yhteyden toimivuutta. Opiskelijoiden tehtävänä on ottaa yhteys ryhmäkohtaisesti omasta työryhmäreitittimestä työryhmäkytkimeen. Telnet-yhteys muodostetaan komennolla Telnet pääkäyttäjätilassa, johon lisätään vastaanottavan laitteen IP-osoite. Yhteyden muodostuminen onnistuu, jos IOS-

käyttöliittymän komentokehotteen otsikkorivin tunnus muuttuu. Opiskelijoiden on tämän jälkeen testattava yhteyksien hallintaa luomalla uusia yhteyksiä sekä katkaisemalla vanhoja yhteyksiä. Yhteyksiä voidaan hallita komennolla *show sessions*, jolla saadaan numeroitu lista tämänhetkisistä Telnet-yhteyksistä muihin laitteisiin. Yhteyksiä voidaan katkaista *disconnect* komennolla ja palauttaa *resume* komennolla. Käskyn perään määritellään yhteyttä koskeva numero. Näppäinkomennolla cntr-shift-6 yhtäaikaisesti + x näppäintä tämän jälkeen painettuna saa aikaan sen, että yhteys yhteyden muodostavaan laitteeseen palautetaan ilman yhteyden katkaisemista.

11.3.6 Osio 5 Reitittimen konfiguraatiotiedostojen käsittely

Harjoituksen viimeinen osio käsittelee reitittimen konfiguraatiotiedostojen käsittelyä. Harjoituksen tässä osiossa opiskelijoiden tarkoituksena on hakea konfiguraatio TFTP-palvelimelta ja korvata tällä konfiguraatiolla reitittimen aloitus konfiguraatio. TFTP-palvelimeen on harjoituksen alkaessa tallennettu reitittimen oletusasetusta vastaava konfiguraatio. Opiskelijat hakevat tämän konfiguraation palvelimelta omalle reitittimelleen käskyllä *copy tftp startup-configuration*. Tämän jälkeen syötetään TFTP-palvelimen IP-osoite sekä konfiguraatio tiedoston nimi, joka vastaa mallia icnd_router1.bin–icnd_router6.bin opiskelijaryhmästä riippuen.

11.4 4. Harjoitus / Dynaaminen reititys ja DHCP–palvelun toiminta reitittimessä

Harjoitus neljä käsittelee dynaamisen reitityksen tekemistä ja DHCP–palvelun toimintaa. Harjoituksen tarkoituksena on käydä läpi, miten dynaamiset reitit toimivat ja miten niitä luodaan laitteiden välille. Harjoitus käsittelee myös DHCP–palvelimen toimintaa ja miten DHCP-palvelin konfiguroidaan jakamaan IP-osoitteita muille laitteille.

Harjoitus jakautuu neljään osa-alueeseen, ensimmäisessä käydään läpi yhteyden muodostamista reitittimeen ja konfiguroidaan reititin automaattisen Setup-toiminnon avulla. Harjoituksen toinen osa käsittelee reititystauluun liittyviä asetuksia sekä RIPv2-protokollan konfigurointia. Harjoituksen kolmas osio käsittelee DHCP-palvelimen asentamista ja viimeisessä osiossa tallennetaan reitittimen konfiguraatio TFTP-palvelimelle.

11.4.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, joka sisältää kuusi reititintä, TFTP-palvelimen, Terminaali palvelimen, sekä Core-kytkimen. Harjoitus jakautuu kahteen osaan, ensimmäisessä osassa reitittimet kytketään Core-kytkimeen portin Fast Ethernet 0/0 kautta. Toisessa osassa

topologia vaihtuu siten, että reitittimet kytketään portin Fast Ethernet 0/1 kautta DHCP-palvelun testaamiseksi. Kuusi opiskelijaryhmää voi tehdä harjoitusta yhtäaikaisesti.

11.4.2 Osio 1 Setup-toiminnon käyttäminen reitittimessä

Harjoituksen ensimmäisessä osuudessa opiskelijat muodostavat yhteyden reitittimiin terminaalipalvelimen kautta ja konfiguroivat reitittimet käyttäen automaattista Setup-toimintoa. Automaattinen Setup-toiminto eroa hieman kytkimen vastaavasta, tarkoitus on tutustuttaa opiskelijat Setup-toiminnon käyttöön kummassakin laitteessa. Reitittimen peruskonfiguraation tekemisen jälkeen opiskelijat määrittävät reitittimen liitännän Fast-Ethernet 0/1 käyttämän IP-osoitteen ja muuttavat liitännän aktiiviseksi sekä poistavat konsoliviesti ilmoitukset IOS-ruudulta. Konsoliviestit voidaan poistaa pääkäyttäjätilassa IOS-komennolla *no logging console*.

11.4.3 Osio 2 Dynaamisen reitityksen tekeminen RIP-protokollaa käyttäen

Harjoituksen toinen osio käsittelee dynaamista reititystä, jossa käytetään RIP-protokollan 2 versiota. Opiskelijoiden tarkoituksena on käynnistää reitittimen reititys ominaisuus globaalissa konfiguraatiotilassa komennolla *enable ip routing*. Tämän jälkeen opiskelijat tutkivat reitittimen reititystaulua komennolla *shop ip route* ja hakevat reititystaulusta tietoa reitittimen tämän hetkisistä reiteistä ja siitä mihin ryhmään kyseiset reitit kuuluvat.

Seuraavassa vaiheessa opiskelijat määrittävät reitittimelle oletusreitin, joka ohjataan IP-osoitteeseen 10.8.4.1, jossa sijaitsee vlan 8:ssa toimiva DHCP-palvelin. Oletusreitti muodostetaan käskyllä *ip route 0.0.0.0 0.0.0.0 10.8.4.1*, käsky muodostuu kolmesta osasta ensimmäinen ja toinen osa kertovat oletusreitin IP-osoitteen ja aliverkkomaskin olevan tuntemattomia. Tässä tapauksessa kaikki paketit ohjataan osoitteeseen 10.8.4.1, joka on VLAN 8:ssa toimiva DHCP-palvelin.

Viimeisessä vaiheessa opiskelijat käynnistävät reitittimeen RIP-protokollan toimimaan versiolla 2 ja tutkivat RIP-protokollan toimintaa reititystaulusta. RIP-protokolla voidaan käynnistää komennolla *router rip* globaalissa konfiguraatiotilassa. Tämän jälkeen määritellään RIP-protokolla toimivaan versiolla 2 ja verkot, joita protokollan halutaan mainostavan. Protokollan versio määritellään käskyllä *version 2* ja mainostuksessa käytetyt verkot voidaan liittää mainostuksen alle komennolla *network*, johon lisätään verkko-osoite ilman aliverkkomaskia. Molemmat käskyt annetaan RIP-protokollan konfiguraatiotilassa. RIP-protokollan toimintaa tutkitaan reititystaulusta käsin, josta opiskelijat voivat tarkistaa ryhmäkohtaisesti RIP-protokollan mainostamat verkot.

11.4.4 Osio 3 DHCP–protokolla

Harjoituksen kolmas osio käsittelee DHCP–palvelun käyttöönottoa. Opiskelijoiden tehtävänä on käynnisttää DHCP-protokolla reitittimeen. DHCP-protokolla konfiguroidaan jakamaan IP-osoitteita ryhmän omasta verkosta siten, että ryhmän kone saa IP-osoitteen reitittimeltä. DHCP-palvelu vaatii toimiakseen osoiteavaruuden, josta osoitteita jaetaan. DHCP–palvelu otetaan käyttöön reitittimessä käskyllä *ip dhcp pool*, johon lisätään käytettävän poolin nimi. Tämän jälkeen DHCP–palvelu vaatii verkon määrittelyn, josta IP-osoitteita jaetaan muille laitteille. Verkko määritellään komennolla *network*, joka tehdään DHCP-protokollan konfiguraatiotilassa. DHPC-palveluun voidaan myös määrittää oletusreittimen IP-osoite, komennolla *defaut-router*, johon lisätään reitittimen oma IP-osoite.

Viimeinen vaihe sisältää DHCP-palvelun testaamisen ryhmäkohtaisesti, opiskelijat siirtävät koneen reitittimen toiseen porttiin ja testaavat DHCP-palvelun toiminnan. Testauksen tarkoituksena on selvittää, saako kytketty tietokone uuden IP-osoitteen reitittimeltä. Harjoituksen muutettu topologia selviää harjoituksen kuvasta, kohdan yksi tilanne on voimassa harjoituksen alussa ja kohdan kaksi tilanne harjoituksessa DHCP-protokollan testauksen yhteydessä.

11.4.5 Osio 4 Konfiguraation tallennus TFTP-palvelimelle

Harjoituksen viimeisessä osiossa opiskelijoiden tarkoitus on tallentaa tähän asti harjoituksessa luotu konfiguraatio TFTP-palvelimelle. Kopiointi suoritetaan samalla tavoin kun toisessa harjoituksessa kytkimen konfiguraatiolle. Konfiguraatio tallennetaan palvelimelle muodossa ex?group.bin, jossa opiskelijaryhmät erotellaan toisistaan numeroilla. TFTP-palvelin kytketään harjoituksessa Core-kytkimeen jo ennen harjoituksen alkua. Reitittimistä yhteys voidaan TFTP-palvelimelle muodostaa tässä tapauksessa Core-kytkimen kautta.

11.5 5. Harjoitus / Virtuaaliset lähiverkot ja VTP sekä STP-protokollan toiminta

Harjoitus viisi käsittelee virtuaalisten lähiverkkojen konfigurointia kytkimeen sekä VTP ja STP-protokollia, jotka ovat kytkimen toiminnan kannalta erityisen tärkeitä protokollia. Harjoituksen tarkoituksena on käydä läpi miten virtuaalisia aliverkkojen luodaan kytkimeen sekä miten kytkin hoitaa virtuaalisten aliverkkojen tietojenlevityksen lähiverkossa VTP–protokollan avulla. Harjoitus käsittelee myös STP-protokollaa ja sen toimintaa vikatilanteessa. Oppilaiden on tarkoitus testata harjoituksessa STP-protokollan toimintaa käytännössä.

Harjoitus jakautuu kuuteen osioon, ensimmäisessä osiossa oppilaat rakentavat harjoituksen topologian sekä tekevät laitteille perusasetukset. Toinen osio keskittyy VTP-protokollan toimintaan ja siihen mitä tietoa VTP-protokollan avulla saadaan kerättyä. Kolmannessa osiossa käydään läpi kytkimen runkoporttiin liittyviä asetuksia ja sitä miten runkoportin konfigurointi tehdään. Neljäs osio käsittelee virtuaalisten lähiverkkojen luomista kytkimeen sekä oletusreittien ja oletusyhdyskäytävän tekemistä kytkimeen. Viidennessä osiossa käydään läpi STP-protokollaa ja sen toimintaa, jota testataan myös käytännössä. Viimeisessä osiossa kopioidaan kytkimen ja reitittimien konfiguraatiot talteen TFTP-palvelimelle.

11.5.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, joka sisältää viisi työryhmäkytkintä, viisi työryhmäreititintä, viis Core-reititintä, Core-kytkimet A ja B sekä terminaalipalvelimen ja TFTP-palvelimen. Opiskelijat tekevät harjoituksen pareittain, jossa jokainen pari käyttää yhtä työryhmäkytkintä, yhtä työryhmäreititintä sekä Core-reititintä. Opiskelivat rakentavat harjoituksen mukaisen topologian laboratorioon ennen varsinainen harjoituksen tekemistä, kytkemällä tarvittavat laitteet keskenään. Työryhmäkytkimet ja Core-reitittimet kytketään toisiinsa Core-kytkimen kautta, Core-kytkin B on harjoituksessa mukana STP-protokollan testaamisen takia, jolloin mahdollistetaan kaksi eri reittiä, työryhmäkytkimistä Core-kytkimeen A. Harjoitus on suunniteltu tehtäväksi 3-5 ryhmän kesken.

11.5.2 Osio 1 Kytkimen ja reitittimen perusasetukset

Harjoituksen ensimmäisessä osiossa opiskelijat rakentavat harjoituksen topologian kuvan mukaiseksi, kytkemällä tarpeelliset kaapelit laitteiden välille. Kytkennän jälkeen topologia tarkistetaan ja opiskelijaryhmät aloittavat varsinaisen harjoituksen tekemisen asettamalla työryhmäkytkimelle ja työryhmäreitittimelle peruskonfiguraation. Konfiguraatio voidaan tehdä joko manuaalista tapaa käyttäen tai käyttämällä automaattista Setup-toimintoa. Kummatkin tavat ovat tuttuja aiemmista harjoituksista. Laitteiden peruskonfiguraatio sisältää IP-osoitteiden ja aliverkkomaskien konfiguraation, salasanat, laitteen nimen sekä muutaman muun perustoiminnon kuten konsoliviestien poistamisen IOS-komentojen yhteydessä.

11.5.3 Osio 2 VTP-protokollan toiminta

Harjoituksen toinen osio keskittyy VTP-protokollan toimintaan. Opiskelijat tutkivat VTP-protokollan toimintaa kytkimessä osion kysymykset liittyvät mm. VTP-protokollan käyttämään toimintatilaan, siihen mitä tietoä VTP-protokolla lähettää, missä laitteissa VTP-protokolla toimii sekä VTP-pruning toimintoon. VTP-protokollan toimintaa voidaan tutkia kytkimessä käyttämällä käskyä *show vtp status* pääkäyttäjätilassa.

11.5.4 Osio 3 Kytkimen porttien konfigurointi

Harjoituksen kolmas osio keskittyy kytkimen porttikohtaisiin asetuksiin. Opiskelijat harjoittelevat kytkimen porttikohtaisten asetusten tekemistä konfiguroimalla kytkimen portit Fast Ethernet 0/10 ja 0/20 Trunk-porteiksi ja määritämällä Trunk-portille enkapsulointi muodoksi dot1q standardin muotoisen enkapsuloinnin. Portti 0/20 jätetään suljettuun tilaan, jotta STP-protokollan toimintaa voidaan myöhemmässä vaiheessa testata. Kaikki porttikohtaiset asetukset tehdään kytkimessä porttikohtaisen konfiguraatiotilan alla. Kytkimessä haluttu portti voidaan määrittää Trunk-portiksi käyttämällä käskyä *swithport mode trunk*, tämän lisäksi portille määritellään encapsulointi muoto käskyllä *switchport trunk encapsulation*. Osiossa käsitellään myös trunk portin neljää eri toimintomuotoa ja niiden keskinäisiä toimintoja.

11.5.5 Osio 4 Virtuaaliset aliverkot

Harjoituksen neljäs osio keskittyy kytkimen VLAN asetuksiin. Opiskelijoiden on tarkoitus oppia lisäämään ja nimeämään kytkimeen uusi VLAN. Tutkimaan kytkimen VLAN-asetuksia ja oppia tunnistamaan mitä kytkimen oletus VLAN ja hallinta VLAN asetukset merkitsevät. Opiskelijat liittävät tämän jälkeen kytkimen portin 0/1 määriteltyyn VLAN:iin ja konfiguroivat kytkimeen hallinta VLAN:iin. Kytkimeen voidaan luoda uusi VLAN tekemällä asetus suoraan kytkimen VLAN tietokantaan tai vastaavasti luomalla uusi VLAN konfiguraatiotilan kautta. VLAN kohtaisessa konfiguraatiotilassa voidaan tehdä myös VLAN:in nimeäminen ja hallinta VLAN:ia koskevat määritykset mm. VLAN:iin liittyvä IP-osoite. Kytkimen portti voidaan liittää haluttuun VLAN verkkoon komennolla *switchport access vlan (+) vlan tunnus*.

Viimeisessä vaiheessa opiskelijat määrittävät kytkimen portille FA 0/1 IP-osoitteen ja aliverkkomaskin sekä tekevät oletusreitit reitittimille, jotka määritellään osoittamaan Core-reitittimien IP-osoitteita. Työryhmäkytkimille määritellään myös oletusyhdyskäytävä Core-reitittimille. Oletusreitti Core-reitittimelle määritellään *käskyllä default-route 0.0.0.0 0.0.0.0 (+) Core-reitittimen ip-osoite*. Oletusyhdyskäytävä määritellään vastaavasti käskyllä *ip default gateway (+) Core-reitittimen ip-osoite*. Kummatkin käskyt annetaan globaalissa konfiguraatiotilassa.

Edellä mainittujen asetusten teon jälkeen työryhmäkytkimistä on luotu yhteys Core-reitittimille, jota testaan osion viimeisessä vaiheessa ping-komennon avulla. Yhteyden toimiminen Core-kytkimeltä Core-reitittimelle edellyttää, että liitännät FA 0/1 kytkimessä ja reitittimessä ovat aktiivisia. Kytkimen liitäntään FA 0/1 on asetettu IP-osoite ja portti käyttää ryhmäkohtaista VLAN:ia. Kytkimen portti FA 0/20 pitää olla asetettu Trunk-muotoiseksi

portiksi, joka ohjaa liikenteen Core-kytkimelle. Oletusyhdyskäytävien ja oletusreittien määritykset kohti Core-reititintä pitää olla myös määriteltyinä.

11.5.6 Osio 5 STP-protokollan toiminta

Harjoituksen viidennessä osiossa keskitytään STP-protokollan toimintaan ja sen testaukseen. Harjoituksen edellisessä osiossa yhteyttä Core-reitittimelle testattiin, joka on vaatimuksena STP-protokollan testauksessa. Osion ensimmäisessä vaiheessa tutkintaan STP-protokollan toimintaa *show spanning-tree* ja *show spanning-tree (+) vlan tunnus* komennoilla. Opiskelijat tutkivat tämän jälkeen esim. mitä toimintovaiheita STP-protokollassa toimiva portti sisältää ja mikä on juurikytkimenä toimivan kytkimen rooli STP-protokollassa ja miten sen valinta tapahtuu.

Osion viimeinen vaihe keskittyy STP-protokollan käytännön testaukseen. Testauksessa tarkoitus on lähettää loputon echo reply-viestien sarja työryhmäreitittimeltä Core-reitittimelle. Echo reply-viestit käyttävät ensimmäisessä vaiheessa työryhmäkytkimen porttia FA 0/10, jolloin Ping-viesti kulkee perille saakka. Testauksen toisessa vaiheessa kytkimen portti FA 0/20 muutetaan aktiiviseksi ja suljetaan portti FA 0/10. Tämä toimenpide aiheuttaa echo reply-viestien katkeamisen. STP-protokolla havaitsee katkoksen verkon topologiassa ja vaihtaa automaattisesti pakettien kulkusuunnaksi vaihtoehtoisen reitin, joka kulkee liitännän FA 0/20 kautta. STP-protokolla tekee muutoksen noin 30 sekunnin kuluttua vian havaitsemisesta, jonka jälkeen ping-viestit kulkevat Core-reitittimeen toista reittiä pitkin. Testauksen jälkeen osiossa käydään vielä teoriassa läpi STP-protokollan portti roolien merkitystä, MSTP-protokollaa ja STP–protokollan EtherChannel ominaisuutta.

11.5.7 Osio 6 Konfiguraation tallennus

Harjoituksen viimeinen osio sisältää muiden harjoitusten tavoin opiskelijaryhmien konfiguroinnin tallentamisen TFTP-palvelimelle. Konfiguraatiot tallennetaan työryhmäreitittimestä sekä työryhmäkytkimestä. Harjoituksen laitteiden konfigurointia on tarkoitus käyttää hyväksi myös seuraavan harjoituksen kytkin ja reititin laitteiden aloituskokoonpanona.

11.6 6. Harjoitus / Pääsylistojen konfigurointi ja osoitemuunnosten teko

Harjoitus kuusi käsittelee laajennettujen pääsylistojen luomista sekä porttikohtaista osoitemuunnosta ja sen toimintaa. Oppilaiden tarkoituksena on oppia vaikuttamaan verkon liikenteeseen pääsylistojen avulla sekä konfiguroimaan reitittimelle porttikohtainen osoitteenmuutos. Oppilaat luovat harjoituksessa kaksi laajennettua pääsylistaa, joilla

estetään Telnet-liikenne sekä TFTP-protokollan liikenne porttikohtaisen osoitemuutoksen yhteydessä. Harjoituksen lopussa työryhmäreitittimien konfiguraatiot koioidaan Core-kytkimen kautta TFTP-palvelimelle.

11.6.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, jossa on mukana 9 reititintä, Core-kytkin, TFTP-palvelin sekä Terminaali-palvelin. Opiskelijat konfiguroivat harjoituksessa yhtä työryhmäreititintä, johon yhteys muodostetaan Terminaalipalvelimen kautta. Harjoitusta voi yhtäaikaisesti tehdä kuusi opiskelijaryhmää, joista jokainen konfiguroi yhtä työryhmäreititintä. Opiskelijat rakentavat harjoituksen topologian tietoliikennelaboratorioon ennen harjoituksen aloittamista. Harjoituksessa työryhmäreititinpari kytketään Core-reitittimelle, joka hoitaa työryhmäparin välistä liikennettä.

11.6.2 Osio 1 Laitekonfiguraation haku TFTP-palvelimelta

Harjoituksen ensimmäinen osio käsittelee edellisen harjoituksen konfiguraation hakemista TFTP-palvelimelta. Harjoituksessa on tarkoitus jatkaa reitittimien konfiguraatiota edellisestä harjoituksesta. Tämä toteutetaan siten, että jokainen opiskelijaryhmä hakee omaan reitittimeensä konfiguraation TFTP-palvelimelta, joka tallennettiin edellisen harjoituksen lopussa. Konfiguraation haku laitteisiin vaatii toimivan yhteyden TFTP-palvelimelle. Konfiguraation hakemisen jälkeen laite käynnistetään uudestaan, jotta konfiguraatio tulee voimaan reitittimeen. Tämän jälkeen opiskelijat valmistelevat harjoituksen topologian tietoliikennelaboratorion laitteille kuvan mukaisesti. Harjoituksen topologiaa tarkistetaan ennen varsinaisen harjoituksen aloittamista.

11.6.3 Osio 2 Staattisten reittien luominen

Harjoituksen toinen osio käsittelee staattisen reitityksen tekemistä. Opiskelijoiden tarkoituksena on luoda staattiset reitit opiskelijaparien kesken. Staattinen reitti luodaan siten, että opiskelijaparit muodostavat keskinäiset yhteydet reitittimien välille. Staattinen reitti tehdään Core-reitittimen kautta, jonka asetukset ovat konfiguroitu harjoituksessa etukäteen.

Osion ensimmäisessä vaiheessa opiskelijat asettavat reitittimen liitännät FA 0/0 ja FA 0/1 aktiiveksi sekä määrittävät liitäntöihin IP-osoitteen ja aliverkkomaskin kuvan mukaisesti. Tämän jälkeen opiskelivat määrittävät työryhmäreitittimeltä oletusreitin Core-reitittimelle sekä staattisen reitin toiselle työryhmäreitittimelle. Staattinen reitti luodaan oletusreitin tavoin IOS-komennolla *ip route (+) kohdeverkon ip-osoite (+) kohdeverkon aliverkkomaski (+)*

seuraavan hypyn ip-osoite. Tämän avulla reititin tietää mitä liitäntää käyttäen kyseiseen verkkoon päästään. Reittien tekemisen jälkeen reitittimien reititystaulut tarkastetaan. Konfiguroinnin onnistuttua staattinen reitti löytyy reitittimen reititystaulusta, tämän jälkeen opiskelijat testaavat reitin toimivuutta lähettämällä echo-reply-komennon naapurilaitteille.

11.6.4 Osio 3 Pääsylistojen konfigurointi

Harjoituksen kolmas osio käsittelee pääsylistoilla tapahtuvaa liikenteen rajoittamista. Opiskelijoiden tarkoituksena on tässä osiossa luoda pääsylista numerolla 110, jonka tarkoituksena on estää Telnet-liikenteen kulku työryhmäreitittimien välissä ja sallia ICMP-protokollan liikenne. Lista kiinnitetään reitittimen porttiin FA 0/1 sisäänpäin menevälle liikenteelle. Listan toimivuutta testataan osion lopussa Telnet-yhteyden avulla.

Pääsylistan asentaminen reitittimen porttiin sisältää kaksi vaihetta ensimmäisessä vaiheessa pääsylista luodaan haluttujen ehtojen perusteella komennolla *ip access-list*, johon lisätään pääsylistan numero ja pääsylistan ehto määritykset. Pääsylistamäärityksillä kerrotaan listalle mitä liikennettä listalla halutaan päästää läpi ja mitä liikennettä rajoittaa. Esimerkiksi harjoituksessa vaadittava lista voidaan määrittää komennoilla *ip access list 110 deny tcp (+) työryhmä-reitittimen ip-osoite ja käänteinen aliverkkomaski (+) Core-reitittimen ip-osoite ja käänteinen aliverkkomaski*. Tämän jälkeen listaan lisätään vielä ICMP-liikenteen salliva määritys komennolla *access list 110 permit icmp any any*. Tehty lista kieltää reitittimien välisen Telnet-liikenteen, mutta sallii ICMP-protokollan liikenteen.

Pääsylistan teon toisessa vaiheessa lista kiinnitetään paikalleen oikeaan liitäntään ja määritellään listalle suunta, mitä liikennettä rajoitetaan. Pääsylista voidaan kiinnittää haluttuun porttiin komennolla *ip-access group*, jonka jälkeen määritetään listan numero mitä listaa portissa halutaan käyttää sekä suunta mitä liikennettä listalla halutaan kieltää.

11.6.5 Osio 4 Porttikohtainen osoitemuunnos

Harjoituksen neljäs osio sisältää porttikohtaisen osoitemuutoksen tekemisen reitittimessä. Oppilaiden tarkoitus on konfiguroida työryhmäreititin siten, että reititin hoitaa IP-osoite muutoksen käyttämällä porttikohtaista osoitemuutosta, josta käytetään nimitystä PAT (Port address translation). Porttikohtaista osoitemuutosta suorittavalle reitittimelle liitetään pääsylista, jossa määritellään mitä liikennettä muutos koskee. Oppilaiden tarkoitus on määrittää reitittimelle pääsylistä, joka kieltää TFTP-liikenteen ja sallii ICMP-liikenteen reitittimen läpi.

Osion alussa opiskelijat määrittävät pääsylistan numerolla 120, jonka tarkoituksena on estää TFTP-yhteys palvelimelle, mutta sallia ICPM-protokollan liikenne eli palvelimeen menevät echo-viestit. Työryhmäreititin määritellään tekemään IP-osoitteille PAT-muunnos. Tämä tapahtuu määrittämällä reitittimen portteihin porttiroolit PAT-muunnoksessa. Portin rooli määritellään sisäänpäin menevälle portille komennolla *IP nat inside* ja ulosmäin menevälle portille komennolla *IP nat outside*. Porttiroolien määrityksen jälkeen pääsylista 120 kiinnitetään rajoittamaan PAT-prosessin liikennettä komennolla *ip nat inside source list 120 interface FA 0/0 overload*.

Osion lopussa opiskelijat testata PAT-prosessin toimintaa naapuriryhmän avulla siten, että naapuriryhmä yrittää muodostaa yhteyttä TFTP-palvelimeen toisen ryhmän PAT-prosessin läpi. PAT-prosessin toiminta edellyttää, että muutos tehdään porttien välillä ja kaikki prosessin läpi mennyt liikenne taltioidaan PAT-tauluun. Tätä taulua tutkimalla ryhmä voi tarkistaa toimiiko PAT-osoitemuunnos. Komentoja *show ip nat translations* sekä *show ip nat statistics* voidaan käyttää PAT-prosessin tutkimisessa.

11.6.6 Osio 5 Konfiguraatiotiedostojen tallennus

Harjoituksen viimeinen vaihe sisältää reititin konfiguraatioiden tallentamisen TFTP-palvelimelle. Konfiguraatiot tallennetaan talteen kaikista työryhmäreitittimistä. Seuraavassa harjoituksessa on tarkoituksena käyttää työryhmäreitittimien aloituskokoonpanona tämän harjoituksen reitittimien konfiguraatiota.

11.7 7. Harjoitus / OSPF-ja EIGRP-reititysprotokollat

Harjoitus seitsemän käsittelee reititysprotokollien toimintaa ja niiden konfigurointiin liittyviä asetuksia. Harjoituksessa käsitellään kahta reititysprotokollaa OSPF-protokollaa sekä EIGRP-protokollaa. Harjoituksen perusteella opiskelijat oppivat konfiguroimaan reititysprotokollan reitittimelle ja käyvät läpi protokollien toimintaa, salausta ja seuraavat protokollien välistä liikennettä.

Harjoitus jakautuu viiteen osa-alueeseen, joista ensimmäisessä valmistellaan harjoituksen topologia laboratoriossa ja laitteiden konfiguraatiot haetaan TFTP-palvelimeltä. Toinen osa käsittelee vanhojen konfiguraatioiden poistamista IOS-järjestelmästä. Kolmannessa osiossa harjoitellaan OSPF-reititysprotokollan konfigurointia, salausta sekä monitorointia. Neljännessä osiossa käsitellään vastaavasti EIGRP-protokollan toimintaa. Viimeinen osio sisältää harjoituksen konfiguraatioiden tallentamisen TFTP-palvelimelle.

11.7.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, jossa on mukana seitsemän työryhmäreititintä, yksi Core-reititin, kaksi Core-kytkintä, TFTP-palvelin ja Terminaalipalvelin. Työryhmäreitittimet kytketään Core-kytkimen kautta Core-reitittimeen, jossa reitittimet erotellaan toisistaan aliliitäntöjen avulla. Core-kytkimen kaksi kautta opiskelijat ovat yhteydessä TFTP-palvelimelle. Opiskelijat konfiguroivat harjoituksessa työryhmäreitittimiä ja tekevät muutamia asetuksia myös Core-kytkimeen ja Core-reitittimeen. Opiskelijat rakentavat harjoituksen topologian tietoliikennelaboratorioon ennen harjoituksen aloittamista. Kuusi opiskelijaryhmää voi tehdä harjoitusta yhtäaikaisesti.

11.7.2 Osio 1 Topologian rakennus ja konfiguraatioiden haku

Harjoituksen alussa opiskelijat hakevat harjoitukseen liittyvän konfiguraation reitittimille TFTP-palvelimelta ja rakentavat harjoituksen verkkotopologian tietoliikennelaboratorioon. Opiskelijoiden tarkoituksena on käyttää harjoituksessa edellisen harjoituksen jälkeistä konfiguraatiota, jota muokataan uuteen harjoitukseen sopivaksi poistamalla vanhoja asetuksia. Harjoituksen topologia tarkistetaan ennen seuraavaan osioon siirtymistä.

11.7.3 Osio 2 IOS-konfiguraation hallinta

Harjoituksen toinen osio käsittelee IOS-käyttöjärjestelmän konfiguraation muokkaamista harjoitukseen sopivaksi. Opiskelijoiden tarkoituksen on muokata edellisen harjoituksen konfiguraatiota reitittimissä siten, että kaikki ylimääräiset asetukset laitteilta poistetaan. Konfiguraatiosta poistetaan esimerkiksi PAT-toiminto, pääsylistoihin liittyvät asetukset, kaikki staattiset reitit sekä porttikohtaiset IP-osoiteasetukset. Asetuksia voidaan poistaa käyttämällä komentoa *no* normaalin komennon edessä. Osion tarkoituksena on kehittää opiskelijoiden kykyä lukemaan reitittimen konfiguraatiota tarpeeksi hyvin, jotta he voivat tämän perusteella löytää poistettavat asetukset laitteesta.

11.7.4 Osio 3 OSPF-reititysprotokollan konfigurointi

Harjoituksen kolmas osio käsittelee OSPF-protokollan konfigurointia. Opiskelijoiden tarkoitus on saada OSPF-reititysprotokolla mainostamaa dynaamisesti reitittimen verkkoa muille laitteille. Opiskelijat tutkivat aluksi OSPF-protokollan loopback-liitännän merkitystä ja konfiguroivat IP-osoitteen loopback-liitäntään. Loopback liitännän konfigurointitilaan päästään komennolla *interface loopback*. Loopback-liitännän konfiguroinnin jälkeen opiskelijaryhmät käynnistävät reitittimille OSPF-reititysprotokollan komennolla *router ospf (+) prosessitunnus*. Tämän jälkeen opiskelijat määrittävät protokollan mainostamaan ryhmien

omaa verkkoa reitittimien liitäntöjen FA 0/0,FA 0/1 sekä loopback-liitännän kautta. Ryhmien kaikki reitittimet konfiguroidaan alueelle 0, joka tarkoittaa ns. backbone aluetta, johon kaikki muut alueet ovat yhdistettyinä. Reitittimen liitäntä voidaan konfiguroida OSPF-protokollan alueelle 0 komennolla *network (+) liitännän ip-osoite (+) käänteinen maski (+) area 0.* Konfiguroinnin jälkeen opiskelijat tutkivat reitittimen reititystaulua ja reitittimen suhteita naapurireitittimiin ja hakevat näiden perusteella tietoa OSPF-protokollan toiminnasta.

Osion seuraava vaihe keskittyy ryhmäkohtaisesti Core-laitteiden konfigurointiin. Kaikki ryhmät tekevät ryhmäkohtaiset asetukset Core-kytkimelle ja Core-reitittimelle. Core-kytkimen asetus koskee kytkimen portin asentamista oikeaan VLAN:iin ryhmäkohtaisesti. Core-reitittimelle portiin FA 0/0 tehdään virtuaaliliitäntä ryhmäkohtaisesti siten, että jokaisesta ryhmästä liikenne kulkee kytkimen VLAN:in määrityksen kautta virtuaaliseen liitäntään reitittimelle.

Virtuaalisen liitännän konfiguraatio sujuu normaalin liitännän konfiguroinnin tavoin. Poikkeuksena virtuaalisen liitännän alaiseen konfiguraatiotilaan tarvitaan, esimerkiksi IOS-komento *interface FA 0/0.1.* Pistettä käytetään tässä tapauksessa erottelemaan haluttu aliliitäntä varsinaisesti liitännästä. Toisena eroavaisuutena on se, että liitäntä joudutaan liittämään tiettyyn VLAN:iin, jotta liikenne voidaan erotella toisistaan. VLAN kohtainen määritys voidaan tehdä reitittimen liitäntään komennolla *encapsulation dot1q vlan (tunnus)*. Näiden kahden määritysten jälkeen reitittimien välinen liikenne käyttää liikennöintiin Core-reitittimen virtuaaliliitäntää.

Osion viimeinen vaihe käsittelee OSPF-protokollan salaukseen liittyviä asioita. Opiskelijoiden tehtävänä on konfiguroida OSPF-protokollaan salaus, joka käyttää selväkielistä tekstiä salauksessa. Salausta testataan osion lopussa, kokeilemalla yhteyksien toimivuutta salauksen asettamisen jälkeen. Osion lopussa OSPF-reititys vielä poistetaan reitittimeltä.

Salaus voidaan määrittää reitittimelle komennolla *ip ospf authentication* globaalissa konfiguraatiotilassa. Salausmääritys tarvitsee tunnus tekstin, jota käytetään salauksessa hyväksi. Selväkielinen salaus ei salaa salauksessa käytettävää tunnustekstiä, vaan tunnus kulkee paketin mukana selväkielisessä muodossa. Selväkielinen salaus voidaan määrittää liitäntäkohtaisesti liitännän alaisessa konfiguraatiotilassa *komennolla ip ospf authentication-key (+) tunnusteksti*. Opiskelijat määrittävät salauksen omaan työryhmäreitittimeensä sekä Core-reitittimelle ja testaava salauksen toimivuutta tämän jälkeen. Viimeinen vaihe testauksessa tehdään muuttamalla salauksessa käytettävää salasanaa yhteen laitteeseen ja testaamalla liikennettä muutoksen jälkeen. Yhteyden pitäisi katketa välittömästi salasanamuutoksen jälkeen, koska reitittimien väliset yhteydet eivät voi toimia reitittimien välillä, jos salaus puuttuu jostakin reitittimestä tai laiteet käyttävät eriäviä tunnuksia.

11.7.5 Osio 4 EIGRP-reititysprotokollan konfigurointi

Harjoituksen neljännessä osiossa opiskelijat konfiguroivat EIGPR-reititysprotokollan ja testaavat sen toimintaa. Opiskelijoiden tarkoituksena on saada reititys toimimaan reitittimien välillä EIGRP-protokollan avulla. EIGRP-protokolla käynnistetään komennolla *router eigrp (+) systeemi numero* globaalissa konfiguraatiotilassa. EIGRP-käyttää reititykseen järjestelmä numeroa, joka pitää olla sama kaikissa reitittimissä, joiden välillä liikennettä halutaan kulkevan. EIGRP-protokollassa verkon määritys voidaan tehdä IOS-komennolla *network (+) verkko-osoite (+) käänteinen maski*. Konfiguroinnin jälkeen opiskelijat seuraavat EIGRP-reitityksen toimintaa reititystaulutietojen ja naapuritietojen perusteella. Reitityksen toimintaa seurataan myös käyttämällä *debug ip eigrp* sekä *debug ip eigrp packet* komentoja, näiden käskyjen avulla reitityksessä kulkevia paketteja voidaan seurata reaaliaikaisesti IOS-käyttöliittymän kautta.

Osion viimeisessä vaiheessa EIGRP-protokollaan liitetään autentikointi, joka käyttää suojattua menetelmää. Salattu autentikointi perustuu MD5-pohjaiseen salausmenetelmään. Salauksessa määritellään nimettyjä avainryhmiä, jotka koostuvat monista avaimista. Yksittäiselle avaimelle voidaan määrittää voimassaoloaika, jonka aikana avainta voidaan käyttää. Opiskelijat määrittävät salausharjoituksessa yhden avainryhmän, joka sisältää kaksi avainta eri voimassaoloajoilla.

Reitittimessä EIGRP-protokollan MD5–menetelmään pohjautuva salaus käynnistetään komennolla *ip authentication mode eigrp md5* globaalissa konfiguraatiotilassa. Salausavaimet määritellään komennolla *ip authentication eigrp key-chain (+) avainlistan nro (+) avainlistan nimi*. Yksittäiset avaimet voidaan määritellä tämän jälkeen komennolla *key (+) avaimen nro*. Viimeisenä vaiheena avaimelle määritellään voimassaoloaika komennolla *key-string (+) nimi* ja tämän jälkeen nimeen perustuva tunnuksen hyväksymisaika komennolla *accept lifetime (+) aloitusaika (+) lopetusaika*. Hyväksymisaika määritellään muodossa kellon aika, kuukausi, päivämäärä ja vuosi. Tämän jälkeen avaimeen voidaan määrittää vielä tunnusta koskeva lähetysaika määritys samalla menetelmällä, komennolla *send lifetime (+) aloitusaika (+) lopetusaika*.

Opiskelijat testaavat salauksen määrityksen jälkeen sen toimintaa, salauksen toiminnan edellytyksenä on, että kaikki laitteet käyttävät samaa salausmenetelmää ja jotain voimassaolevaa avainta. Testissä kokeillaan myös miten EIGRP-reititys reagoi siihen, että työryhmäreitittimeltä poistetaan käytössä oleva avainsarja. Harjoituksen viimeisessä vaiheessa EIGPR-reititys poistetaan käytöstä.

11.7.6 Osio 5 Konfiguraation tallennus

Harjoituksen viimeinen vaihe sisältää reititin konfiguraatioiden tallentamisen TFTP-palvelimelle. Konfiguraatiot tallennetaan talteen kaikista työryhmäreitittimistä. Seuraavassa harjoituksessa on tarkoituksena käyttää työryhmäreitittimien aloituskokoonpanona tämän harjoituksen reitittimien lopullista konfiguraatiota.

11.8 8. Harjoitus / IPv6–reitityksen konfigurointi

Harjoituksessa käsitellään IPv6:n toimintaa ja sen konfigurointia. Oppilaiden tarkoituksena on saada työryhmäreitittimien välillä liikenne kulkemaan staattisesti luotujen reittien kautta sekä RIPng reititysprotokollan avulla. Opiskelijat tutustuvat harjoituksessa myös IPv6-osoitteiden rakenteeseen sekä kirjoitusmuotoon.

Harjoitus jakautuu viiteen osioon, ensimmäisessä vaiheessa opiskelijat noutavat reititinkohtaisen konfiguraation TFTP-palvelimelta ja rakentavat harjoituksen topologian tietoliikennelaboratorion laitteilla. Toisessa osiossa edellisen harjoituksen konfiguraatiosta poistetaan asetukset, jotka eivät liity IPv6-harjoituksen toteutukseen. Kolmannessa osiossa keskitytään IPv6-protokollan konfiguroimiseen ja luodaan IPv6-protokollaa tukevat staattiset reitit työryhmäreitittimien väliin. Neljännessä osiossa luodaan reitittimille IPv6-protokollaa tukeva dynaaminen reititys RIPng-protokollan avulla. Harjoituksen viimeinen osio sisältää tietojen tallentamisen TFTP-palvelimelle.

11.8.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, joka sisältää 5 työryhmäreititintä, 2 Core-kytkintä, 1 Core-reitittimen sekä TFTP-palvelimen ja Terminaalipalvelimen. Työryhmäreitittimet yhdistetään Core-kytkimen kautta Core-reitittimelle. Opiskelijaryhmät erotellaan edellisen harjoituksen tavoin Core-reitittimessä virtuaaliporteilla. Opiskelijat konfiguroivat harjoituksessa työryhmäreitittimiä sekä Core-kytkintä ja Core-reititintä. Opiskelijat tallentavat harjoituksen lopussa laitekonfiguraatiot TFTP-palvelimelle. Harjoitusta voi tehdä viisi opiskelijaryhmää yhtäaikaisesti.

11.8.2 Osio 1 Harjoituksen topologia sekä laitekonfiguraatiot

Harjoituksen alussa opiskelijat rakentavat tietoliikennelaboratorioon kuvan mukaisen topologian ja hakevat edellisen harjoituksen konfiguraation TFTP-palvelimelta. Topologia tarkistetaan ennen seuraavaan osioon siirtymistä.

11.8.3 Osio 2 Konfiguraation hallinta

Harjoituksen toisessa osiossa muokataan reitittimien konfiguraatioita, poistamalla konfiguraatiosta edellisen harjoituksen asetukset, jotka eivät liity IPv6-harjoitukseen. Reitittimen konfiguraatiosta poistetaan IPv4-reititysprotokollat, porttikohtaiset asetukset sekä staattiset reitit. Opiskelijoiden tarkoituksena on saada reititin käyttämään oletusasetuksia, jotta IPv6-reitityksen tekeminen onnistuu. Osion tarkoituksena on kerrata edellisestä harjoituksesta reitin konfiguraation hallintaa ja sen ymmärtämistä.

11.8.4 Osio 3 IPV6-osoitteiden konfigurointi ja staattiset reitit

Harjoituksen kolmannessa osiossa opiskelijat luovat reitittimien välisen yhteyden staattisen reitityksen avulla. Reitityksen tekemisessä käytetään tässä harjoituksessa IPv6-osoitteita. Opiskelijaryhmä luo omalta reitittimeltään staattisen reitin toisen ryhmän laitteelle Core-reitittimen kautta. Ennen reittien luomista reitittimelle joudutaan käynnistämään IPv6-reititys IOS-komennolla *ipv6 unicast routing* globaalissa konfiguraatiotilassa. Harjoituksessa käytetään IPv6-protokollan eui-64 muotoa tapaa osoitteiden yhteydessä. Esimerkiksi opiskelijaryhmä 1 käyttää reitittimessä IPv6-osoitetta 2430:1111:AAAA:1 /64, jossa käytetään osoitteeen loppuosan merkitsemisessä, reitittimen MAC-osoitetta sekä täytebittejä.

Opiskelijat määrittävät eui-64 muotoisen IPv6-osoitteen reitittimen porttiin FA 0/1 komennolla *ipv6 address (+) ipv6-osoite* eui-64 muodossa. IPv6-osoitteen yhteydessä ei tarvita aliverkkomaskin määrittämistä. Portin määrittämisen jälkeen opiskelijat luovat staattisen reitin toiseen reitittimeen. Staattinen IPv6-reitti luodaan samalla tavoin kun IPv4-reitti, ainoana poikkeuksena osoitteina käytetään IPv6-osoitteita. Reitti määritellään IOS-komennolla *ipv6 route (+) kohdereitittimen ipv6-osoite (+) seuraavan hypyn ipv6-osoite* globaalissa konfiguraatiotilassa. Opiskelijat tutkivat tämän jälkeen reitittimen IPv6-reititystaulua staattisten reittien osalta komennolla show *ipv6 route*.

Osion seuraavassa vaiheessa opiskelijat luovat Core-kytkimelle ryhmäkohtaiset VLAN-asetukset sekä Core-reitittimen virtuaaliporttiin IPv6-asetukset, jotta liikenne toiseen ryhmään saavutetaan. Core-laitteiden konfiguraation tekemisen jälkeen IPv6-reititystaulu tarkistetaan uudestaan ja tehdään IPv6-reittien testaukset käyttämällä ping-komentoa toisen ryhmän reitittimen porttiin FA 0/1. Osion viimeisessä vaiheessa IPv6:een pohjautuvat staattiset reitit poistetaan laitteilta.

11.8.5 Osio 4 RIPng-reititysprotokolla

Harjoituksen neljännessä osiossa käsitellään RIP-protokollan IPv6-reititystä tukevaa protokollaa RIPng:tä (next generation) sekä IPv6-osoitteiden koostumusta. Opiskelijat käynnistävät tässä vaiheessa harjoitusta RIPng-protokollan toimimaan reitittimissä sekä asettavat protokollan toimimaan reitittimen porttiin FA 0/1. IPV6-reititysprotokollan toimimisen edellytyksenä vaaditaan, että protokolla määritellään erikseen porttikohtaisesti. RIPng-protokolla otetaan käyttöön reitittimissä komennolla *ipv6 router rip (+) tunnus* globaalissa konfiguraatiotilassa ja määritellään toimimaan reitittimen porttiin komennolla *ipv6 rip (+) tunnus enable*.

Osion viimeisessä vaiheessa opiskelijat konfiguroivat ryhmäkohtaisesti RIPng-protokollan toimimaan Core-reitittimen virtuaaliliitännöissä ja tutkivat miten IPv6-reititys toimii käytännössä. Reititystä testataan työryhmäreitittimien välillä ping-komennon avulla. Osion loppuosassa käsitellään IPv6-protokollan eri lähetysmuotoja ja tunnelointia.

11.8.6 Osio 5 Konfiguraation tallennus

Harjoituksen viimeinen vaihe sisältää reitin konfiguraatioiden tallentamisen TFTP-palvelimelle. Konfiguraatiot tallennetaan talteen kaikista työryhmäreitittimistä. Viimeisessä harjoituksessa on tarkoituksena käyttää työryhmäreitittimien aloituskokoonpanona tämän harjoituksen reitittimien lopullista konfiguraatiota.

11.9 9. Harjoitus / WLAN-verkot sekä ACS–palvelun toiminta

Harjoitus yhdeksän käsittelee WLAN-verkkojen toimintaa sekä ACS-palvelimella tapahtuvaa verkkoliikenteen salausta. Opiskelijoiden tarkoituksena harjoituksessa on saada tietoliikennelaboratorioon rakennettua kaksi WLAN-verkkoa, jotka toteutetaan käyttämällä Ciscon Aironet 1100 langattomia tukiasemia sekä Ciscon Secure Access Control palvelinta.

Harjoitus jakautuu kuuteen osa-alueeseen, jossa ensimmäisessa haetaan kytkinkonfiguraatio harjoituksesta viisi, jossa kytkinkonfiguraatio on edellisen kerran tallennettu TFTP-palvelimelle. Konfiguraatiosta poistetaan ylimääräiset VLAN ja Trunk portti asetukset. Harjoituksen toisessa osassa konfiguroidaan harjoituksen kytkin toimimaan WLAN-verkossa. Kytkimeltä tehdään yhteydet tukiasemiin ja ACS-palvelimelle ryhmäkohtaisesti. Harjoituksen kolmannessa osassa siirrytään konfiguroimaan WLAN-tukiasemia selainyhteyden kautta. Tukiasemiin konfiguroidaan perusasetukset VLAN asetukset sekä käytettävät salausmenetelmät. Tämän jälkeen tukiasemiin määritellään kaksi käytettävää verkkoa yksi

salattu WLAN-verkko ja yksi suojaamaton WLAN-verkko. Harjoituksen neljäs osio jakautuu ACS-palvelimen asetuksiin, jota opiskelijaryhmät konfiguroivat yksittäisesti. ACS-palvelimelle tehdään asetukset jokaista ryhmän tukiasemaa kohden. Harjoituksen viides osio käsittelee WLAN-verkkokorttikohtaisia asetuksia tietokoneesta ja kahden WLAN verkon testausta. Harjoituksen viimeisessä osiossa laitteiden konfiguraatiot tallennetaan TFTP-palvelimelle.

11.9.1 Harjoituksen topologia

Harjoituksessa käytetään topologiaa, joka sisältää kuusi työryhmäkytkintä,Core-kytkimen, kuusi Cisco Access Point tukiasemaa, Core-reititimen sekä Terminaali-palvelimen ja TFTP-palvelimen. Harjoituksen topologia rakennetaan siten, että jokainen opiskelijaryhmä saa käyttöönsä yhden työryhmäkytkimen sekä yhden WLAN-tukiaseman. Harjoituksen alussa konfiguroidaan työryhmäkytkintä, johon luodaan VLAN verkot jokaista ryhmää kohden. Harjoituksen keskivaiheessa topologia vaihtuu siten, että tietokoneet kytketään suoraan työryhmäkytkimiin WLAN-asetusten testaamista varten. Harjoituksen konfiguraatio rakennetaan ennen harjoituksen aloittamista ja tallennetaan harjoituksen lopussa TFTP-palvelimelle. Harjoitusta voi tehdä 6 opiskelijaryhmää kerrallaan.

11.9.2 Osio 1 Konfiguraation haku

Harjoituksen alussa opiskelijaryhmät rakentavat harjoituksen mukaisen topologian tietoliikennelaboratorioon ja noutavat kytkimien konfiguraation TFTP-palvelimelta. Topologian tarkistetaan ennen varsinaisen harjoituksen aloittamista.

11.9.3 Osio 2 Kytkimen asetukset

Harjoituksen toinen osio käsittelee kytkimeen tehtäviä asetuksia. Opiskelijat määrittävät kytkimen portin FA 0/20 ja FA 0/10 asetuksia. Porttiin FA 0/20 asetetaan toimimaan Trunk-porttina, josta liikenne ohjataan tukiasemiin. Trunk-portti määritellään sallimaan VLAN:it 8,26 ja 150. Porttia FA/10 käytetään harjoituksen seuraavassa vaiheessa WLAN–tukiasemien konfiguroinnissa. Kytkimelle asetetaan VLAN 150 toimintamuodoksi Natiivi VLAN muoto, IOS-komennolla *swithport trunk vlan 150 native*. Natiivimuotoisen VLAN:in erottaa siitä, että natiivi VLAN:iin konfiguroitu portti ei tarvitse mitään datan enkapsulointi muotoa. Kytkimen portti FA 0/10 kytketään VLAN:iin 150, jotta ryhmät voivat muodostaa oman tietokoneensa kautta yhteyden ryhmän tukiasemaan. Osion viimeisessä vaiheessa kytkimen portti FA 0/24 muutetaan Trunk-muotoon, jotta yhteys Core-laitteisiin ja TFTP-palvelimelle toimii. Viimeisenä vaiheena ryhmän tietokone siirretään kytkimen porttiin FA 0/10 ja kokeillaan saako ryhmän tietokone IP-osoitteen Core-reitittimen DHCP-palvelulta.

11.9.4 Osio 3 WLAN tukiasemien konfigurointi

Harjoituksen kolmas osuus käsittelee tukiasemien konfigurointia. Jokainen opiskelijaryhmä konfiguroi omaa tukiasemaansa ja määrittelee tukiasemaan kaksi WLAN-verkkoa, jotka toimivat eri taajuuksilla ja salauksella. Yhteys tukiasemaan muodostetaan selaimen kautta IP-osoitteen perusteella, suositeltavin tapa on käyttää Internet Explorer selainta.

Tukiasemaan tehdään asetuksia graafisen käyttöliittymän (GUI) avulla. Opiskelijat tekevat asetukset ja vastaavaan komennon lisäksi myös kysymykseen missä tilassa mikäkin komento tehdään, jotta tukiaseman graafinen ympäristö tulisi tutuksi. Ensimmäisessä vaiheessa opiskelijat luovat tukiaseman perusasetukset, tukiaseman nimen sekä käyttäjätunnukset tukiasemaan kirjauduttuessa. Toisessa vaiheessa tukiasemaan tehdään VLAN-kohtaiset asetukset samalla tavoin mitä tehtiin harjoituksen toisessa vaiheessa kytkimelle. VLAN-perusasetusten lisäksi määritellään VLAN-kohtainen salausmenetelmä TKIP, jota hallinta VLAN 8 käyttää. Kolmas vaihe sisältää Cisco Radius-palvelimen lisäämisen tukiasemien käyttöön. Palvelimelle määritellään IP-osoite ja EAP-muotoinen autentikointi. Osion viimeisessä vaiheessa määritellään varsinaiset WLAN-verkot tukiasemiin niiden SSID-tunnukset ja käytetyt radiotaajuudet. Verkkoja luodaan kaksi erilaista WG?-Common verkko toimii VLAN 8:ssa ilman salausmenetelmää. WG?-Secure verkko on VLAN 26:ssa toimiva suojattu verkko, joka käyttää EAP-autentikointi menetelmää. Kummatkin verkot toimivat eri radiotaajuudella, jotta ne eivät häiritse toisiaan.

11.9.5 Osio 4 ACS-palvelimen konfigurointi

Harjoituksen neljäs osio käsittelee ACS-palvelimen konfigurointia. Opiskelijaryhmät tekevät ACS-palvelimelle ryhmäkohtaiset asetukset. Asetukset liittyvät tukiasemien lisäämiseen palvelimelle sekä autentikoinnin määrittämiseen. Tukiasemien lisäksi palvelimelle määritellään ryhmäkohtaiset tunnukset ja salasanat, jota tukiasemat käyttävät kommunikoidessaan palvelimen kanssa.

11.9.6 Osio 5 WLAN-verkkojen testaus

Harjoituksen viidennessä osiossa opiskelijaryhmät testaavat WLAN-verkkojen toimivuutta tietoliikennelaboratoriossa. Verkkojen toimiminen edellyttää, että tietokoneen langattomaan verkon verkkokortti konfiguroidaan oikein. Verkkoja testaan vuorotellen, ensimmäisessä vaiheessa testataan suojaamatonta verkkoa. Verkkoyhteyden saamiseksi suojaamattomaan verkkoon verkkokortille määritellään asetukseksi salaamaton verkko ja SSID-tunnus WG?-Common, jolloin kone saa IP-osoitteen VLAN 26:n kautta.

Suojatun verkon toiminta edellyttää, että opiskelijaryhmät määrittävät TKIP ja Protected-EAP tyyppiset salausmääritykset verkkokortille sekä kirjautumisen käyttäjätunnuksilla. Yhteyden muodostumisen jälkeen opiskelijat kirjautuvat verkkoon omilla tunnuksillaan, vasta kirjautumisen jälkeen verkon resurssit ovat saatavilla. Salatun verkon SSID-tunnuksena käytetään tunnusta WG?-Secure. Kirjautumisen onnistuessa opiskelijaryhmän koneet saavat IP-osoitteet suojatusta VLAN 8:sta.

11.9.7 Osio 6 Konfiguraatioiden tallennus

Harjoituksen viimeinen vaihe käsittelee konfiguraatioiden tallentamista TFTP-palvelimelle. Konfiguraatiot tallennetaan talteen kaikista työryhmäreitittimistä sekä kaikista Cisco tukiasemista. Tukiaseman konfiguiroinnin tallentamisessa tukiasemaan IOS-käyttöliittymään luodaan yhteys Telnet-yhteyden kautta. Konfiguraation kopiointi tehdään samalla komennolla kuin normaalisti pääkäyttäjätilan komennolla *copy running-config tftp*.

12 Palautekyselyn toteuttaminen

Opiskelijoille suunnattu palautekysely tehtiin vanhojen harjoitusten pohjalta. Palautekyselyyn vastanneet opiskelijat olivat pääsääntöisesti Laurea-ammattikorkeakoulun toisen ja kolmannen vuoden opiskelijoita. Palautekyselyn tarkoituksena oli saada selville mikä opiskelijoiden mielestä oli harjoitusten yleinen vaikeustaso, mitkä aiheet olivat helppoja ja mitkä vaikeita sekä mihin osa-alueisiin minun tulisi keskittyä uusien harjoituksien tekemisessä. Palautelomakkeissa painotin muutamia seikkoja, joita olivat viikkokohtaisien harjoitusten yleinen vaikeustaso, harjoitusten teoriapainotukset sekä kuvien selkeys.

Palautekysely toteutettiin huhtikuun lopulla viimeisen harjoituskerran yhteydessä. Palautelomake jakautui kahteen osaan viikkokohtaisien harjoitusten osioihin sekä vapaasanapalautteeseen. Viikkokohtaisten harjoitusten palauteosio sisälsi kysymykset harjoituksen yleisestä vaikeustasosta sekä harjoitukseen kuuluvista teoriaosuuksista, näiden lisäksi kysyttiin harjoitukseen liittyvästä kuvasta sekä aiheeseen liittyvästä luennosta. Vapaasanaosuuden tarkoituksena oli antaa yleistä palautetta kurssista sekä opetuksen tasosta sekä asioista, joihin on syytä kiinnittää huomioita tulevien opintojaksojen yhteydessä.

Palautelomake täytettiin rastiruutuun periaatteella, jonka tarkoituksena oli selvittää prosentuaalisesti harjoituksen yleinen vaikeustaso. Harjoituksen vaikeuden selvittämisessä käytettiin kysymyksiä, joissa oli viisi vaihtoehtoa harjoituksen vaikeustasoksi helposta vaikeaan. Harjoitukseen liittyvien teoria-aiheiden ymmärtäminen ja harjoituksiin liittyvän kuvan ja luennon ymmärtäminen testattiin kysymyksillä, joihin vastattiin kyllä tai ei. Teoria-aiheisiin liittyvien kysymysten tarkoituksena oli selvittää oliko opiskelija ymmärtänyt

harjoituksen eri osioihin liittyvän konfiguroinnin merkityksen eli käytännössä ymmärsikö opiskelija harjoituksen loputtua mitä oli tehnyt ja minkä takia harjoitus tehtiin. Kuvaan liittyvän kysymyksen tarkoituksena oli selvittää oliko harjoituksen kuva tarpeeksi selkeä, jotta sen perusteella kytkennän tekeminen olisi mahdollista. Teoria-aiheeseen liittyvä kysymyksen tarkoituksena oli selvittää sitä, oliko MentorAid-oppimisympäristössä olevasta luennosta ollut apua harjoituksen tekemisessä.

13 Palautekyselyn arviointi

Opiskelijat vastasivat palautteisiin kiitettävästi ja vastauksia kertyi noin 40 kappaletta. Palautteet koostuivat yhdeksästä viikko harjoituksesta. Käyn seuraavaksi harjoitukset viikoittaisesti läpi ja luon katsauksen asioihin, joita palautteiden perusteella harjoituksiin tehtiin.

Viikon yksi harjoituksena oli Petri Viinikaisen opinnäytetyönään luoma kytkinharjoitus, sen aiheena oli kytkimen perusasetuksien tekeminen ja VLAN verkkojen luominen kytkimeen. Palautteiden perusteella harjoitus oli kohtuullisen helppo vastanneista 31 % perusteella, mutta 7,1 % vastanneista piti harjoitusta melko vaikeana. Harjoitukseen liittyvät teoria asiat olivat vastaajien mielestä helppo ymmärtää, yli 90 % vastaajista piti teoriaosuuksia selkeinä. Harjoituksen kuva oli opiskelijoiden mielestä selkeä yli 90 % perusteella.

Harjoituksessa oli selkeä teoriaosuuksien jako ja aihealueet eikä niiden suhteen tarvinnut tehdä muutoksia. Jaottelin harjoituksen teoria-aiheet omissa harjoituksissani eri tavalla. Käsittelin kytkimen perusasetuksia omissa harjoituksissani yksi ja kaksi sekä VLAN asetuksia harjoituksessa viisi.

Viikon kaksi harjoituksena oli Viinikaisen opinnäytetyönään luoma reititinharjoituksen ensimmäinen osa, sen aiheena olivat reitittimen perusasetukset, staattinen reititys sekä DHCP-palvelun käyttöönotto. Palautteiden perusteella harjoitus oli kohtuullisen helppo 23 % mielestä, muut vastaajat jakautuivat tasaisesti helpon ja melko vaikean välille. Harjoituksen teoria-asioiden ymmärtämisen kanssa oli ongelmia muutamissa kohdissa. RIP-protokollan konfigurointi, staattisen reitityksen tekeminen ja DHCP-palvelun käyttöönotto tuottivat ongelmia noin 15 % vastanneista.

Harjoitus oli selkeä teoriaosuuksiltaan mutta harjoituksen teoria aihe-alueet tuottivat hieman ongelmia. Harjoitus käsitteli mielestäni liian monia teoria-aiheita, joten muutin niitä hieman omiin harjoituksiini. DHCP-palvelua ja dynaamisia reittejä käsittelin harjoituksessa neljä, mutta siirsin staattisen reitityksen harjoitukseen kuusi tehtäväksi myöhemmin. Harjoituksen

teoria-aiheet olivat hieman vaikeita ymmärtää, joten siirsin DHPC-palvelua ja dynaamisia reittejä käsittelevän harjoituksen reitittimen perusasioita käsittelevän harjoituksen jälkeen.

Viikon kolme harjoituksena oli WLAN-tukiasemien ja ACS-palvelimeen liittyvä WLAN verkon konfigurointi harjoitus. Harjoitus osoittautui kohtuullisen vaikeaksi ja 24,3 % vastanneista tulkitsi sen tähän luokkaan. Kukaan ei tulkinnut harjoitusta kuitenkaan erittäin vaikeaksi ja 21,6 % piti sitä kohtuullisen helppona. Teoria-aiheista tukiaseman konfigurointi tuotti jonkun verran ongelmia, mutta ACS -palvelimen asetusten tekeminen osoittautui todella ongelmalliseksi, ainoastaan noin 60 % opiskelijoista ymmärsi palvelimen konfiguroinnin.

Harjoitus muodostui vaikeaksi suurimmaksi osaksi sen takia, että graafinen käyttöliittymä oli opiskelijoille outo ja siihen tottuminen vei aikaa. ACS-palvelimen konfigurointi oli vaikea, koska opiskelijat tekivät sen harjoituksen lopussa itsenäisesti ja assistenteilla ei ollut aikaa auttaa jokaista ryhmää vuorollaan. Omissa harjoituksissani muutin tämän harjoituksen viimeiseksi yhdeksänneksi harjoitukseksi, koska se käsitteli erillään olevaa teoria-aluetta. Harjoituksen sisältämät teoria-aiheet olivat selkeitä mielestäni, mutta harjoituksessa oli tarpeen muuttaa hieman harjoituksen tekotapaa esim. opiskelijat joutuvat kirjaamaan ylös missä kohtaa graafisessa ympäristössä käsky tehdään, jotta graafisessa ympäristössä liikkuminen jää mieleen paremmin. Toinen asia oli ACS-palvelimen konfigurointi, johon piti kiinnittää huomiota enemmän, samoin kuin WLAN-verkkojen testaamiseen harjoituksen lopussa. Nämä tehdään yhtäaikaisesti, joten harjoituksen ylläpitäjät joutuvat jakautumaan siten, että toinen ylläpitäjä ohjaa WLAN-verkkojen testausta ja toinen ACS-palvelimen konfigurointia.

Viikon neljä harjoituksena oli Viinikaisen opinnäytetyön reititinharjoituksen toinen osa, sen aiheena olivat NAT–toiminnallisuus, staattiset reitit ja OSPF–reititysprotokolla. Harjoitus oli vaikein tähän mennessä olevista harjoituksista ja 23,3 % tulkitsi sen melko vaikeaksi. Harjoituksen kaikki teoria-aiheet olivat suhteellisen vaikeita ymmärtää, eniten ongelmia tuottivat OSPF-protokollan konfigurointi ja NAT–protokollan toiminnallisuus Port Address translation, jonka omasta mielestään ymmärsi vain noin 65 % vastaajista.

Harjoitus koettiin vaikeaksi johtuen siitä, että Viinikaisen tekemä alkuperäinen harjoitus käsitteli liian monia aihe-alueita yhdessä harjoituksessa. Harjoitus jaettiin kahtia, mutta harjoituksessa oli vielä pääsylistat ja reititys samassa, joten muutin harjoituksen rakennetta hieman. Omissa harjoituksissani erottelin harjoituksen teoria-alueet toisistaan, siten että OSPF-protokollaa ja reititystä yleensä käsiteltiin harjoituksessa seitsemän ja PAT-toiminnallisuutta harjoituksessa kuusi yhdessä pääsylistoihin liittyvän teoria-aiheiden kanssa. Harjoituksien tekotapaa myös muutettiin niin, että edellisen harjoituksen konfiguraatiota käytetään seuraavassa harjoituksessa aloituskokoonpanona.

Viikon viisi harjoituksena oli Ciscon opetusmateriaalista otettu IOS-perusteiden harjoitus, joka sisälsi mm. Cisco IOS-käyttöliittymän perusasetuksien tekemistä ja Help-toimintojen käyttämistä. Harjoituksen tehneistä yllättävän suuri määri 22,7 % piti harjoitusta melko vaikeana, vaikka kyseessä oli perusteisiin liittyvä harjoitus. Aiheista ongelmallisinta oli virheiden korjausta IOS-käyttöliittymässä, jota noin 20 % vastanneista ei vastausten perusteella ymmärtänyt.

Harjoitus käsitteli yksinkertaisia asioita, mutta ongelmat johtuivat siitä, että Ciscon materiaaleista otettu harjoitus käsitteli sarjaportteja ja muita asioita, joita ei ollut mahdollista tietoliikennelaboratorion laitteille toteuttaa. Jouduimme muuttamaan viime keväänä harjoituksen monisteita ja niistä tuli tämän jälkeen epäselviä. Siirsin tämän harjoituksen teoria-aiheet omaan harjoitukseeni, joka pidetään ensimmäisenä omista harjoituksistani. Lisäksi yhdistin harjoituksen monisteet yhteen kokonaisuuteen ja tein harjoitukseen uuden topologian joka sopi tietoliikennelaboratorion laitteilla paremmin toteuttavaksi.

Viikon kuusi harjoituksena oli Ciscon materiaaleista otettu CDP-protokollan toimintaan ja tiedostojen hallintaan liittyvä harjoitus, harjoituksessa käsiteltiin myös TFTP-palvelinta. Harjoitus muodostui vastausten perusteella melko vaikeaksi, tätä mieltä olivat 21,4 % vastanneista. Teoriaosuuksista vaikeimpia olivat CDP-protokollan käyttäminen ja IOS–image tiedostoon liittyvä tietojen haku, noin ¼ osalle vastaajista asiat olivat vaikeita ymmärtää.

Harjoituksessa oli sama ongelma kuin edeltävässä harjoituksessa sarjaporttien ja epäselvien ohjeistuksien kanssa. Siirsin tämän harjoituksen toteuttavaksi toisena harjoituksenani. Omassa harjoituksessani painotan etenkin TFTP-protokollan toimintaa harjoituksen loppuvaiheessa. CDP-protokollan käsittelyn sopii mielestäni paremmin omaan reititysharjoitukseeni, joka on tarkoitus pitää kolmannella viikolla, joten erotin protokollan käsittelyn tästä harjoituksesta. Muutin tämän harjoituksen topologian myös vastaamaan paremmin tietoliikennelaboratorion laitteita.

Viikon seitsemän harjoituksena oli Ciscon materiaaliin pohjautuva harjoitus, joka sisälsi virtuaalisten lähiverkkojen tekemisen, VTP-protokollan toiminnan sekä virityspuualgoritmin toimintaperiaatteen ja testauksen tekemisen. Harjoitus koettiin melko vaikeaksi 30,2 % vastaajan perusteella ja erittäin vaikeaksi noin 10 % vastaajan perusteella. Harjoituksen teoriapohjaisten kysymysten perusteella harjoituksesta osoittautui VTP-protokollan konfigurointi ja siihen liittyvät domain määritykset ongelmallisiksi, ainoastaan hieman yli 50 % vastaajista ymmärsi protokollan konfiguroinnin omasta mielestään. Virityspuualgoritmin testaus tuotti myös ongelmia noin 30 % vastaajista.

Harjoitus käsitteli kytkimen VLAN asetuksia, VTP-protokollaa ja STP-protokollan toimintaa, jota myös testataan harjoituksessa. Kaikki teoria-aiheet liittyvät toisiinsa, joten niitä ei ollut tässä yhteydessä syytä irrottaa toisistaan. Oma viides harjoitukseni käsitteli samoja teoria-aiheita, mutta muutin hieman harjoituksen rakennetta. Lisäsin harjoitukseen myös teoriapohjaisia kysymyksiä sekä käsittelin tarkemmin omassa harjoituksessani STP-protokollan toimintaa, koska sitä käsitellään melko laajasti kurssin luennoilla.

Oma harjoitukseni sisälsi myös STP-protokollan toiminnan testaamisen käytännössä, koska se on yksi tärkeimmistä asioista opintojaksolla. Lisäsin myös omaan harjoitukseeni EThernChannelia koskevia kysymyksiä sekä RSTP ja MSTP protokollaan liittyviä kysymyksiä SPT-protokollan osalta. VTP-protokollaa käsittelin heti oman harjoitukseni alussa, lisäsin myös tähän alueeseen teoriakysymyksiä mm. VTP-pruning ominaisuudesta. VTP-protokollan ominaisuuksien selvittämiseen panostin myös enemmän, koska se oli aiheuttanut melkein puolelle opiskelijoista ongelmia. Harjoituksen konfiguraatioita oli tarkoitus käyttää myös pääsylistaharjoituksen yhteydessä hyväksi.

Viikon kahdeksan harjoituksena oli Ciscon materiaalin pohjautuva reititysprotokollien konfigurointiin liittyvä harjoitus. Harjoitus osoittautui kaikista vaikeimmaksi harjoitukseksi, harjoitus oli 38,1 % mielestä melko vaikea ja yli 10 % vastaajista piti sitä erittäin vaikeana. Harjoitus oli myös ainoa harjoitus, jota kukaan ei pitänyt helppona. Harjoitus jakautui teoriaosuuden puolesta kahteen osaan, OSPF-protokollan konfigurointi ymmärrettiin, mutta EIGRP–protokolla tuotti ongelmia. Eroavaisuus oli protokollien välillä yllättävän suuri, noin 85 % prosenttia vastaajista ymmärsi OSPF-protokollan toiminnan, mutta vain noin 60 % EIGRP-protokollan toiminnan.

Harjoitus sisälsi reitityksen kannalta kaksi tärkeintä protokollaa, jotka oli syytä pitää yhdessä. Palautteet kertoivat selvästi sen, että EIGRP-protokollan toimintaan pitää kiinnittää erityistä huomiota. Käsittelin reititykseen liittyviä asioita omassa kuudennsessa harjoituksessani. Sijoitin tämän harjoituksen pääsylistoja koskevan harjoituksen jälkeen, joka käyttää samankaltaista topologiaa. Harjoituksen rakennetta ei omasta mielestäni tarvinnut muuttaa, ainoastaan harjoituksen alku muuttui, koska harjoitus tuli käyttämään osittain edellisen harjoituksen topologiaa hyväkseen.

Uutena asiana harjoituksessa käytettävässä Core-reitittimessä kokeiltiin tässä harjoituksessa virtuaaliporttien kautta tapahtuvaa reititystä. Oma harjoitukseni sisälsi samalla tavoin protokollien testauksen siten, että OSPF protokolla testataan ensimmäisenä ja EIGRP-protokolla tämän jälkeen. Lisäsin harjoitukseen uuden teoria-alueen, joka käsittelee reititysprotokollien salausta, jota myös testataan kummankin protokollan yhteydessä.

Viimeisenä viikkoharjoituksena oli Ciscon materiaalin perustuva pääsylistoihin liittyvä harjoitus. Harjoitus käsitteli RIP-protokollaa, pääsylistojen tekemistä ja liikenteen estämistä listojen avulla. Harjoitus noudatteli muiden harjoitusten linjaa, ja 1/3 osa vastaajista piti sitä melko vaikeana. Harjoitus sisälsi eniten teoria-alueita kaikista harjoituksista, niiden ymmärtäminen jakautui tasaisesti, noin kolmannekselle vastaajista harjoitukseen liittyvät teoria-asiat olivat vaikeita ymmärtää. Vaikeimmat alueet olivat työryhmäreitittimen ja Core-reitittimien välisen yhteyden muodostamiseen liittyvät seikat.

Harjoitus käsitteli pääsylistoja sekä PAT-toiminnallisuutta. Käsittelin omassa harjoituksessa kuusi samoja asioita, mutta lisäsin harjoitukseen myös staattisten reittien tekemisen. PAT-protokolla tuotti ongelmia monille opiskelijoista aiemmassa harjoituksessa, joten muutin PAT-protokollan asetuksia hieman. Pääsylistoja tehtiin omassa harjoituksessani myös eri tavoitteilla ja niillä estettiin erilaista liikennettä ja eri tavoitteilla. Muutin myös harjoituksessa käytettävää topologiaa. Harjoituksessa käytettiin edellisen oman kytkinharjoitukseni konfiguraatiota aloituskokoonpanoja.

Kehitin edellä mainittujen harjoituksien lisäksi vielä IPv6-protollaa käsittelevän harjoituksen, joka ei liity vanhojen harjoitusten teoria-aiheisiin, koska IPv6 on otettu uutena asiana mukaan uuden CCNA-sertifikaatin suorittamiseen. Harjoitus on tarkoitus pitää kahdeksannella viikolla ennen viimeistä WLAN-asioihin keskittyvää harjoitusta.

14 Verkkoharjoitusten toteuttaminen opintojaksolle Interconnecting Networks

14.1 Verkkoharjoitusten suunnitteluprosessi

Verkkoharjoitusten suunnitteluprosessi aloitettiin vuoden 2008 huhtikuussa edellisen Interconnecting Networks opintojakson yhteydessä. Harjoitusten suunnittelu perustui Ciscon CCNA-sertifikaatin sisältämiin teoria-aiheisiin. Tarkoituksena oli suunnitella Laurean tietoliikennelaboratorioon uudet verkkoharjoitukset, joiden teoria tukisi Ciscon julkaisemien CCNA ICND 1 ja ICND 2 kirjojen vuoden 2007 painoksia. Suunnitteluprosessi koostui vanhojen verkkoharjoitusten arvioinnista, harjoituksien aihe-alueiden suunnittelusta, teoria-aiheen rajauksesta sekä vanhojen harjoitusten palautteiden suunnittelusta ja analysoinnista.

14.1.1 Harjoitusten aihe-alueiden suunnittelu

Suunnitteluprosessia jatkettiin seuraavassa vaiheessa huhtikuussa, kartoittamalla harjoituksien aihe-alueita. Harjoituksiin liittyviä aiheita kehitettiin siten, että harjoitukset kattaisivat koko opintojakson. Tämä tarkoitti noin yhdeksää kappaletta harjoituksia, jotka

kaikki käsittelisivät eri aihe-alueita. Harjoituksien suunnittelussa kiinnitettiin erityistä huomioita harjoitusten rakenteeseen, kuviin sekä harjoitusten aihe-alueiden jakoon. Harjoituksien suunnittelussa otettiin myös huomioon verkkolaboratorion resurssit.

Harjoitusten aihe-alueiksi valittiin suunnittelun päätteeksi seuraavat aihe-alueet, ensimmäiset kaksi harjoitusta käsittelivät kytkimen perusasetuksia sekä IOS-käyttöjärjestelmän perusteita ja TFTP-palvelinta. Harjoitukset kolme ja neljä käsittelivät reitittimen perusasetuksia ja DHCP-protokollan toimintaa. Varsinainen CCNA-sertifikaattia tukeva teoria-alueiden käsittely alkoi harjoituksesta viisi, jossa käsiteltiin SPT-protokollaa sekä VLAN-verkkojen tekemistä. Harjoitus kuusi käsitteli pääsylistoja sekä porttikohtaista osoitemuutosta. Harjoitus seitsemän käsitteli reititystä ja reititysprotokollien toimintaa. Harjoitus kahdeksan käsitteli IPv6-protokollan asentamista ja viimeinen harjoitus käsitteli WLAN-verkkojen luomista tukiasemien ja ACS-palvelimen avulla.

Harjoituksia saatiin suunniteltua koko opintojakson ajaksi, ensimmäisestä neljästä harjoituksesta, joku harjoitus on myös mahdollista jättää pois, mikäli käytössä on vähemmän kuin yhdeksän viikkoa harjoitusten tekemiseen. Harjoitukset käsittelivät kaikkia CCNA-sertifikaatin aihealueita poislukien WAN (Wide Area Network) -verkkoihin liittyvän harjoituksen, mikä todettiin vaikeaksi toteuttaa tietoliikennelaboratoriossa käytössä olevilla laitteilla.

14.1.2 Harjoitusten rakenteen suunnittelu

Harjoituksien rakenteen suunnittelu oli viimeinen osa suunnitteluprosessia toukokuun alussa. Harjoituksien rakenteista luotiin samankaltaisia keskenään. Kaikki harjoituslomakkeet koostuvat neljästä osa-alueesta, josta ensimmäisen muodostaa harjoitukseen liittyvä verkkokuva. Kuvasta selviää harjoituksen toiminta, käytettävät laitteet sekä tarvittavat kytkennät ryhmäkohtaisesti. Toinen osa-alue koostuu harjoituksen ohjeistuksesta, joka pitää sisällään harjoituksen lähtötilanteen kuvauksen, ryhmäkokoonpanon, harjoituksen teoreettiset aihe-alueet sekä tarvittavat toimenpiteet harjoituksen vastuuhenkilöltä. Harjoituksen kolmas osa koostuu harjoituksen käskylistasta sekä itse harjoituksesta. Harjoituksen tekeminen etenee kohta kohdalta vaiheittaisesti, jossa suoritetaan, joko kohtaan liittyvä toimenpide Cisco IOS-käyttöjärjestelmässä tai vaihtoehtoisesti vastataan kohdassa esitettyyn teoria kysymykseen. Harjoituksen viimeinen osa sisältää harjoituksen aihe-alueisiin liittyvien kertauskysymyksiin vastaamisen. Kysymykset koostuvat monivalintakysymyksistä, joista yksi tai useampi vastaus voi olla oikein. Harjoituslomakkeisiin liitetään myös viimeiseksi osaksi oikeat vastaukset kaikkiin kysymyksiin, tämä paperi luovutetaan harjoituksesta vastaavalla henkilölle.

14.1.3 Palautekyselyn suunnittelu

Harjoituksen suunnitteluprosessia jatkettiin huhtikuussa palautekyselyn suunnittelulla. Palautekysely päätettiin tehdä, jotta opintojakson opiskelijoilta saataisiin palautetta harjoitusten sisällöstä. Saatua palautetta käytettiin kyselyn jälkeen hyväksi uusien harjoitusten sisällön suunnittelussa. Palautelomakkeissa kiinnitettiin huomioita muutamaan erityiseen osa-alueeseen, joita olivat yleinen vaikeustaso, teoriapainotukset sekä opintojakson teoria-aiheita vastaavat luentopaketit verkossa.

14.1.4 Vanhojen verkkoharjoitusten arviointi

Suunnitteluprosessin ensimmäinen vaihe koostui tietoliikennelaboratorion verkkoharjoitusten arvioinnista. Tutkimuksen yhteydessä huomattiin, että vanhat harjoitukset oli rakennettu eri tarkoitusta varten eivätkä ne käsitelleet kaikkia CCNA-sertifikaatin aihe-alueita. Verkkopuolen opiskelu uudistuksen myötä CCNA-sertifikaattia tukevaa koulutusta annettiin vuoden 2007 syksystä alkaen tietoliikennelaboratorion laitteilla ulkopuolisen kouluttajan sijasta. Tämä muutos oli osaltaan vaikuttamassa siihen, että tietoliikennelaboratoriossa tuli tarve uusien harjoituksien tekemiselle. Suunnittelun tavoitteena oli kehittää harjoitukset tukemaan CCNA-sertifikaatin suorittamista siten, että mahdollisimman moni kirjoissa käsitellyistä asioista voitaisiin testata tietoliikennelaboratorion laitteilla.

14.2 Verkkoharjoitusten toteutusprosessi

Opinnäytetyön toteutusprosessi aloitettiin toukokuussa palautteiden analysoinnin jälkeen. Opinnäytetyön toteuttamisprosessiin kuului harjoitusten rakentaminen ja testaus sekä opinnäytetyöhön liittyvä kirjoitusosuuden tekeminen. Toteutusprosessi vei suurimman osan opinnäytetyöhön kulutetusta ajasta, toukokuun alusta lokakuun loppuun.

14.2.1 Työhön liittyvä kirjoitusosuus

Työn kirjoitusosuuden teko alkoi heinäkuun lopulla harjoituslomakkeiden rakentamisen jälkeen. Kirjoitusprosessia jatkettiin yhtäaikaisesti harjoituksien testaamisen yhteydessä aina marraskuuhun saakka, jolloin kirjoitettiin opinnäytetyöhön liittyvää analysointia. Kirjoitusprosessin myötä opinnäytetyö sai nykyisen rakenteensa, joka koostui kuudesta osa-alueesta. Ensimmäinen osa sisältää lähtötilanteen kuvauksen sekä kohdeympäristön esittelyn, toisessa käsitellään harjoituksiin liittyviä teoria-aiheita, kolmannessa käydään läpi työn teko vaiheet, neljäs osa esittelee tehdyt harjoitukset ja viimeinen osa sisältää työhön liittyvää analysointia ja arviointia.

14.2.2 Harjoitusten rakentaminen ja testaus

Harjoituslomakkeiden valmistus koostui harjoitusten tehtävien ja kysymysten tekemisestä kuvien piirtämisestä, käskylistojen tekemisestä sekä kertauskysymysten ja oikeiden vastauksien tekemisestä. Harjoituslomakkeita tehtiin yhdeksän kappaletta yksi jokaista harjoitusta varten. Harjoituksien tekemiseen käytettiin aikaa noin kolme kuukautta toukokuusta–heinäkuuhun. Harjoituksien toimivuutta ei varsinaisesti testattu toteutusprosessin aikana vaan vasta testauksen yhteydessä myöhemmin. Testausprosessi aloitettiin harjoituslomakkeiden rakentamisen jälkeen elokuun lopussa. Testausprosessissa kaikki yhdeksän harjoitusta rakennettiin tietoliikennelaboratorioon laitteille tietoliikennelaboratorio assistentin avustuksella.

Harjoitukset testattiin kohta kohdalta läpi ja niihin tehtiin muutoksia tarvittaessa. Osasta harjoituksista ilmeni ongelmia, jotka koskivat harjoituksien järjestystä sekä harjoituksien yleistä toimimattomuutta. Osaa harjoituksista muutettiin testausvaiheessa, esimerkiksi harjoituksessa kuusi muutettiin PAT-toiminnon muotoa sekä pääsylistojen kieltomäärityksiä, jotta harjoituksen tekeminen onnistuisi. Teoriakohtia myös tarkennettiin ja niiden läpikäynti ja järjestystä muutettiin osissa harjoituksista.

14.3 Verkkoharjoitusten arviointiprosessi

Verkkoharjoitusten arviointia tehtiin marraskuussa 2008. Verkkoharjoitusten arviointiprosessissa otettiin huomiooon harjoitusten yleinen taso sekä harjoitusten aihe-alueet. Arviointiprosessissa painotettiin harjoitusten teoreettista sisältöä, harjoitusten rakennetta sekä loogisuutta ja yleistä selkeyttä sekä ohjeistuksia. Harjoitusten arviointiin kuului lisäksi yhden valmiin verkkoharjoituksen testaus tietoliikennelaboratoriossa sekä sen onnistumisen arviointi syksyn Interconnecting Networks-opintojaksolla marraskuussa.

14.4 STP-protokollaa käsittelevän harjoituksen arviointi ja testaus

Viidennettä viikkoharjoitusta testattiin tietoliikennelaboratoriossa 6.11.2008 opintojakson Interconnecting networks yhteydessä yhtenä opiskelijoiden verkkoharjoituksena. Harjoituksen kaksi tärkeintä aihepiiriä olivat VLAN-asetusten tekeminen sekä SPT-protokollan konfiguroiminen ja sen testaus. Harjoitusta kävi tekemässä 12 oppilasta ryhmäkoon vaihdellessa yhdestä kolmeen henkilöön. Harjoituksen alussa opiskelijaryhmät rakensivat kuvan mukaisen topologian tietoliikennelaboratorioon. Laitetopologian rakentaminen ei aiheuttanut suuria ongelmia, kun harjoituksien vetäjät olivat kertoneet laitteiden roolit harjoituksessa. Opiskelijat suoriutuivat todella hyvin laitteiden kytkennästä, vaikka kyseessä

oli osalla opiskelijoista ensimmäinen kytkentä kerta. Tietoliikennelaboratoriossa harjoituksen vetäjinä toimivat kaksi assistenttia itse toimin tämän harjoituksen osalta heidän kanssaan, tarkoituksenani oli tarkkailla harjoituksen suorittamista ja arvioida sitä.

Topologian rakentamisen jälkeen opiskelijat aloittivat harjoituksen teon ensimmäisestä osasta, jossa peruskonfiguraatiot luotiin kytkimeen ja reitittimeen SETUP-toiminnon avulla. Ainoa ongelma ensimmäisessä vaiheessa oli reitittimien salasanojen määritys, joka ei mahdollistanut saman salasanan käyttöä kahteen kertaan.

Toisessa vaiheessa opiskelijat hakivat VTP-protokollaan liittyviä tietoja kytkimestä. Opiskelijaryhmät löysivät kaikki halutut tiedot ilman ongelmia ja ymmärsivät miten VTP-protokolla mainostaa VLAN-tietoja verkossa. VTP-pruning-ominaisuuden toimiminen aiheutti muutaman ryhmän osalta kyselyjä. Neuvoimme ryhmäläisiä kuuntelemaan STP-protokollan liittyvän teoria osuuden verkosta.

Kolmannessa vaiheessa opiskelijat määrittivät kytkimelle Trunk-portti asetukset ja enkapsulointi muodon sekä tutkivat Trunk-porttien VLAN-kohtaisia asetuksia. Tässä vaiheessa harjoitusta huomasin muutaman käskylistassa olevan käskyn, jotka eivät toimineet tietoliikennelaboratorion kytkimien IOS-versiossa, joten poistin käskyt harjoituksen käskylistalta.

Harjoituksen neljännessä vaiheessa opiskelijat tekivät VLAN-määritykset kytkimille sekä määrittivät oletusreitin ja oletusyhdyskäytävän laitteilta Core-reitittimelle. Huomasin että opiskelijoiden VLAN tiedot puuttuivat harjoituksen kuvasta, lisäsin ne sinne harjoituksen jälkeen.

Harjoituksen viides vaihe sisälsi STP-protokollan testauksen. Odotin tästä osuudesta harjoituksen vaikeinta, koska se oli aiheuttanut ongelmia testausvaiheessa. Tämä vaihe onnistui opiskelijaryhmiltä todella hyvin, kaikki opiskelijaryhmät onnistuivat tekemään testausvaiheen kokonaisuudessaan. Muutin tässä kohtaa harjotusta yhden Ping-komentoon liittyvän testauksen myöhemmäksi, koska se vaikutti harjoituksen toimintaan.

Harjoituksen kuudennessa vaiheessa laitteiden ajonaikainen konfigurointi kopioitiin TFTP-palvelimelle. Huomasin kopioinnissa sen, että VLAN-asetusten poistamisen jälkeen yhteyttä TFTP-palvelimelle ei saatu enää reitittimestä käsin. Muutin tästä johtuen VLAN:ien poistamisen harjoituksen viimeiseksi osaksi.

Harjoitus sujui kokonaisuudessaan hyvin kaikilta opiskelijoilta. Harjoituksen tekemiseen kului aikaa noin puolestatoista tunnista kolmeen tuntiin. Huomasin myös sen, että ryhmän koolla on

vaikutusta harjoitukseen tekemiseen hidastavasti. Yksin tekevä henkilö teki harjoituksen nopeimpien parien kanssa samaa vauhtia, mutta ainoa kolmen hengen ryhmä käytti harjoituksen tekemiseen eniten aikaa, melkein kolme tuntia.

Suurin ongelma harjoituksen yhteydessä liittyi silmukkaan, joka syntyi laitteiden välillä ja hidasti VLAN:in sisäistä liikennettä väliaikaisesti. Silmukka aiheutui työryhmäkytkimien ja työryhmäreitittimien välissä, Trunk-porttiin liittyvän konfiguroinnin yhteydessä. Silmukan syntymistä ei saatu selville, mutta päädyimme siihen tulokseen, että paketti tuli tietoliikennelaboratorion ulkopuolelta. Silmukka saatiin pysähtymään katkaisemalla työryhmäkytkimen ja Core-kytkimien välinen Trunk-yhteys. Silmukkaa ei syntynyt enää uudestaan vaikka sama tilanne kytkettiin uudelleen harjoituksen myöhemmässä vaiheessa.

14.5 Verkkoharjoitusten suunnittelun arviointi

Työn arvioinnissa on kiinnitetty huomioita moniin yksittäisiin asioihin työn eri vaiheissa. Arvionnissa käsitellään harjoitusten suunnittelua, tekemistä, niiden sisältöä ja selkeyttä sekä harjoitusten onnistumista tavoitteiden kannalta. Arviointia tehdään myös koko työn raportoinnin ja selkeyden perusteella sekä arvioidaan lisäksi työprosessia yleisesti: mitä olisi voitu tehdä toisin tai eri järjestyksessä? Arvioinnissa pohditaan myös sitä, tuottiko työ tarpeellista hyötyä tietoliikennelaboratorioon.

Harjoitusten suunnittelu sujui hyvin aihe-alueiden jaon osalta ja lopulliset harjoitukset sisälsivät suunnitellut teoria osa-alueet. Sain rajattua harjoituksissa käytettävän teoria-alueen kohtuullisesti, vaikka teoria-alue oli melko laaja. Aiempien harjoitusten palautekyselyn osalta jäi parantamisen varaa, etenkin palautekyselyn suunnittelun osalta. Palautekyselylomakkeen suunnitteluun olisin voinut käyttää enemmän aikaa, jolloin palautteiden analysointi olisi ollut helpompaa. Palautekyselyssä käytetystä lomakkeesta tuli hieman liian laaja opiskelijoiden oli vaikeaa muistaa kaikkien tehtyjen harjoituksien sisältöä ja niiden käsittelemiä teoria-aiheita, vaikka vanhat harjoitukset olivat käytettävissä palautekyselyn yhteydessä. Omasta mielestäni sain palautekyselyn ansioista riittävästi tarpeellista tietoa aihe-alueista, jotka vaativat lisää painotusta omissa harjoituksissani.

Päädyin työn suunnitteluvaihessa harjoitusten rakentamiseen ennen kirjoitustyön tekemistä. Omasta mielestäni onnistuin tässä hyvin, vaikka työprosessia olisi voinut jakaa myös eri tavalla, esimerkiksi harjoitusten yhtäaikaiseen tekemiseen ja raportointiin. Harjoitusten sisältö noudatteli mielestäni tarkasti sitä kaavaa, jonka olin suunnitellut etukäteen ja ne koostuivat CCNA-sertifikaatin suorittamisen kannalta tarpeellisista aihe-alueista. Lopullisista harjoituksista jätin pois suunnitellun teoriaosuuden, jossa oli tarkoitus kuvata käytännön tilanne, missä kyseistä harjoitusta voitaisiin käyttää todellisuudessa hyväksi.

Harjoituksista tuli omasta mielestäni opiskelijoiden kannalta riittävän selkeitä, jotta he pystyvät suoriutumaan niistä ja lisäksi ymmärtämään harjoitusten käsittelemät aiheet. Harjoituksista kiitettävästi suoriutuminen vaatii opiskelijoilta opintojaksolla käsiteltävien teorialuentojen kuuntelemisen ennen harjoituksien tekemistä, jotta teoriapohjaisiin kysymyksiin olisi mahdollista vastata. Harjoituksissa käsiteltävät aiheet jaoin aihe-alueittain, jolloin yhtä aihetta käsitellään aina yhdessä kappaleessa. Näin opiskelijat voivat keskittyä yhteen aihe-alueeseen kerrallaan. Lisäsin harjoituksien aihe-alueita käsittelevän Exel-taulun Optimaan, jotta opiskelijat voivat tarkastaa, mitä aiheita harjoituksissa käsitellään viikottain. Parannettavaa harjoituksien rakenteeseen myös jäi, esimerkiksi teoriaiheiden käsittely osana harjoitusta ei välttämättä edistä harjoituksen tekemistä, vaan niiden käsittelyn olisin voinut myös siirtää harjoituksen loppuun. Päädyin kuitenkin siihen, että teoriakysymyksiä on parempi käsitellä samalla, kun itse aihetta käsitellään ja tehdään harjoituksessa.

Harjoituksien tekeminen onnistui kokonaisuudessaan hyvin ja ne vastasivat asetettuja tavoitteita aihe-alueiden osalta. Harjoituksien vaikeustaso asettui melko korkeaksi, mutta se kuului osaltaan myös työn tavoitteisiin. Harjoituksen testauksen yhteydessä kiinnitin erityistä huomioita siihen, miten opiskelijat suoriutuivat harjoituksen tekemisestä. Mielestäni opiskelijat suoriutuivat harjoituksesta kokonaisuudessaan hyvin. Ainoastaan teoria-osuuteen liityvissä kysymyksissä oli osalla opiskelijoilla ongelmia, koska he eivät olleet tutustuneet ennalta harjoitukseen liittyvään luentoon. Opiskelijoiden yleinen osaamistaso ja motivaatio tehdä harjoituksia vaikuttivat mielestäni todella hyvältä syksyn opiskelijoiden osalta.

Verkkoharjoitukset 5-9 toteutettiin Laurean tietoliikennelaboratoriossa syksyn Information Networks-toteutuksella testausmielessä uusien tietoliikennelaboratorioassistenttien toimesta, jolloin harjoituksissa ilmenneitä virheitä voitiin vielä korjata. Erityisesti testattiin harjoitusta viisi, jossa olin itse myös mukana ohjaamassa harjoitusta. Muiden harjoitusten osalta harjoittelijat raportoivat ilmenneistä ongelmista ja kohdista, joita oli tarvetta muuttaa.

Mikään yksittäinen harjoitus ei aiheuttanut ylitsepääsemättömiä ongelmia. Vaikeimmaksi harjoitukseksi läpikäydyistä harjoituksista nousi reititysprotokolliin liityvä harjoitus ja sen yhteydessä tehtävä reitityksen konfigurointi, joka vei opiskelijoilta paljon aikaa, minkä johdosta muutama opiskelijaryhmä ei saanut harjoitusta valmiiksi lasketussa ajassa.

Ohjaajien mukaan yksittäisista teoria-aiheista vaikeimpana, tehtyjen harjoitusten perusteella, opiskelijat kokivat reititykseen liittyvän harjoituksen. Aihepiiriin liittyvää harjoitusta pidettiin etenkin EIGRP-protokollan suhteen vaikeimpana harjoituksena myös viime keväänä. Tämä johtuu mielestäni siitä että, reititysprotokollien konfiguroiminen vaatii

laajaa teorian ymmärtämistä. Tästä johtuen muutin viime kevään harjoitusta lisäämällä teoriaan liittyviä kysymyksiä, jotta opiskelijat ymmärtäisivät paremmin miten reititysprotokollat toimivat käytännössä. Käsittelin omassa harjoituksessa myös kokonaan uutta aihe-aluetta, joka liittyi protokollien salauksen tekemiseen, jotta ongelmallista EIGRP-protokollaa käsiteltäisiin enemmän kuin aiemmissa harjoitusta oli tehty.

Suurimpia ongelmia harjoituksissa aiheuttivat topologian rakentaminen varsinkin harjoituksessa viisi, jossa se tehtiin ensimmäistä kertaa. Tietoliikennelaboratorion käytössä olevat laitteet on syytä esitellä opiskelijoille jo aiemmissa harjoituksissa, jotta kytkentä viidennessä harjoituksessa onnistuu. Tähän on tulevien ohjaajien syytä kiinnittää huomiota jatkossa. Muita ongelmia aiheuttivat harjoituksiin käytettävä aika, joka vaihteli todella paljon harjoitusten välillä, helpoimmat harjoitukset veivät opiskelijoilta vajaan tunnin ja pisimmät joidenkin ryhmien kohdalla jopa yli kolme tuntia. Kaikki harjoitukset on kuitenkin tarkoitus pitää tämän hetkisissä muodoissaan ja jättää ohjaajien vastuulle se, että opiskelijaryhmät saavat ohjeistusta, jos harjoituksen teko ei syystä tai toisesta etene.

Muita pienempiä ongelmia harjoituksissa aiheuttivat teoria-aiheisiin liittyvät kysymykset, joihin vastaaminen aiheutti osalla opiskelijoista vaikeuksia. Harjoitukset suunniteltiin tarkoituksella melko haastaviksi ja niissä esitettyihin kysymyksiin vastaaminen vaatii harjoituksiin liittyvien teorialuentojen etukäteen kuuntelemista. Tästä syystä Optimaan lisättiin aihelista, mistä on mahdollista selvittää harjoitusten käsittelemät aihe-alueet etukäteen. Opiskelijoille on muistutettava tästä asiasta jatkossa ennen harjoitusten tekoa, koska teorialuentojen kuuntelu on tärkeää harjoitusten ja opintojakson suorittamisen kannalta.

Työn raportista tuli melko pitkä työhön liittyvän teoriaosuuden laajuuden vuoksi. Raportti käsitteli alussa tarkasti läpi kaikki CCNA-sertifikaatin liittyvät aihe-alueet, jotka oli tarpeellista tehdä tarvittavan teoriatiedon saamiseksi. Harjoituksen seuraavassa vaiheessa kävin harjoitukset osa-alueittain läpi. Tarkoitukseni oli tehdä harjoituksien käsittely melko tarkasti, jotta työn raportoinnista on mahdollista nähdä tarvittaessa, mitä aiheita harjoituksen tietty osa sisältää.

Raportoinnin loppuvaiheessa käsittelin itse opinnäytetyön tekoprosessia ja sen onnistumista tavoitteiden kannalta. Omasta mielestäni tämä jako on selkeä ja ymmärrettävä lukijan kannalta. Raportoinnin pituutta olisin voinut lyhentää jättämällä alkuosan teoria-aiheiden käsittelystä verkkoteorian käsittelyn tai kaapeloinnin käsittelyn pois. Muiden aihe-alueiden suhteen omasta mielestäni työtä ei voi tiivistää enempää.

Kokonaisuudessa työn onnistumisen kannalta tavoitteisiin voitaisiin myös päästä monella eri tavalla. Työssä olisi voitu esimerkiksi keskittyä ainoastaan tietyn aihe-alueen käsittelyyn yksittäisessä harjoituksessa tai tehdä yksi iso harjoitus joka käsittelee kaikkia aihe-alueita. Oma tapani oli sekoitus näitä molempia, ensimmäiset neljä harjoitusta muodostivat omat kokonaisuudet ja sen jälkeen harjoitukset viidestä eteenpäin muodostivat jatkumon, jolloin harjoituksien lopputilan konfiguraatiota käytettiin seuraavassa harjoituksessa hyväksi aloituskokoonpanona.

15 Päätelmät

Opinnäytetyön tavoitteena oli kehittää Laurean tietoliikennelaboratoriota kehittämällä uusia verkkoharjoituksia opiskelijoiden käyttöön. Harjoituksien oli tarkoitus käsittää Ciscon ICND-kirjojen sisältämiä aihe-alueita. Opiskelijoilta tiedusteltiin mielipiteitä vanhojen harjoitusten hyvistä ja huonoista puolista palautekyselyn muodossa. Palautekyselyn perusteella saatava tieto käytettiin hyödyksi uusien harjoituksien suunnittelussa. Uusien harjoituksien lähtökohtana oli se, että opiskelijat pystyvät MentorAid-järjestelmässä olevien verkkoteorialuentojen ja demojen sekä tietoliikennelaboratoriossa käytännön harjoituksien konfiguroinnin jälkeen hallitsemaan ne aihe-alueet, jotka kuuluvat Ciscon CCNA-sertifikaattin suorittamiseen vuonna 2008.

Opinnäytetyö sisälsi yhdeksän verkkoharjoitusta, jotka käsittelivät CCNA-sertifikaatin aihe-alueita. Neljä ensimmäistä harjoitusta käsittelivät perusverkkoteoriaa ja toimivat opastavina harjoituksina kytkimen ja reitittimen Cisco IOS-käyttöliittymään tutustumisessa. Harjoitukset viidestä eteenpäin käsittelivät vaativimpia aihe-alueita kuten VLAN-verkkojen konfigurointia, STP-toimintaa, reititysprotokollien konfigurointia, pääsylistoilla tehtävää liikenteen rajoittamista sekä IPv6-osoitteita ja konfigurointia. Viimeinen harjoitus käsitteli omaa kokonaisuuttaan WLAN-verkkojen konfigurointia.

Opinnäytetyön ansioista tietoliikennelaboratorio sai käyttöönsä uudet verkkoharjoitukset, joita voidaan käyttää tulevilla opintojaksoilla. Perustason harjoitukset sopivat käytettäväksi ensimmäisen vuoden verkko-opetuksen peruskursseilla, joilla opiskellaan Cisco IOS-käyttöjärjestelmän toimintaa ja verkkoteorian perusteita. Toisen vuoden ja sitä vanhemmat opiskelijat, jotka erikoistuvat verkko-puolen opiskeluun voivat tehdä vaikeimpia harjoituksia, osana CCNA–sertifikaattiin liittyvien teorialuentojen kanssa.

Tulevaisuus kertoo enemmän siitä, miten hyödyllinen työni on tietoliikennelaboratoriossa jatkossa. Oma tavoitteeni on se, että harjoituksia käytetään laboratoriossa hyödyksi tulevina vuosina ja että niillä tullaan korvaamaan kaikki samoja aiheita käsittelevät vanhat

harjoitukset. Harjoituksia on mahdollista myös jatkokehittää ja muuttaa tulevaisuudessa edelleen, jos tarve niin vaatii. Harjoituksia voidaan myös tehdä tulevaisuudessa uusilla Ciscon IOS-käyttöjärjestelmän sisältävillä verkkolaitteilla. Harjoitukset dokumentoidaan tietoliikennelaboratorioon jatkokäyttöä varten paperimuotoon sekä sähköiseen muotoon, jossa niitä voidaan käyttää jatkossa vapaasti erilaisissa projekteissa ja opintojaksoilla sekä tulevien harjoitusten kehittämisen yhteydessä.

Harjoitusten tekeminen oli vaativaa, mutta myös samalla mielenkiintoista ja antoisaa aikaa. Käytin opinnäytetyön tekemiseen kokonaisuudessaan noin kahdeksan kuukautta, joka jakautui kahteen osaan. Ensimmäisessä suunnittelin harjoitukset sekä toteutin ne. Toisessa osassa testasin harjoituksia käytännössä, korjasin virheitä sekä valmistin opinnäytetyön raporttia. Hankkimastani taidoista aluksi tietoliikennelaboratorion harjoittelijana ja harjoitusten vetäjänä ja sen jälkeen opinnäytetyön yhteydessä harjoitusten suunnittelun, toteutuksen verkkolaiteiden konfiguroinnin sekä dokumentoinnin tekemisestä ja kaiken teoriatiedon saamisesta on melko varmasti hyötyä tulevaisuudessa töitä hakiessani.

LÄHTEET

Kirjallisuus

Chappel, L. 1999. Cisco reitittimet. Jyväskylä: IT Press.

Cisco Systems 2007a. CCENT/CCNA ICND1. Indianapolis (IN): Cisco Press.

Cisco Systems 2007b. CCENT/CCNA ICND2. Indianapolis (IN): Cisco Press.

Cisco Systems. 2002. Cisco Verkkoakatemia. Helsinki. Edita Prima Oy.

Geier, J.2005 Langattomat verkot perusteet. Helsinki: Edita Prima Oy.

Hakala, M & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: WS Bookwell.

Jaakohuhta, H. 2002. Lähiverkot Ethernet. Helsinki. Edita Prima Oy.

Järvinen, P & Järvinen, A. 2000. Tutkimustyön metodeista. Tampereen Yliopistopaino Oy.

Kaario, K. 2002. TCP/IP -verkot. Porvoo: WS Bookwell.

Opetusasianhallinto. 2007. Laurea Fakta. Helsinki. Edita Oyj.

Elektroniset lähteet

Cisco Systems. 2008a. Cisco Secure Access Control Server 4.2 for Windows: Data Sheet. Viitattu 29.9.2008.
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/data_sheet_c78-453387.html

Cisco Systems. 2008b. Configuring a Terminal/Comm Server. Viitattu 24.9.2008.
http://www.cisco.com/en/US/tech/tk801/tk36/technologies_configuration_example09186a008014f8e7.shtml

Internet Engineering Task Force. 1981a. RFC 790 Assigned numbers. Viitattu 12.11.2008.
http://www.faqs.org/rfcs/rfc790.html

Internet Engineering Task Force. 1981b. RFC 791 Internet Protocol. Viitattu 12.11.2008.
http://tools.ietf.org/html/rfc791

Internet Engineering Task Force. 1981c. RFC 792 Internet Control Message Protocol. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc792

Internet Engineering Task Force. 1982. RFC 826 An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses. Viitattu 13.11.2008.
http://tools.ietf.org/html/rfc826

Internet Engineering Task Force. 1984. RFC 920 Domain Requirements. Viitattu 13.11.2008.
http://tools.ietf.org/html/rfc920

Internet Engineering Task Force. 1988. RFC 1058 Routing Information Protocol. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc1058

Internet Engineering Task Force. 1989. RFC 1122 Requirements for Internet Hosts. Viitattu 12.11.2008. http://tools.ietf.org/html/rfc1122

Internet Engineering Task Force. 1993. RFC 1518 An Architech for IP Address Allocation with CIDR. Viitattu 12.11.2008. http://tools.ietf.org/html/rfc1518

Internet Engineering Task Force. 1997a. RFC 2082 RIP-2 MD5 Authentication. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc2082

Internet Engineering Task Force. 1997b. RFC 2131 Dynamic Host Configuration Protocol. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc2131

Internet Engineering Task Force. 1998a. RFC 2328 OSPF Version 2. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc2328

Internet Engineering Task Force. 1998b. RFC 2460 Internet Protocol, Version 6 IPv6 Specification. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc2460

Internet Engineering Task Force. 1999a. Part 11:Wireless LAN Medium Access Control MAC and Physical Layer PHY Specifications High-speed Physical Layer in the 5GHz Band. Viitattu 12.11.2008. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

Internet Engineering Task Force. 1999b. Part 11:Wireless LAN Medium Access Control MAC and Physical Layer PHY Specifications Higher-Speed Physical Layer Extension in the 2.4GHz Band. Viitattu 12.11.2008. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

Internet Engineering Task Force. 2001. RFC 3022 The IP Network Address Translator NAT. Viitattu 13.11.2008. http://tools.ietf.org/html/rfc3022

Internet Engineering Task Force. 2003. Part 11: Wireless LAN Medium Access Control MAC and Physical Layer PHY Specifications Amendment4: Further Higher Data Rate Extension in the 2.4 GHz Band. Luettu 12.11.2008. http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

Internet Engineering Task Force. 2004. IEEE Standard for Local and Metropolitan Area Networks: Media Access Control MAC Bridges. Viitattu 13.11.2008. http://standards.ieee.org/getieee802/download/802.1D-2004.pdf

Internet Engineering Task Force. 2005a. Part 3: Carrier Sense Multiple Access with Collision Detection CSMA/CD Access Method and Physical Layer Specifications. Viitattu 12.11.2008. http://standards.ieee.org/getieee802/download/802.3-2005_section1.pdf

Internet Engineering Task Force. 2005b. Part 3: Carrier Sense Multiple Access with Collision Detection CSMA/CD Access Method and Physical Layer Specifications. Viitattu 12.11.2008. http://standards.ieee.org/getieee802/download/802.3-2005_section2.pdf

Internet Engineering Task Force. 2005c. Part 3: Carrier Sense Multiple Access with Collision Detection CSMA/CD Access Method and Physical Layer Specifications. Viitattu 12.11.2008. http://standards.ieee.org/getieee802/download/802.3-2005_section3.pdf

Internet Engineering Task Force. 2007. Part 11: Wireless LAN Medium Access Control MAC and Physical Layer PHY Specifications. Viitattu 12.11.2008. http://standards.ieee.org/getieee802/download/802.11-2007.pdf

Internet Engineering Task Force. 2008. Operating Rules of IEEE Project 802 Working group 802.3, CSMA/CD LANs. Viitattu 12.11.2008. http://www.ieee802.org/3/rules/P802_3_rules.pdf

International Standards Organization. 2008. Freely available standards. ISO/IEC 7498-1. Viitattu 12.11.2008. http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip

Laurea-ammattikorkeakoulu. 2008. Tietoa Laureasta: Esittely. Viitattu 7.8.2008. http://www.laurea.fi/internet/fi/03_tietoa_laureasta/01/01_Esittely/index.jsp

Sollins, K. 1992. RFC1350: The TFTP Protocol (Revision 2). Viitattu 3.10.2008. http://www.faqs.org/rfcs/rfc1350.html

LIITTEET

KUVAT

KUVIOT

Liite 1 Palautelomakekyselyn pohja

Interconnecting networks course feedback (LAB exams) 1/7

1=easy 4=pretty hard
2=pretty easy 5=very hard
3=appropriate

	Weekly subject:	Exam overall difficulty: 1 2 3 4 5	Did i understand exam theory parts? YES NO	picture? YES NO
week 1	**Switch basic configurations and VLANS**			
1	How to list switch configuration changes from running and startup configuration ?			
2	How to configure switch ports to use specific VLAN?			
3	How to configure switch port to trunk port mode?			
week 3	**Wlan access point practise**	1 2 3 4 5	theory parts? YES NO	picture? YES NO
1	How to configure switch ports to use specific Wlan?			
2	How to configure Access point?			
3	How to configure ACS server?			
4	How to configure Wlan settings to your computer?			

Interconnecting networks course feedback (LAB exams) 2/7

1=easy 4=pretty hard
2=pretty easy 5=very hard
3=appropriate

	Weekly subject:	**Exam overall difficulty:** 1 2 3 4 5	**Did i understand exam theory parts?** YES NO	**picture?** YES NO
week 2	**Router basic configurations**			
1	How to show router configuration changes from running and startup config?			
2	How to configure dynamic routing with RIP?			
3	How to configure static routing?			
4	How to configure DHCP service?			
week 4	**Router basic configurations and making static and dynamic routing**	1 2 3 4 5	**theory parts?** YES NO	**picture?** YES NO
1	How to configure dynamic routing with OSPF?			
2	How to deny traffic with ACL?			
3	What is meaning of Network address translation ?			
4	How to configure NAT using Port Address Translation?			

Interconnecting networks course feedback (ICND exams) 3/7

1=easy 4=pretty hard
2=pretty easy 5=very hard
3=appropriate

	Weekly subject:	Exam overall difficulty: 1 2 3 4 5	Did i understand exam theory parts? YES NO	picture? YES NO
week 5	**CLI and IOS basics (router)**			
1	How to use IOS help functions ?			
2	How to edit incorrect commands?			
3	How to examine router status using show commands?			
week 6	**Gathering information about neighboring devices and using system files (router and switch)**	1 2 3 4 5	theory parts? YES NO	picture? YES NO
1	How to use cdp command to discover local workgroup network from switch and router?			
2	How to use telnet and take connections between switch and router?			
3	How to find information about IOS image file and where it is stored?			
4	What is TFTP server?			
5	How to copy configuration files to TFTP server or vice versa?			

Interconnecting networks course feedback (ICND exams) 4/7

1=easy 4=pretty hard
2=pretty easy 5=very hard
3=appropriate

	Weekly subject:	Exam overall difficulty: 1 2 3 4 5	Did i understand exam: theory parts? YES NO	picture? YES NO
week 7	**Configuring a switch for extended functionality (switch)**			
1	How to configure VTP domain on a switch?			
2	How to assign a switch to the approriate VTP mode?			
3	How to configure seperate VLANs on a switch?			
4	How to Configure and monitor Spanning Tree protocol?			
week 8	**Determining IP Routes with EIGRP (router)**	1 2 3 4 5	theory parts? YES NO	picture? YES NO
1	How to enable routing with EIGRP?			
2	How to verify routing with EIGRP?			
3	How to debug routing with EIGRP?			
	Determining IP Routes with OSPF (router)			
1	How to enable routing with OSPF?			
2	How to verify OSPF routing?			
3	How to debug routing with OSPF?			

Interconnecting networks course feedback (ICND exams) 5/7

1=easy 4=pretty hard
2=pretty easy 5=very hard
3=appropriate

	Weekly subject:	Exam overall difficulty: 1 2 3 4 5	Did i understand exam theory parts? YES NO	picture? YES NO
week 9	**Determining IP routes with RIP (router)**			
1	How to set up lan connections from a WG router to a core site?			
2	How to enable fast ethernet connections from a WG router to a core site?			
3	How to enable and verify routing with RIP?			
	Configuring IP ACLs (router)	1 2 3 4 5	YES NO	
1	How to create IP ACL to block traffic?			
2	How to create IP ACL to block TFTP traffic?			
3	How to remove ACLs from interfaces?			
	Configuring PAT (router and switch)	1 2 3 4 5	YES NO	
1	How to configure Port address translation?			
2	How to verify PAT using show commands?			

Interconnecting networks course feedback (ICND exams) 6/7

1=easy 4 pretty hard
2=pretty easy 5=very hard
3=appropriate

	Weekly subject:	**Exam overall difficulty:** 1 2 3 4 5	**Did i understand repeating subjects?** YES NO	**picture?** YES NO
week 10	**Repeatition exam**			
1	Repeating switch configuration			
2	Repeating router configuration			
3	Repeating VLANs configuration			
4	Repeating ACLs configuration			
5	Troubleshooting switch and router installations			

Mentor AID Lectures

Did i find weekly topics theory information at MentorAid lectures 7/7

		YES	NO
week11	CLI and IOS basics (router)		
week12	Gathering information about neighboring devices and using system files (router and switch)		
week13	Configuring a switch for extended functionality (switch)		
week14	Determining IP Routes with EIGRP (router)		
	Determining IP Routes with OSPF (router)		
week15	Determining IP routes with RIP (router)		
	Configuring IP ACLs (router)		
	Configuring PAT (router and switch)		

Development proposals

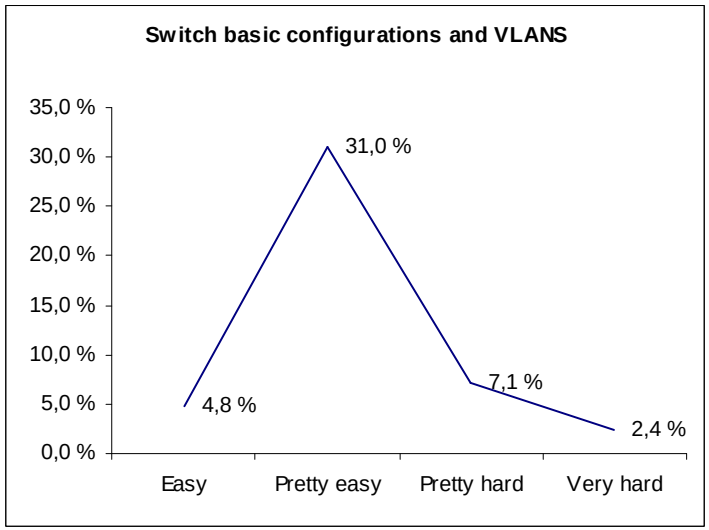
If you remember some things that i need
to consider when i start to design next years exams?

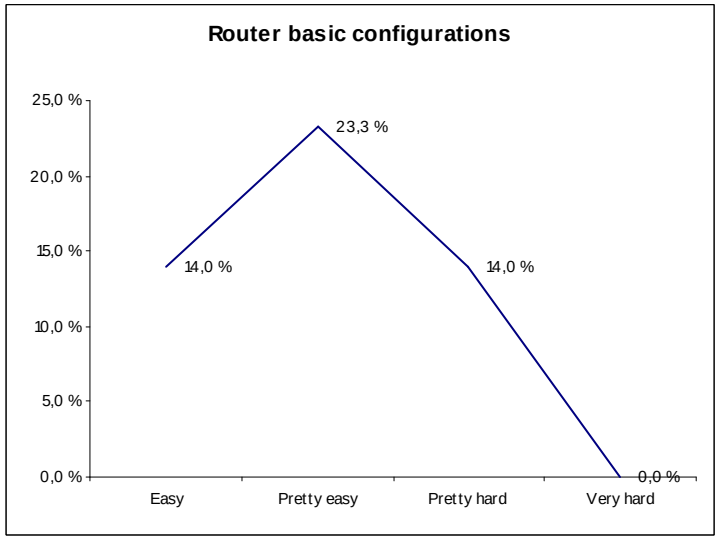
example following things:

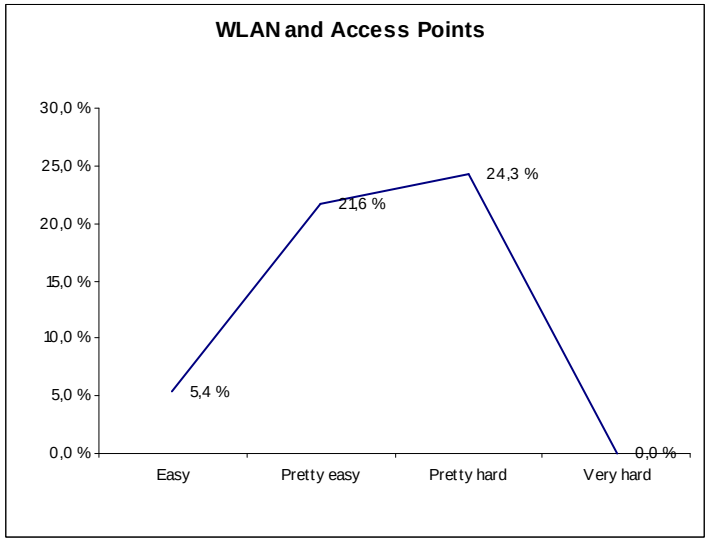
exercises pictures layout or design
exercises papers layout (switch and router exams)
what need to be improved with former Cisco book exams (icnd exams)
exercises theory order
command lists
connecting exams topology
MentorAid lectures

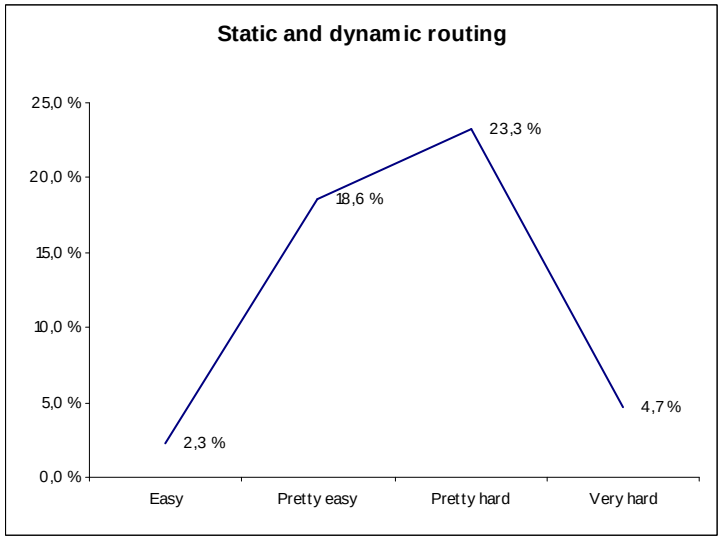
Free word (you can write also in finnish):

Liite 2 Palautekyselyn tulokset vaikeustason perusteella

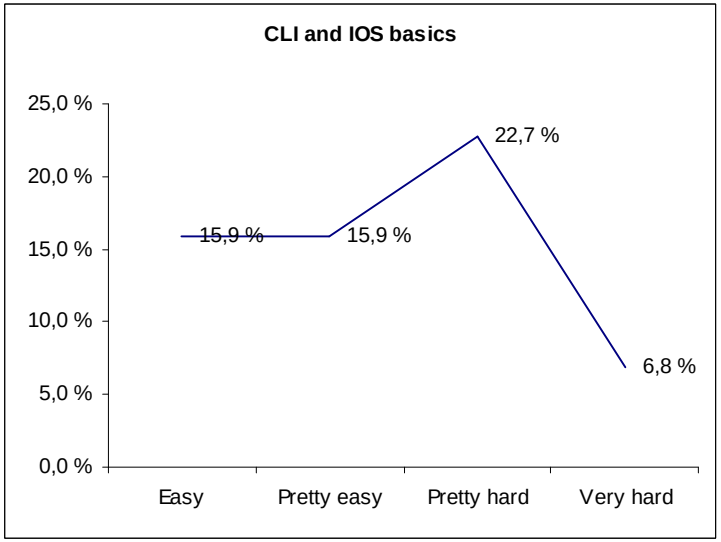


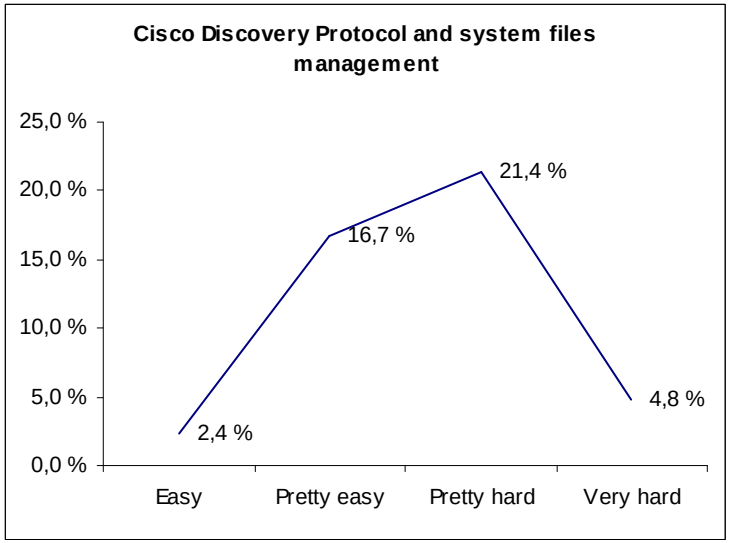


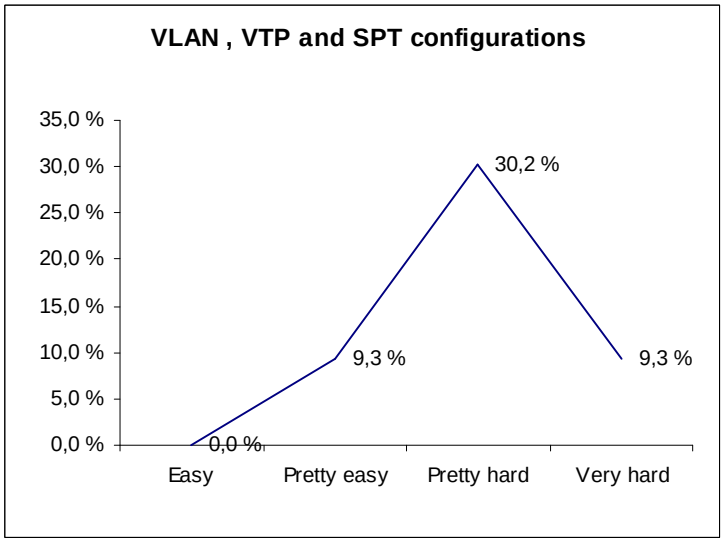


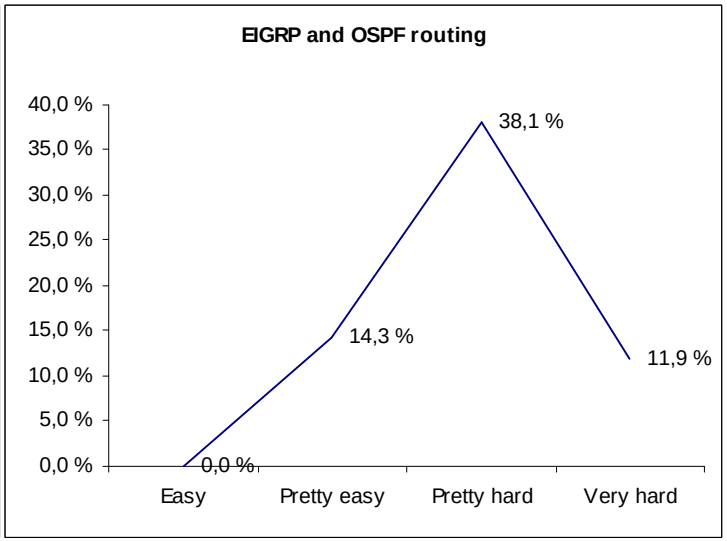


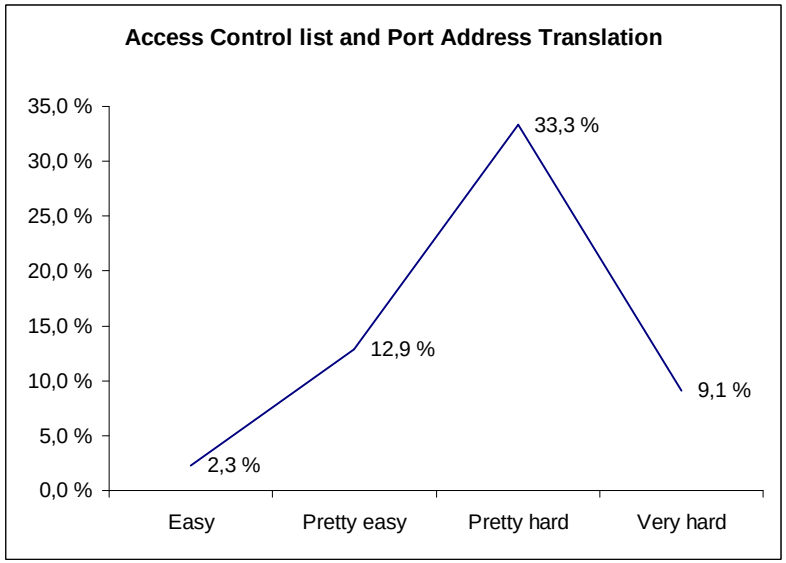
Liite 2


CLI and IOS basics
25,0 %
20,0 %
15,0 %
10,0 %
5,0 %
0,0 %
15,9 %
15,9 %
22,7 %
6,8 %
Easy
Pretty easy
Pretty hard
Very hard

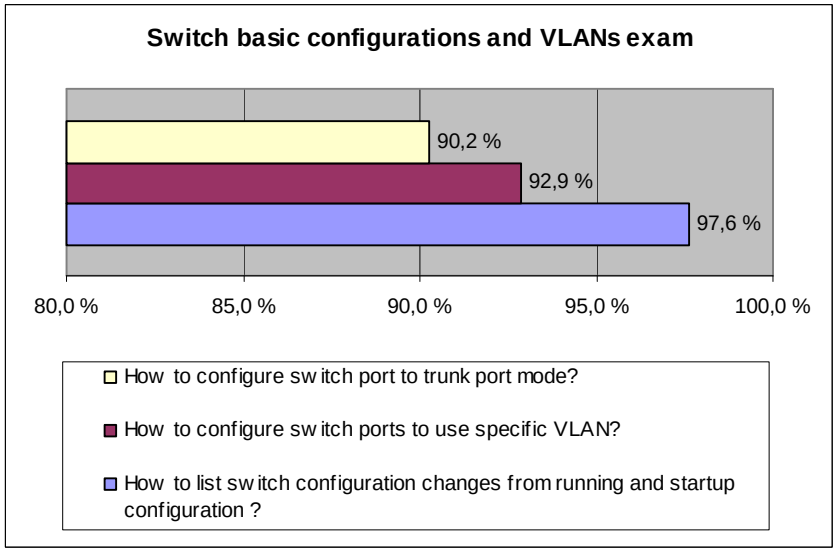

Cisco Discovery Protocol and system files management
25,0 %
20,0 %
15,0 %
10,0 %
5,0 %
0,0 %
2,4 %
16,7 %
21,4 %
4,8 %
Easy
Pretty easy
Pretty hard
Very hard

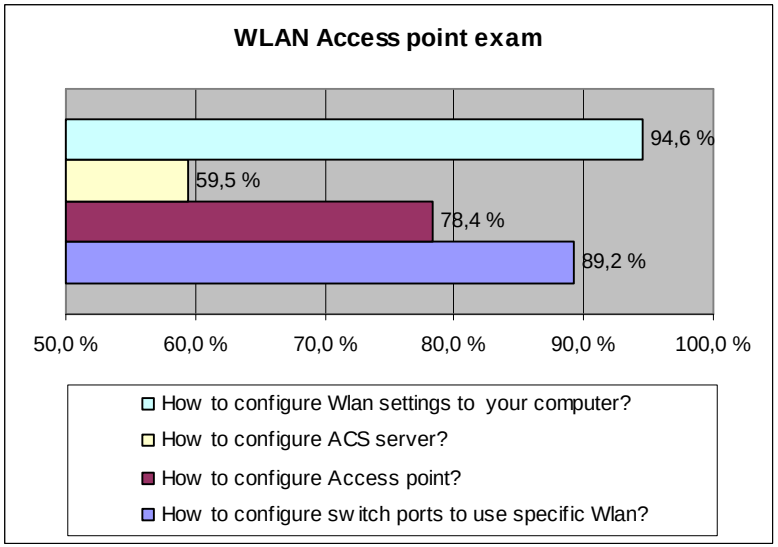

VLAN , VTP and SPT configurations
35,0 %
30,0 %
25,0 %
20,0 %
15,0 %
10,0 %
5,0 %
0,0 %
0,0 %
9,3 %
30,2 %
9,3 %
Easy
Pretty easy
Pretty hard
Very hard

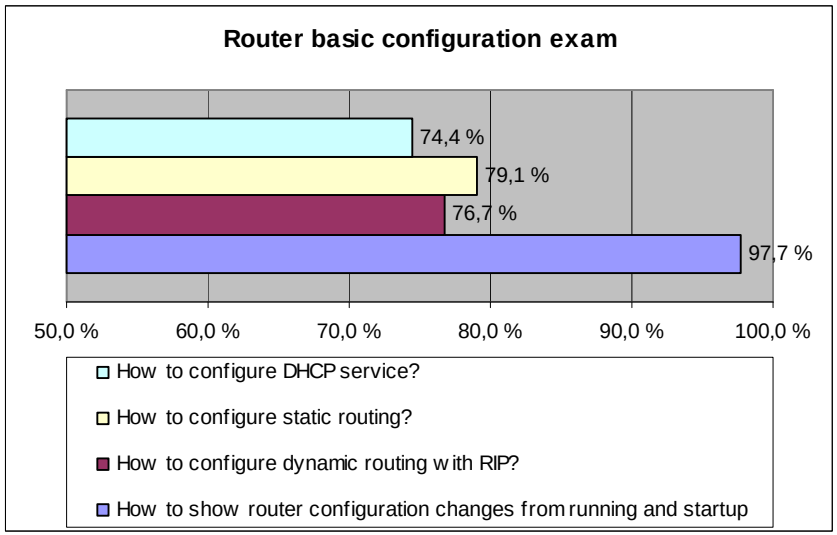

EIGRP and OSPF routing
40,0 %
35,0 %
30,0 %
25,0 %
20,0 %
15,0 %
10,0 %
5,0 %
0,0 %
0,0 %
14,3 %
38,1 %
11,9 %
Easy
Pretty easy
Pretty hard
Very hard

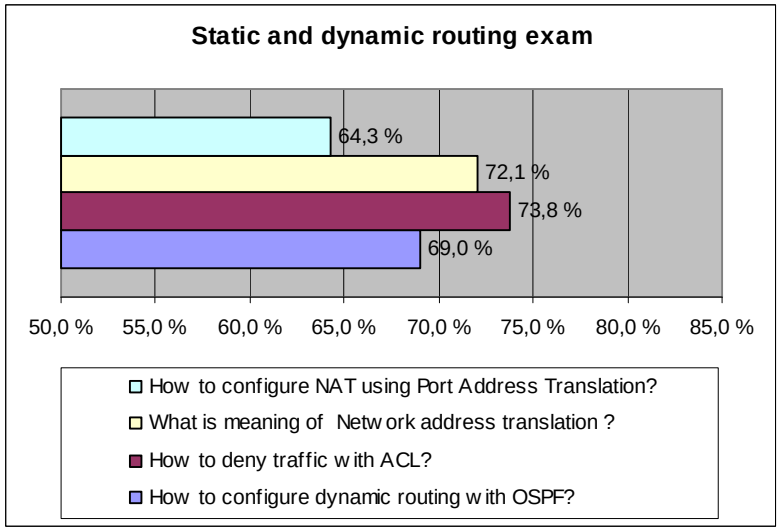

Access Control list and Port Address Translation
35,0 %
30,0 %
25,0 %
20,0 %
15,0 %
10,0 %
5,0 %
0,0 %
2,3 %
12,9 %
33,3 %
9,1 %
Easy
Pretty easy
Pretty hard
Very hard

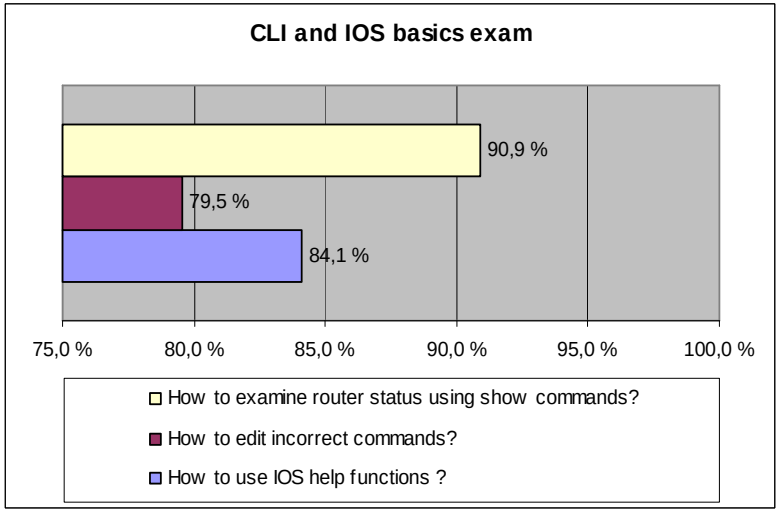
Liite 3 Palautekyselyn tulokset teoria-aiheiden perusteella

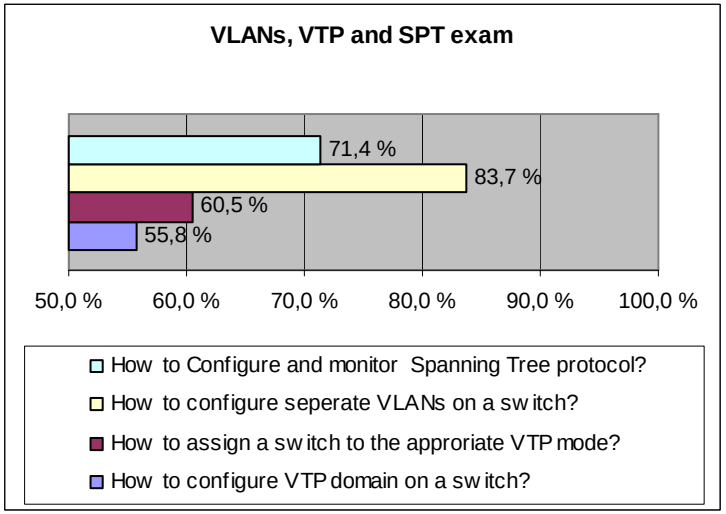


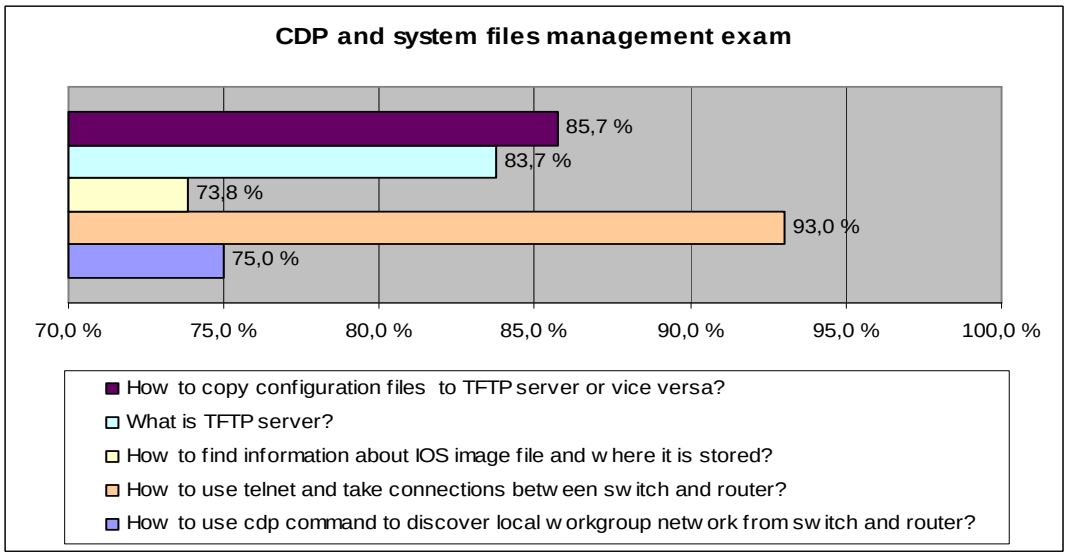




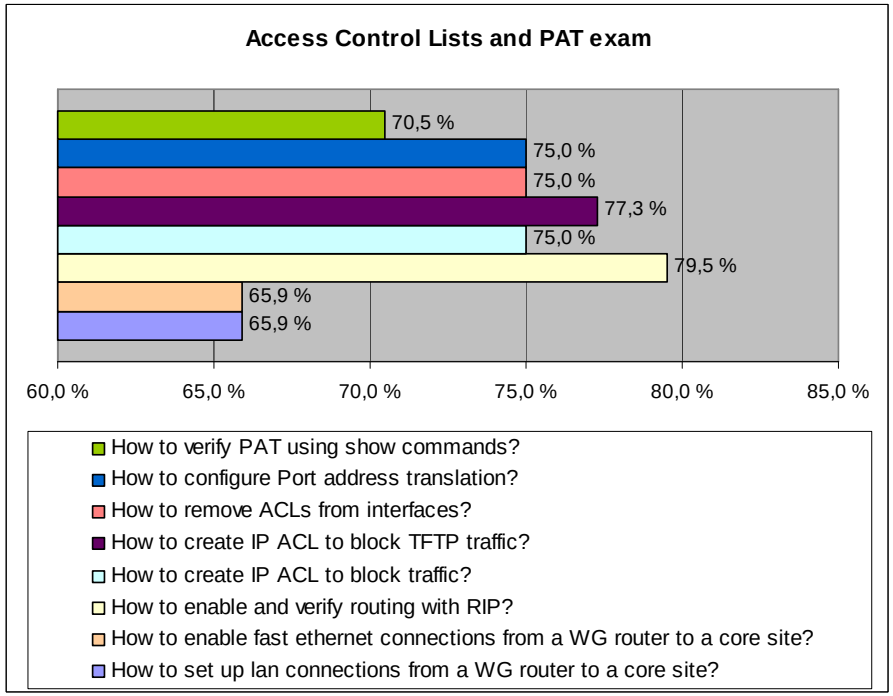


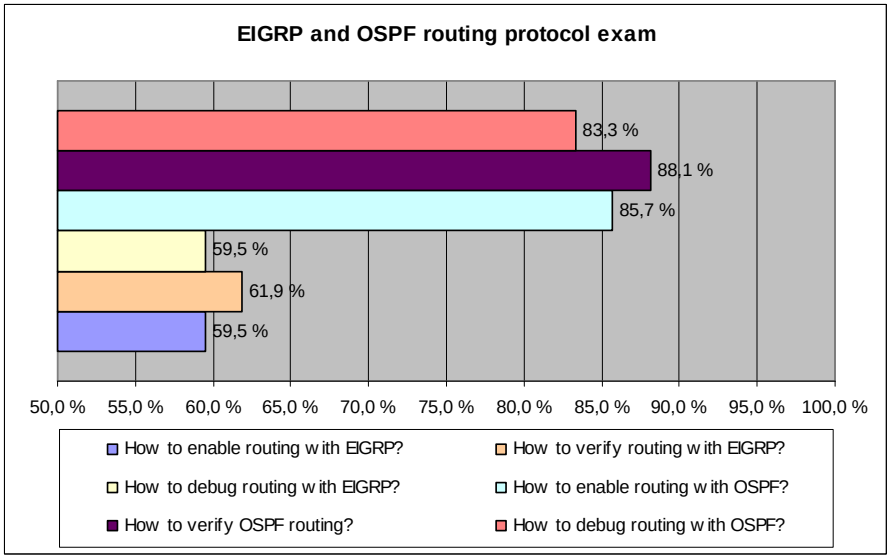

CLI and IOS basics exam
90,9 %
79,5 %
84,1 %
75,0 %
80,0 %
85,0 %
90,0 %
95,0 %
100,0 %
How to examine router status using show commands?
How to edit incorrect commands?
How to use IOS help functions ?


VLANs, VTP and SPT exam
71,4 %
83,7 %
60,5 %
55,8 %
50,0 %
60,0 %
70,0 %
80,0 %
90,0 %
100,0 %
How to Configure and monitor Spanning Tree protocol?
How to configure seperate VLANs on a switch?
How to assign a switch to the approriate VTP mode?
How to configure VTP domain on a switch?


CDP and system files management exam
85,7 %
83,7 %
73,8 %
93,0 %
75,0 %
70,0 %
75,0 %
80,0 %
85,0 %
90,0 %
95,0 %
100,0 %
How to copy configuration files to TFTP server or vice versa?
What is TFTP server?
How to find information about IOS image file and where it is stored?
How to use telnet and take connections between switch and router?
How to use cdp command to discover local workgroup network from switch and router?

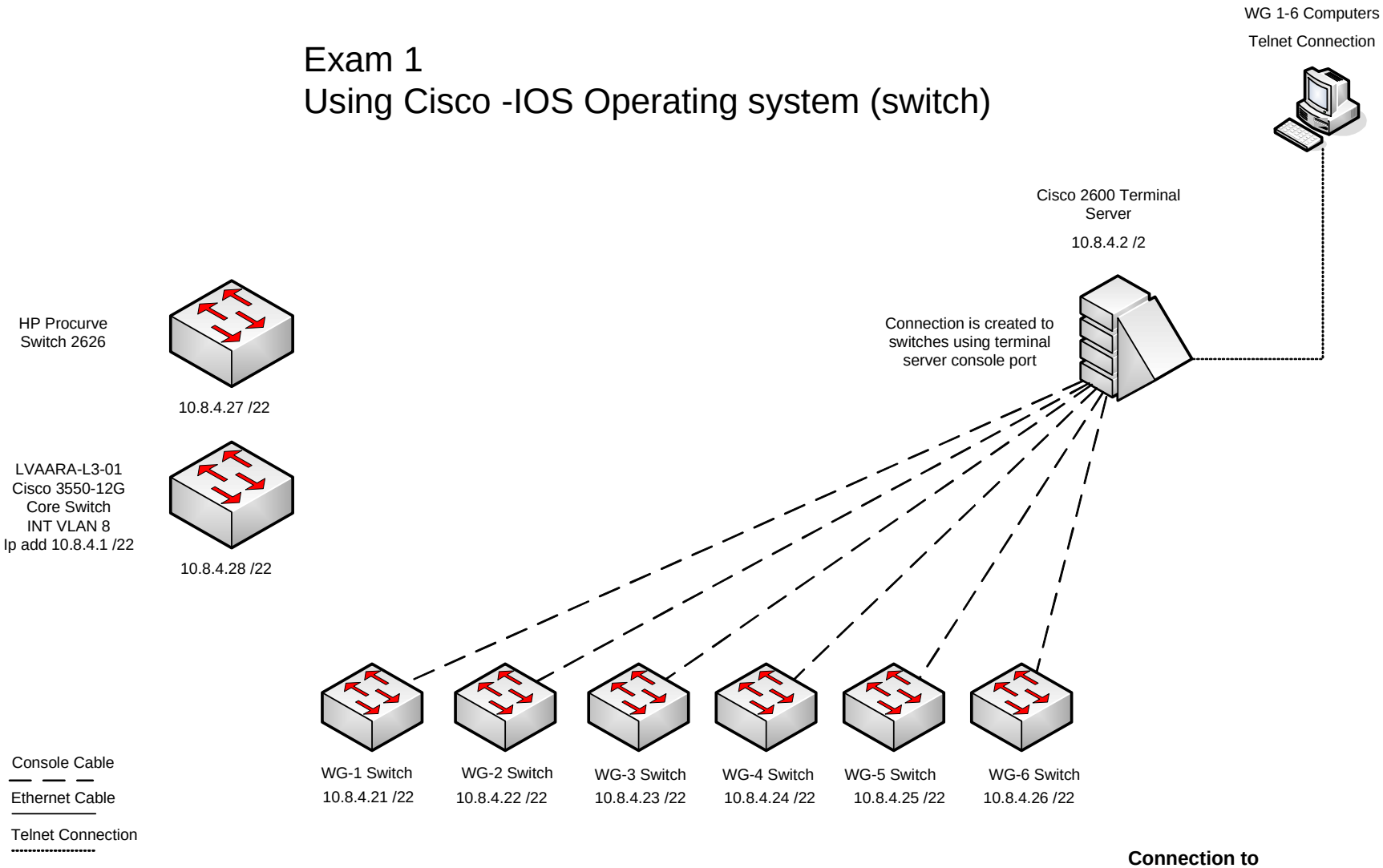
Liite 3


Access Control Lists and PAT exam
70,5 %
75,0 %
75,0 %
77,3 %
75,0 %
79,5 %
65,9 %
65,9 %
60,0 %
65,0 %
70,0 %
75,0 %
80,0 %
85,0 %
How to verify PAT using show commands?
How to configure Port address translation?
How to remove ACLs from interfaces?
How to create IP ACL to block TFTP traffic?
How to create IP ACL to block traffic?
How to enable and verify routing with RIP?
How to enable fast ethernet connections from a WG router to a core site?
How to set up lan connections from a WG router to a core site?


EIGRP and OSPF routing protocol exam
83,3 %
88,1 %
85,7 %
59,5 %
61,9 %
59,5 %
50,0 %
55,0 %
60,0 %
65,0 %
70,0 %
75,0 %
80,0 %
85,0 %
90,0 %
95,0 %
100,0 %
How to enable routing with EIGRP?
How to verify routing with EIGRP?
How to debug routing with EIGRP?
How to enable routing with OSPF?
How to verify OSPF routing?
How to debug routing with OSPF?

Liite 4

Exam 1
Using Cisco -IOS Operating system (switch)



Connection to Devices:

WG 1 Switch: 10.8.4.2 2033	WG 3 Switch: 10.8.4.2 2035	WG 5 Switch: 10.8.4.2 2037
WG 2 Switch: 10.8.4.2 2034	WG 4 Switch: 10.8.4.2 2036	WG 6 Switch: 10.8.4.2 2038

Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week1

Using Cisco IOS Operating system (switch)

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- **Taking connection to switch from terminal server**
- **Using IOS CLI basic commands**
- **Learning to move between different IOS modes**
- **Using help functions**
- **Examine switch status**
- **Setting VTY line username and password**
- **Copy configuration into NVRAM memory**

NEW THEORY CONCEPTS

- IOS basic commands
- IOS help commands
- User exec mode
- Privileged “enable” mode
- Global configuration mode
- Telnet line configuration mode
- Console line configuration mode
- Running-configuration
- Start-up configuration
- RAM memory
- NVRAM memory

ADVANCE JOBS (exam instructor)

- Ensure that switch has right configuration before practise
- Ensure that terminal server ports is cleared, when students take connections

EXAM JOBS (exam instructor)

- Troubleshooting purposes if needed

Week 1 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
show history	privileged	Show last used commands
show version	privileged	Show Cisco -IOS version information
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
terminal history size	privileged	Sets terminal history size
show terminal	privileged	Show content of terminal setups
copy startup config running config	privileged	Copies running-configuration information from NVRAM to RAM
copy running-config startup config	privileged	Copies running-configuration information from RAM to NVRAM
login local	line vty conf	Tell IOS to prompt for username and password
exec timeout	line vty conf	Sets console timeout perioid
logging syncronous	line vty conf	Syncronous messages that are sent to console
username (value) (+) password (value)	conf.mode	Sets username and password required if the login local command is configured
exit	conf.mode	Moving back to the next higher mode
end	conf.mode	Exits in any conf. mode and goes user mode
line console 0	conf.mode	Moving to console line conf.mode
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode

TASK 1 Connecting to switch and explore IOS help functions

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take connection to your workgroup switch. (Check terminal server IP address and port number with picture included)

STEP 3

Enter the (**?**) command at the user EXEC prompt. Press **Return** and then **space bar**.

What happened?

_____

STEP 4

Enter privileged mode using command **enable.**

What happened?

_____

STEP 5

Move back to user exec mode using command **disable**.

How do you know which mode you are?

_____

STEP 6

Enter the (**?**) command at the user EXEC prompt. Press Return and then **(q)** when "- - More - -"is displayed.

What happened?

_____

STEP 7

At the switch# prompt, Enter sh? command and then show ? command.

What is difference between these two commands?

_____

_____

STEP 8

Press **Tab** key after command sh?

What happened?

_____

STEP 9

Press **Ctrl-P** several times and then **Ctrl-N**

What happened?

_____

TASK 2 Examine switch status information

STEP 1

In a privileged mode, Enter show version command and collect information below.

IOS Software:

_____

IOS Software version:

_____

System uptime:

_____

System image file name:

_____

Number of Ethernet interfaces:

_____

Amount of NVRAM:

_____

STEP 2

Enter the show running-config command and collect information below.

Version number:

_____

Host name:

_____

STEP 3

Enter the show history command.

What happened?

_____

STEP 4

In a Privileged EXEC mode, find command that sets terminal line history parameters and after that set terminal history size to **50** lines.

_____

STEP 5

Enter right command to check if terminal history size is correct?

_____

TASK 3 Modify VTY lines configuration and save running configuration

STEP 1

Enter global configuration mode using command **configure terminal**.

STEP 2

Enter virtual lines configuration mode using command **line vty 0 15**.

STEP 3

Find command that set console messages off. This ends messages that console sends to screen.

STEP 4

If the switch console port detects no activity for a specified time, switch terminates the session automatically. You can disable the session termination feature by setting timeout period to infinity.

STEP 5

Enter command “password **cisco**”, this command sets only password, for virtual lines 0-15, when login command is configured.

STEP 6

Change EXEC timeout by using the exec-timeout 0 0 command. Time is then adjusted to 0 minutes and 0 seconds.

STEP 7

Next find out which command must be used when user wants to synchronize messages that are sent to the console display?

STEP 8

Enter command login local and find out what this command means?

STEP 9

Move back to global configuration mode by typing **exit**

STEP 10

Create username and password for telnet connection. (both username and password must be “**cisco**”)

STEP 11

What command you must use if you want to go console line configuration mode?

STEP 12

Return to privileged EXEC mode by typing **exit** or **end**.

STEP 13

Final task is to copy running configuration from start -up configuration. Display first start-up configuration information. What is right command for that?

STEP 14

Display then information in running configuration. What is right command for that?

STEP 15

Then you must copy running configuration into NVRAM by typing copy running-config startup-config. Display then information again in start-up configuration. What is happened?

Week 1 Exam Revision Questions

1 In which of the following modes of the CLI could you issue a command to reboot the switch?

a User mode
b Enable mode
c Global configuration mode
d Interface configure mode

2 What type of switch memory is used to store configuration used by the switch when it is up and working?

a RAM
b ROM
c Flash
d NVRAM
e Bubble

3 What command copies the configuration from RAM into NVRAM?

a copy running-config tftp
b copy tftp running-config
c copy running-config start-up config
d copy start-up-config running-config
e copy startup-config running-config
f copy running-config startup config

4 Which mode prompts the user for basic configuration information?

a User mode
b Enable mode
c Global configuration mode
d Setup mode
e Interface configuration mdoe

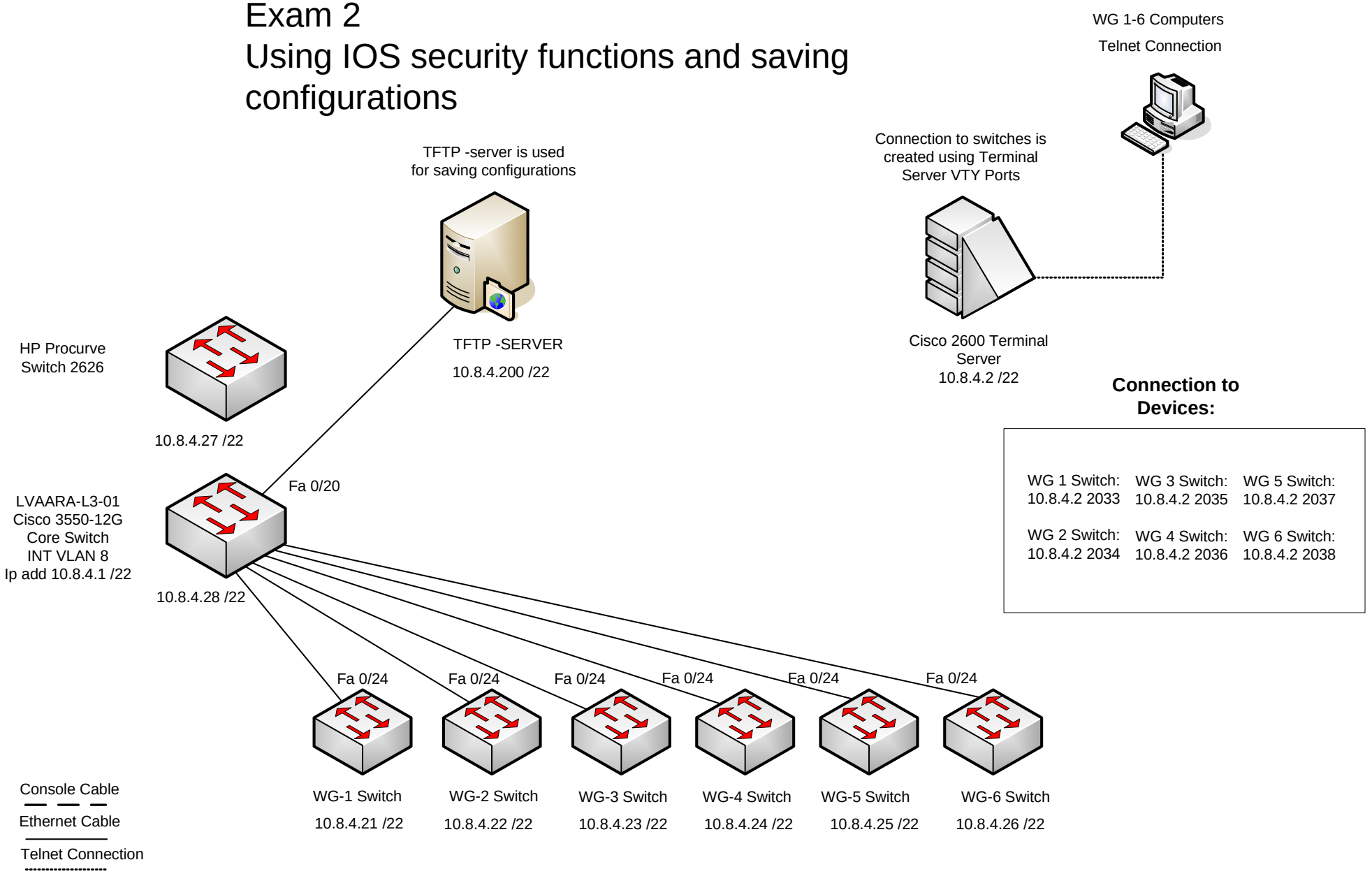
5 A switch is currently in virtual line configuration mode. Which of the following would place the user in privileged mode?

a Using exit command once
b Using exit command twice
c Using quit command
d Using disable command
e Using Enable command

Week 1 Exam Answers

TASK	STEP	ANSWER
1	3	command list screen scrolls down "space bar" one page "return" one line
1	4	prompt changes to #
1	5	IOS prompt character changes when moving between modes
1	6	list scrolling continues when pressing "return" >scrolling quits when pressing "q"
1	7	a) list all commands that begins with sh*
1	7	b)list all commands that is possibility to enter after command "show"
1	8	IOS automatically write remaining characters for command "show"
1	8	if enough characters are entered
1	9	a)IOS lists previous command what is taked from history list
1	9	b)IOS lists next command what is taked from history list
2	1	a) C3500xl b)12.0 c)week,day,hour,minute
2	1	d)c3500XL-c3h2-mz.120-5.3.WC.1.bin e) 24 f) 32kb
2	2	a)12.0 b)switch
2	3	IOS lists all entered commands
2	4	terminal history size 50
2	5	show terminal
3	1	configure terminal
3	2	line vty 015
3	3	no logging console
3	6	exec timeout 0 0
3	7	logging syncronous
3	8	when command is entered, IOS allows users login switch locally
3	10	username cisco password cisco
3	11	line console 0
3	13	copy running-config startup-config
3	14	show running config
3	15	start up configuration content is same that running-config content
Q	1	b
Q	2	a
Q	3	f
Q	4	d
Q	5	b

Exam 2
Using IOS security functions and saving configurations



Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week2

Using IOS security functions and saving configurations (switch)

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- **Connecting switch and using configuration dialog**
- **Setting up passwords and using password encryption**
- **Using banners and line descriptions**
- **Image file information**
- **Setting IP address and subnet mask**
- **Using TFTP server**

NEW THEORY CONCEPTS

- Switch Initial configuration dialog
- Banners
- Line descriptions
- Hostname
- Fast Ethernet line configuration mode
- Configuring IP address and mask to interface
- Enabling and disabling interface
- TFTP server
- IOS image-file content

ADVANCE JOBS (exam instructor)

- Building exam topology and ensuring that topology matches with picture.
- Ensure that switch has right configuration before practise
- Ensure that terminal server ports is cleared, when students take connections
- Ensure that connection with TFTP server is working

EXAM JOBS (exam instructor)

- Ensure that students configuration files are saved to TFTP server
- Troubleshooting purposes if needed

Week 2 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
show mac address-table dynamic	privileged	Lists the dynamically learnerd entries in the switch's address table
show interfaces	privileged	Displays detailed information about interface status
show interfaces status	privileged	Displays summary information about interface status
ping (+) ip-address	privileged	Used for troubleshooting purposes
erase startup-config	privileged	erase startup config file
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
show version	privileged	Show Cisco -IOS version information
copy startup-config running config	privileged	Copies running-configuration information from NVRAM to RAM
copy running-config startup config	privileged	Copies running-configuration information from RAM to NVRAM
copy running-config tftp	privileged	Copies configuration from running-config to tftp -server
copy startup-config tftp	privileged	Copies configuration from startup config to tftp -server
quit	privileged	exits IOS -system
reload	privileged	reboots the switch
end	conf.mode	Exits in any conf. mode and goes user mode
exit	conf.mode	Moving back to the next higher mode
enable secret	conf.mode	Sets clear text- password
enable password	conf.mode	Sets automatically encrypted password
hostname	conf.mode	Sets switch's hostname
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
line console 0	conf.mode	Moving to console line conf.mode
banner motd	conf.mode	Sets banner thats is shown before the login prompt
interface fastethernet	conf.mode	Moving to interface conf.mode
username (value) (+) password (value)	conf.mode	Sets username and password required if the login local command is configured
no logging console	conf.mode	disables IOS -logging information
interface vlan (id)	conf mode	Moving to vlan configuration mode
login local	line vty conf	Tell IOS to prompt for username and password
description (text)	line fa conf	Lists any information text that is connected to interface
ip address (value) (+) mask (value)	line fa conf	Sets ip address and mask for interface
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
ip address (value) (+) mask (value)	vlan conf	Sets ip address and mask for VLAN
management	vlan conf	Make management VLAN

TASK 1 Connect switch and use Cisco system configuring dialog

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take connection to your switch. (Check terminal server IP address and port number with a picture included)

STEP 3

Enter privileged mode:

_____

Enter command **setup** and answer **yes** to question would you like to enter the initial configuration dialog?

STEP 4

You must now enter switch basic configuration settings. Enter switch IP address "**10.8.4.?**" look right address for the picture, mask "**255.255.252.0**" host name "**wg?_switch**", enable secret password "**cisco**" and VTY password "**cisco**" when IOS prompts the questions.

STEP 5

Save this configuration to nvram and exit.

STEP 6

What difference is between enable secret and enable password, find answer using command show running-config.

_____

_____

STEP 7

Enter command that disables console messages from IOS screen.

_____

STEP 8

Enter global configuration mode:

_____

STEP 9

Enter terminal line 0 4 configuration mode.

_____

STEP 10

What is meaning of final two numbers of that command?

_____

What is meaning of VTY -line password?

_____

STEP 11

Go back to privileged mode and check password settings. Console line password must be "cisco", Enable password "sanfran" and enable secret password "cisco".

STEP 12

Then you must copy running configuration into NVRAM by typing copy running config startup config.

TASK 2 Create banners and interface descriptions

STEP 1

Go back to global configure mode and create Message-of-the-day banner, IOS shows MOTD -banner above the login screen where username and password are entered. Using "?" find command that creates MOTD -banner.

STEP 2

Create short text message "Maintenance today 22.00 pm"in the banner. Use help to guide your through process. How do you end typing message.

Enter banner command:

How is possibility to end inserting command?

Enter interface fast Ethernet 0/1 configure mode using the "**interface fastethernet 0/1"** command.

STEP 3

Create description for interface fast Ethernet 0/1. Meaning of port description is told user, what interface does and where it is connected to.

STEP 4

Go back to privileged mode and enter show running-config command and find following information below.

VTY password:

Enable password:

Description for Ethernet interface 0/1:

MOTD Banner:

STEP 5

What is command that lists switch's learned mac -address table information?

TASK 3

Show image file name information and configuration files management

STEP 1

In a privileged mode, using show version command find following information below

Name of Cisco IOS Image file:

Version of the Cisco IOS Software:

Location of the image file:

Find specific information about image file name below:

Image File extension:

Type of switch platform:

Supported feature set:

File version number:

TASK 4 Configure Fast Ethernet 0/1 interface on the switch and management VLAN

STEP 1

Enter interface FA 0/1 configure mode:

STEP 2

What command do must use to enable interface? Enable then interface FA 0/1.

STEP 3

What is a state of interface after it was enabled? What command you must use if you want to determine the state of the interface?

STEP 4

What is encapsulation type of that interface?

STEP 5

What is Fast Ethernet address of that interface?

STEP 6

Return to global configuration mode.

STEP 7

Move to VLAN 1 configuration mode

STEP 8

Remove IP address for VLAN 1

STEP 9

Return to global configuration mode

STEP 10

Move to VLAN 8 configuration mode

STEP 11

Configure IP address 10.8.4.? and subnet mask 255.255.252.0 for VLAN 8

STEP 12

Set VLAN 8 to management mode

TASK 5 Copy switch configuration to TFTP server

STEP 1

Final task is copy your configuration to TFTP server. In a privileged mode type right command, that copies you configuration file to TFTP server. (Image file name and IP address are found at the picture)

Three most important things at the copy process are followed, write answers below:

What is saved image file name?

_____

What is TFTP server IP address?

_____

Where new configuration is purposed to place?

_____

Enter right copy command below.

_____

Use following image file name: "**Ex2Group?"** where "?" is your workgroup number.

STEP 2

How do you know that copy process is successfully completed?

_____

Week 2 Exam Revision Questions

1 If you have configured enable secret command and then enable password command and reload switch. Which command defines the password that you had to enter to access privileged mode?

a enable password
b enable secret
c neither
d password command

2 Using command banner login this is the login banner. Which is the following are true about what occurs the next time user logs in from the console?

a no banner at all
b "his is" is displayed
c "this is the login banner" is displayed
d "Login banner configured, no text defined" is displayed

3 Where configuration must be copied from TFTP -server if user wants to use only new copied configuration?

a startup-configuration
b running-configuration
c both
d either

4 What happens if user copies new configuration from TFTP -server to switch's functioning running-configuration?

a new runningconfiguration exists
b old running configuration exists
c configurations merged each other
d IOS denies copying

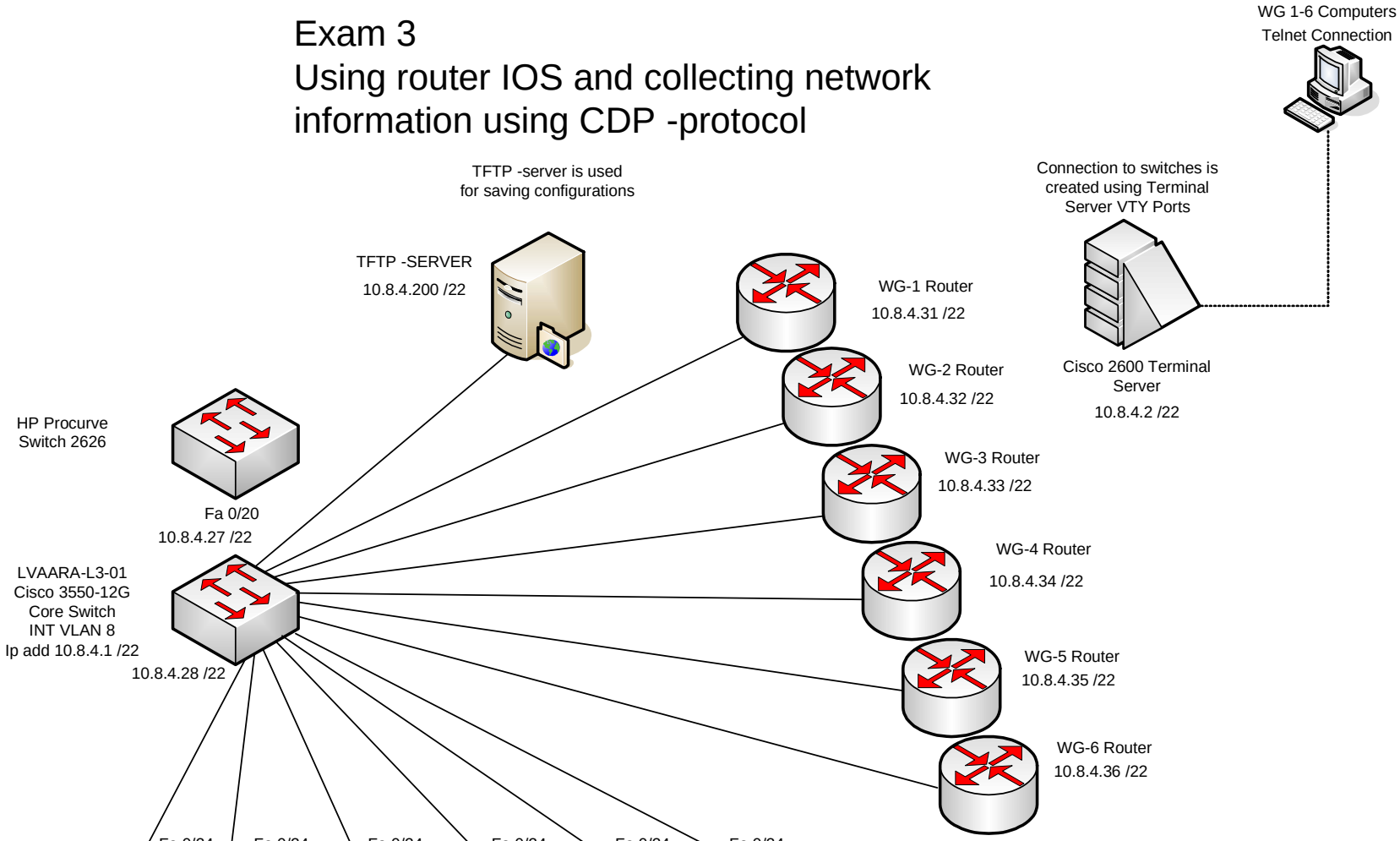
5 What is right command if user wants to check information about IOS -image file name and version?

a show IOS information
b show version
c show runnning-config
d show interfaces
e show status

Week 2 Exam Question Answers

TASK	STEP	ANSWER
1	3	enable
1	6	enable secret command encrypts the password enable password not
1	7	no logging console
1	8	configure terminal
1	9	line vty 0 4
1	10	a)it means that what vty lines are included with command
1	11	b)it protects virtual terminal lines when connecting switch or router
1	12	copy running-config
2	1	motd banner + separate mark+enter "text" + separate mark
2	2	a)motd banner + "Maintenance today 22.00 pm" + z
2	2	b)with delimiting character (it can be any character)
2	3	description "text"
2	4	a)cisco b)cisco c)description text d) maintenance today 22.00 pm
2	5	show mac-address table dynamic
3	1	a)c3500xl…bin b)12.0 c)flash memory d)bin e) c3500XL f)c3h2s g) 5.3
4	1	interface fastethernet 0/1
4	2	no shutdown
4	3	a) up
4	3	b) show interface fa 0/0
4	4	ARPA
4	5	switch mac address >example 0005.9ba8.5cc1
4	6	exit
4	7	int vlan 1
4	8	remove ip address
4	9	exit
4	10	int vlan 8
4	11	ip address 10.8.4.21 255.255.252.0
4	12	management
5	1	a) Ex2Group1-6 b) 10.8.4.200 c)TFTP-server d) copy running-config tftp
5	2	Copy process has been completed message
Q	1	b
Q	2	b
Q	3	a
Q	4	c
Q	5	b

Exam 3
Using router IOS and collecting network information using CDP -protocol



Console Cable

Ethernet Cable

Telnet Connection

Connection to Devices:

WG 1 Switch: 10.8.4.2 2033	WG 3 Switch: 10.8.4.2 2035	WG 5 Switch: 10.8.4.2 2037
WG 1 Router: 10.8.4.2 2049	WG 3 Router: 10.8.4.2 2051	WG 5 Router: 10.8.4.2 2053
WG 2 Switch: 10.8.4.2 2034	WG 4 Switch: 10.8.4.2 2036	WG 6 Switch: 10.8.4.2 2038
WG 2 Router: 10.8.4.2 2050	WG 4 Router: 10.8.4.2 2052	WG 6 Router: 10.8.4.2 2054

Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week3

Using router IOS and collecting network information using Cisco Discovery protocol, CDP

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- **Connecting router from terminal server**
- **Comparing Switch and Router IOS systems**
- **Using Cisco Discovery Protocol**
- **Using Telnet connections between Cisco devices**
- **Getting configuration from TFTP server**

THEORY CONCEPTS

- Cisco Discovery protocol
- Telnet connections between devices

ADVANCE JOBS (exam instructor)

- Building exam topology and ensuring that topology matches with picture.
- Ensure that terminal server ports is cleared, when students take connections
- Ensure that routers has right configuration before practise
- Ensure that routers telnet connection to switches are working before practise

EXAM JOBS (exam instructor)

- Ensure that connection with TFTP server is working
- Ensure that configuration files are located on TFTP server
- Troubleshooting purposes if needed

Week 3 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
ping (+) ip-address	privileged	Used for troubleshooting purposes
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup-config	privileged	Copies running-configuration information
running config		from NVRAM to RAM
copy running-config	privileged	Copies running-configuration information
startup config		from RAM to NVRAM
copy tftp startup-config	privileged	Copies tftp server configuration to startup-config
copy tftp running-config	privileged	Copies tftp server configuration to running-configuration
erase startup-config	privileged	erase startup config file
erase nvram	privileged	erase startup config file
show interfaces (type)	privileged	Displays detailed information about interface status
show interfaces status	privileged	Displays summary information about interface status
show ip interface brief	privileged	Displays single line information about each interface
show protocols (type)	privileged	Displays ip address, mask and line protocol status inf
show controllers (type)	privileged	Displays hardware controller information per interface
show version	privileged	Show Cisco -IOS version information
show cdp neighbors (type)	privileged	Displays neighbor information
show cdp neigbors detail	privileged	Displays detailed neighbor information
show cdp traffic (type)	privileged	Displays statistics of CDP advertisements
show sessions		Lists the suspended Telnet and SSH connections
telnet (hostname)	privileged	Connects the CLI to another host using telnet
resume	privileged	Resumes connection to suspended host
disconnect	privileged	Disconnects connection to suspended host
login local	line vty conf	Tell IOS to prompt for username and password
username (value) (+)	conf.mode	Sets username and password required
password (value)		if the login local command is configured
exit	conf.mode	Moving back to the next higher mode
end	conf.mode	Exits in any conf. mode and goes user mode
line console 0	conf.mode	Moving to console line conf.mode
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
ip address (value) (+)	line fa conf	Sets ip address and mask for interface
mask (value)		
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
Cntr+Shift-6, x	keyboard sc	Key sequence to suspend Telnet or SSH connection

TASK 1 Connect router and compare IOS functions between switch and router

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take connection to your router. (Check terminal server IP address and right port number with a picture included)

STEP 3

Enter privileged mode.

STEP 4

Enter show running-config and collect information. What different router interfaces information did you find? Write below:

STEP 5

Move between different IOS modes by typing necessary commands. Do you notice some differences between router and switch IOS mode? Write below?

STEP 6

Create username and password for vty lines. (username and password must be “cisco”). Write commands below:

STEP 7

Enter virtual lines 0-4 configuration mode.

STEP 8

Enter command that allows users login locally.

STEP 9

You can now close current connection and take new connection to router. When logged in you must type username and password for when using VTY lines connection.

TASK 2 Examine router interfaces and router information

STEP 1

Enter privileged mode.

STEP 2

Show router interfaces information using different show commands.

What is state of fast Ethernet interface 0/0?

What is protocol state of Ethernet interface 0/1?

STEP 3

When typing commands you can use shortened version of commands. Example interface fast Ethernet 0/0 can be shortened "**sh int fa 0/0**".

STEP 4

Enter global configuration mode.

STEP5

Enter router interface FA 0/0 configuration mode.

STEP 6

Define IP address and subnet mask to interface FA 0/0. Look right addresses and masks from the exam picture.

STEP 7

Enable router interface FA 0/0.

STEP 8

Move back to privileged mode.

STEP 9

Use command show version and collect information below:

IOS Version:

_____

System Uptime:

_____

Time of the last loading of IOS:

_____

Amount of RAM memory:

_____

Amount on NVRAM memory:

_____

Amount of Flash memory:

_____

Configuration registers current value:

_____

TASK 3 Collect network environment information using Cisco Discovery Protocol

STEP 1

In a privileged mode, enter show cdp "?" command, what are options for that command?

STEP 2

Use right command that shows network neighbourhood information around router. Collect information below:

Device identifier:

Address list:

Local Interface:

Port Identifier:

Capabilities list:

Platform:

STEP 3

Use command that shows advertisement traffic between devices. Are there traffic now between router and other network devices?

TASK 4 Use telnet connections between switch and router

STEP 1

Use command telnet and take connection to workgroup switch from your router, use only IP address (look at the picture below). Write right command below:

_____

STEP 2

What is your console prompt after successful connection?

_____

STEP 3

When connected to switch, press Ctrl-Shift-6 and then x. What happened?

_____

STEP 4

Show sessions command displays your current connections to other devices.

How many connections do you have?

_____

Disconnect your current session to your workgroup switch. What is right command for close connection to switch?

_____

TASK 5 Getting new configuration from TFTP server

STEP 1

Final task is to get new configuration file from TFTP server. First you must ping TFTP server to verify that your router has connectivity to it. (TFTP server address is found at the picture)

STEP 2

Enter command to erase the start-up configuration in NVRAM. What is right command for that?

_____

STEP 3

Finally you must boot-up router to reload new configuration. What is right command that boots up router?

_____

STEP 4

Check router start-up processes and when the system is running again enter command show running-config. What configuration router is now using?

_____

Week 3 Exam Revision Questions

1 Which of the following installation steps are typically required on a Cisco router but not typically on Cisco Switch?

a Connect ethernet cables
b Connect to the console port
c Connect the power cable
d Turn on / off switch to "on"

2 Which of the following features would you typically expect to be assiciated with the router CLI, but not with the switch CLI?

a clock rate command
b ip address address mask command
c ip address dhcp command
d interface vlan 1

3 Which of the following hexadecimal values in the last nibble of the configuration register would cause a router to not look Flash memory for an IOS?

a 0
b 4
c 5
d 6

4 Which of the following CDP command could identify a neighbor model of hardware?

a show neighbors
b show cdp
c show cdp interface
d show cdp neighbors

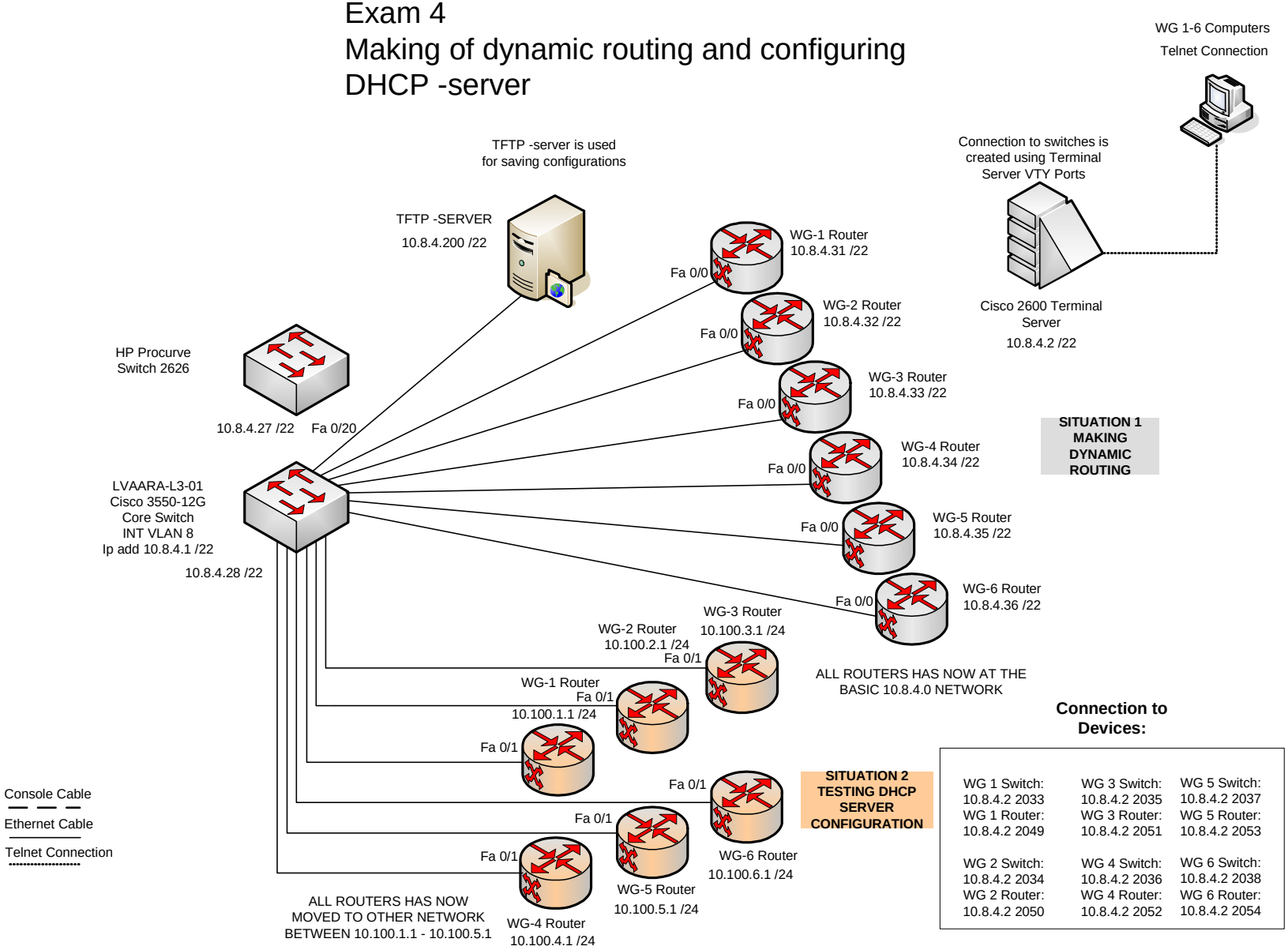
5 Can you take multiple telnet connections to simultaneusly from one router to many other network devices?

a yes but connecting is only possible to specific routers
b yes all routers can take multiple connections to any devices anywhere
c no only one connection is possible
d yes but only other routers
e yes but only devices in same VLAN

Week 3 Exam Question Answers

TASK	STEP	ANSWER
1	3	enable
1	4	fastethernet interface 0/0 and 0/1, line console 0, line vty 015
1	5	there are no differences between switch and router IOS modes
1	6	username cisco password cisco
1	7	line vty 0 4
1	8	login local
2	1	enable
2	2	a)state is down
2	2	b)line protocol down
2	4	configure terminal
2	5	interface fa 0/0
2	7	enable
2	8	exit, exit
2	9	a)12.0 b) week, hours, minutes c) restart time d) 249Kb / 12288Kb
2	9	e) 239 Kb f) 62720 Kb g) 0x2142
3	1	a) entry,interface,neigbors,traffic
3	2	a) Devide ID b)Local Intrface c)IP address (only detail) d)Port ID
3	2	e)Capability f)Platform
3	3	show cdp traffic
4	1	telnet wg switch ip address example 10.8.4.21
4	2	switch #
4	3	Telnet connection is suspended and router ios connection is returned
4	4	a)one b)disconnect 1
5	2	erase nvram, erase startup-config or write erase
5	3	reload
5	4	router is using now empty default configuration
Q	1	e
Q	2	a
Q	3	a
Q	4	d
Q	5	b

Exam 4
Making of dynamic routing and configuring DHCP -server



Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week4

Making Dynamic Routing using RIPv2 and configuring router DHCP server

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- Booting up router and using configuration dialog
- Examining router table information
- Configuring dynamic routing
- Configuring DHCP server

THEORY CONCEPTS

- Routing table
- Dynamic routing
- Routing information Protocol (RIP)
- DHCP server

ADVANCE JOBS (exam instructor)

- Building exam topology and ensuring that topology matches with picture.
- Ensure that terminal server ports is cleared, when students take connections
- Ensure that router has right configuration image before practise, router must boot with right configuration.

EXAM JOBS (exam instructor)

- Ensure that connection with TFTP server is working
- Ensure that configuration files are saved to TFTP server
- Ensure that connections between routers are working when testing connections using ping command
- Troubleshooting purposes if needed

Week 4 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
ping (ip-address)	privileged	Used for troubleshooting purposes
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup config	privileged	Copies running-configuration information
running config		from NVRAM to RAM
copy running-config	privileged	Copies running-configuration information
startup config		from RAM to NVRAM
copy running-config tftp	privileged	Copies configuration from running-config to tftp
copy startup config tftp	privileged	Copies configuration from startup config to tftp
show interfaces (type)	privileged	Displays detail information about interface status
show interfaces status	privileged	Displays summary info about interface status
show ip interface brief	privileged	Displays single line info about each interface
show protocols (type)	privileged	Displays ip add, mask and line protocol status inf
show controllers (type)	privileged	Displays hardware controller info per interface
show version	privileged	Shows Cisco -IOS version information
show ip route	privileged	Shows routing table information
ip route 0.0.0.0 0.0.0.0 (+)	conf.mode	Defines default IP -route
mask (+) destination address		
router rip	conf.mode	Starts (dynamical) RIP -routing protocol
ip dhcp pool +name	conf.mode	Defines DHCP -pool name
end	conf.mode	Exits in any conf. mode and goes user mode
exit	conf.mode	Moving back to the next higher mode
enable secret	conf.mode	Sets clear text- password
enable password	conf.mode	Sets automatically encrypted password
hostname	conf.mode	Sets switch's hostname
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
line console 0	conf.mode	Moving to console line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
username (value) (+)	conf.mode	Sets username and password required
password (value)		if the login local command is configured
no logging console	conf.mode	Disables IOS -logging information
enable ip routing	conf.mode	Enables IP Routing
login local	line vty conf	Tell IOS to prompt for username and password
ip address (value) (+)	line fa conf	Sets ip address and mask for interface
mask (value)		
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
version	RIP conf.mode	Defines RIP -protocol version
network (value)	RIP conf.mode	Defines networks for RIP -protocol
network (value) (+)	DHCP conf.mode	Adds DHCP -pool IP -address
mask (value)		
default-router	DHCP conf.mode	Adds DHCP -pool default router address

TASK 1 Boot up router and configure IP address to interface fast Ethernet 0/0

STEP 1

First task is to power on your router with using default configuration settings.

STEP 2

From your PC, Open connection to terminal server.

STEP 3

Take connection to your router. (Check terminal server IP address and port number with a picture included)

STEP 4

Check router start-up processes and answer **yes** to question. Would you like to enter the initial configuration dialog?

STEP 5

Cisco System configuration dialog is started, answer questions and set up router **hostname**, **enable secret, enable password**, **vty password, FA 0/0 interface IP address** and **subnet mask**. (answers is found at the picture)

STEP 6

When configuration dialog is ended, save configurations to nvram.

STEP 7

Open new command prompt windows and check your computer network configuration. Fill starting information below:

IP Address:

_____

Subnet Mask:

_____

Default Gateway:

_____

DHCP server:

_____

STEP 8

Enter privileged mode.

_____

STEP 9

Enter show running-config and show interfaces commands and collect information below. Ensure that hostname and passwords are same that you entered earlier.

Router Hostname:

_____

Enable password:

_____

FA 0/0 interface IP address:

_____

FA 0/0 interface subnet mask:

_____

STEP 10

Move interface Fast Ethernet 0/1 configuration mode.

STEP 11

Add IP address and subnet mask to router interface FA 0/1. (check picture for right address and mask)

STEP 12

Set up interface FA 0/1.

STEP 13

Go back to global configuration mode.

STEP 14

Enter command that disables console messages from IOS screen.

STEP 15

Show running-configuration information and ensure that both interfaces have now IP addresses and masks.

STEP 16

Ping your router interface FA 0/1 IP address from your computer. Can you get echo reply message?

TASK 2 Examine router table information and use dynamic routing to advertise network

STEP 1

Enable IP routing for router

STEP 2

Now, when you have configured router interfaces. Next task is set dynamic routing protocol (RIPv2) to advertise your network.

In a privileged mode show router routing table information. Search right command for that function.

What routes are listed on a table?

There are some letters before the route marking. What information these letters give you? Check explanations above the routing table.

What routes are now at the table?

STEP 3

Go to global configuration mode.

STEP 4

Insert default route to address 10.8.4.1 that is working DHCP server for a network 10.8.4.0. What is right command to set default route from your router to another router?

What is meaning of three groups of numbers of that command?

First group:

Second group:

Third group:

STEP 5

Start up dynamic routing protocol RIPv2 to your own network and network 10.8.4.0.

Insert right commands below:

STEP 6

Go back to privileged mode.

STEP 7

Show content of routing table information. What new information did you find?

STEP 8

Other groups routing protocol information is listed after they have configured their routing protocol and they have enabled their router interfaces and IP addresses.

Ping other groups routers FA 0/1 interface IP addresses, including your own IP address. (look right IP addresses with a picture) Did you get reply after ping command? Answer below:

Group 1

Group 2

Group 3

Group 4

Group 5

Group 6

Use command show IP route “address number” to one of the addresses that is replied for your ping command. What information did you get?

What are functional differences between RIP 1 and RIP 2 protocol?

STEP 9

Move computer to a new network (change cable to other socket from your table)

Check computer network configuration from that network, before DHCP server configuration.

IP Address:

_____

Subnet Mask:

_____

Default Gateway:

_____

DHCP server:

_____

Did you get correct information, are the network connections now working?

_____

TASK 3 Set up DHCP (Dynamic Host Control Protocol) server

STEP 1

Move computer back to original network. (change cable back to left socket from your table)

STEP 2

Move to global configuration mode.

_____

STEP 3

Add DHCP pool “DHCP_WG?” to router, where “?” is your group number.

_____

STEP 4

Router is now moved to DHCP configuration mode. What is router prompt now?

_____

STEP 5

Add DHCP network IP address. Use your workgroup network address for that.

_____

STEP 6

Add default router IP address. Use your router FA 0/1 interface address for that.

_____

STEP 7

Move computer to a new network. (change cable to other socket from your table)

IP Address:

Subnet Mask:

Default Gateway:

DHCP server:

Did you get correct information, are the network connections now working?

What is device that gives IP address to your computer?

TASK 4 Copy router configuration to TFTP server

STEP 1

Go to privileged mode.

STEP 2

Final task is copy your configuration to TFTP server. Type right command, that copy configuration file to TFTP server. (Image file name and IP address is found at the picture).

Enter right copy command below.

Use following image file name: "**Ex4Group?"** where "?" is your workgroup number.

STEP 3

Can router use switch configuration file or vice versa. What happen if example switch configurations file is copies over router start-up configuration?

Week 4 Exam Revision Questions

1 What is right command, when user wants to configurate working IP -address and mask to router first Fast Ethernet interface?

a interface fa 0/1 then ip address 10.0.0.1 mask 255.255.255.0
b interface fa 0/0 then ip address 10.0.0.1 0.0.0.255
c interface fa 0/1 ip address 10.0.0.1 mask 255.255.255.0
d interface fa 0/0 then ip address 127.0.0.1 255.255.255.0

2 Router 1 has interfaces with address 9.1.1.1 and 10.1.1.1. Router 2 has connected to router 1 over fa link and has addresses 10.1.1.2 and 11.1.1.2. Which command is right if user wants to configure rip 2 protocol which advertises out all interfaces and all routes?

a router rip
b router rip 3
c router rip then number 2
d version 2

3 Router 1 has interfaces with address 9.1.1.1 and 10.1.1.1. Router 2 has connected to router 1 over fa link and has addresses 10.1.1.2 and 11.1.1.2. Which command is right if user wants to configure rip 2 protocol which advertises out all interfaces and all routes?

a network 9.0.0.0
b network 11.0.0.0
c network 10.1.1.1
d network 11.1.1.2

4 When inserting default route from router1 to default router2 10.10.10.1, what is right command to do that?

a ip route 10.10.10.1 255.255.255.0
b ip route 10.10.10.1 0.0.0.0 0.0.0.0 255.255.255.0
c ip route 0.0.0.0.0.0.0.0 10.10.10.1 255.255.255.0
d ip route 0.0.0.0 0.0.0.0 10.10.10.1

5 What is right command to set DHCP -server DHCP1 to router 1? DHCP server is sharing addresses from network 10.100.100.0.

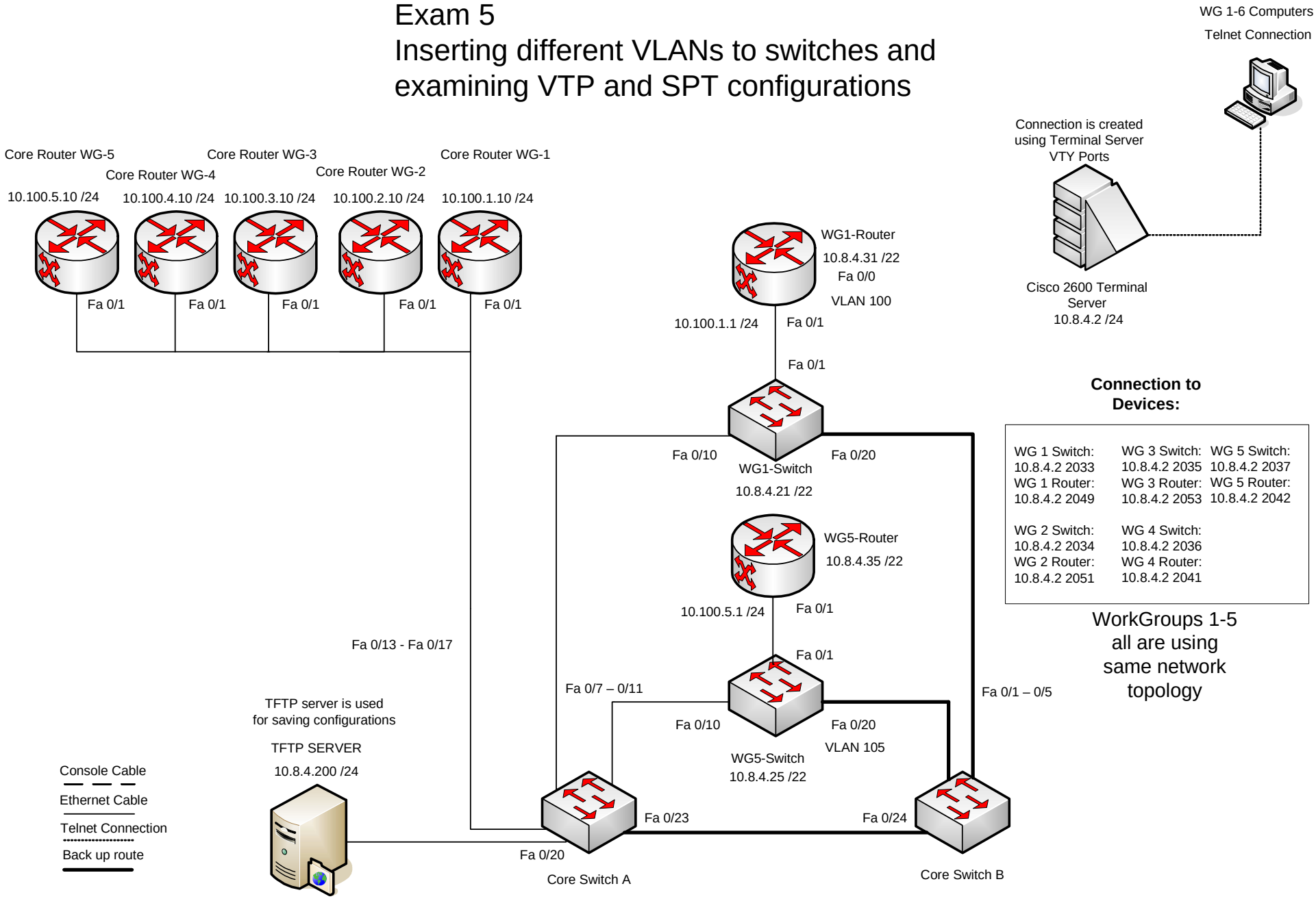
a ip dhcp pool DHCP1 then network 10.100.100.0 255.255.255.0
b ip dhcp pool DHCP1 then network 10.100.100.1
c dhcp pool DHCP1 network 10.100.100.0
d dhcp pool DHCP 1 then network 10.100.100.0 255.255.255.0

Week 4 Exam Question Answers

TASK	STEP	ANSWER
1	7	a) 10.8.4.? b)255.255.252.0 c) 10.8.4.1 d) 10.8.4.1
1	8	enable
1	9	a)wg1router b) cisco c) 10.8.4.? d) 255.255.252.0
1	10	a) configure terminal, interface 0/1
1	11	example ip address 10.8.4.31. 255.255.0.0 for wg 1
1	12	enable
1	13	exit
1	14	no logging console
1	16	example ping 10.8.4.31 for wg 1 / yes reply message show when ping
1	16	command is used to right addresses
2	1	enable ip routing
2	2	a) show ip route b) connected routes which are connected with cables
2	2	c) letters meant that which type of routing protocol is used for routing
2	2	d) only connected routes
2	3	configure terminal
2	4	a) ip route 0.0.0.0 0.0.0.0 10.8.4.1
2	4	b) default route ip address is marked with four zeros
2	4	c) default route ip subnet mask is marked with four zeros
2	4	d) destination address for default router "nearest router"
2	5	a) router rip b) version 2 c) network 10.8.4.0
2	6	exit,exit
2	7	show router table > rip routes is addes to table if there are connected
2	8	a)ping 10.8.4.31 - ping 10.8.4.36 > addresses must be replied if rip
2	8	protocol is running both ends
2	8	b)if ping command is replied destination address must be show at
2	8	the table with rip protocol 2 running
2	8	c) rip 2 is modest version of rip1 and can route to subnetworks
2	9	a) 169…. b) - c) - d) no
2	9	e) network is not working when address begins to 169….
3	2	configure terminal
3	3	dhcp pool DHCP_WG?
3	4	dhcp-config
3	5	example network 10.100.1.0 for wg 1
3	6	default router 10.100.1-5.1
3	7	a)10.100.1-5.1 b)255.255.255.0 c) 10.100.1-5.1 d) 10.100.1-5.1
3	7	e)yes, computer now has ip address f) wg ? router deliveres address
4	1	exit
4	2	copy running-config tftp >10.8.4.200>Ex4Group>confirmation
4	3	no configurations are merged together if there are mixed router
4	3	and switch configurations

Q	**1**	d
Q	**2**	a,d
Q	**3**	b
Q	**4**	d
Q	**5**	a

Exam 5
Inserting different VLANs to switches and examining VTP and SPT configurations



Connection to Devices:

WG 1 Switch: 10.8.4.2 2033	WG 3 Switch: 10.8.4.2 2035	WG 5 Switch: 10.8.4.2 2037
WG 1 Router: 10.8.4.2 2049	WG 3 Router: 10.8.4.2 2053	WG 5 Router: 10.8.4.2 2042
WG 2 Switch: 10.8.4.2 2034	WG 4 Switch: 10.8.4.2 2036	
WG 2 Router: 10.8.4.2 2051	WG 4 Router: 10.8.4.2 2041	

WorkGroups 1-5 all are using same network topology

Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week5

Inserting VLANs and making VLAN Trunking Protocol, and Spanning Tree Protocol configurations

WORKING METHOD

2 people / workgroup max 3 groups

ACTIVITY OBJECTIVES

- Booting up switch and router and making default configurations for devices
- Examining VTP configurations
- Configuring trunk ports
- Configuring VLANs and setting switch port to use different VLANs
- Configuring and testing STP
- Copy configurations to TFTP server

THEORY CONCEPTS

- VTP (VLAN trunk protocol)
- Trunk port
- VLAN
- STP (Spanning Tree Protocol)
- RSTP (Rapid Spanning Tree Protocol)
- EtherChannel

ADVANCE JOBS (exam instructor)

- Ensure that terminal server ports is cleared, when students take connections
- Ensure that switch and router has empty configuration before practise, devices must boot with right configuration.
- Ensure that connection with TFTP server is working
- Ensure that, Core Router configurations are made before exam
- Ensure that Core switch is configured correctly using STP

EXAM JOBS (exam instructor)

- Ensure that VLANs are correctly configured
- Ensure that STP configurations are correctly made to switches
- Ensure that connections between devices are working when testing connections using ping command
- Ensure that configuration files are saved to TFTP server after exam
- Troubleshooting purposes if needed

Exam 5 Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
ping (+) ip-address	privileged	Used for troubleshooting purposes
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup config running config	privileged	Copies running-configuration information from NVRAM to RAM
copy running-config startup config	privileged	Copies running-configuration information from RAM to NVRAM
copy running-config tftp	privileged	Copies configuration from running-config to tftp
copy startup config tftp	privileged	Copies configuration from startup config to tftp
erase startup-config	privileged	erase startup config file
show interfaces (type)	privileged	Displays detail information about interface status
show ip interface brief	privileged	Displays single line info about each interface
show interfaces (id) switchport	privileged	Displays interface adminstrative settings
show vlan (brief,name, summary)	privileged	Displays VLAN information
show vtp status	privileged	Lists VTP configuration and status information
show vtp password	privileged	Lists VTP password
show spanning-tree	privileged	Lists details about STP including port state
show spanning-tree (interface,id)	privileged	Lists STP information only for specified port
show spanning-tree (vlan id)	privileged	Lists STP information only for specified VLAN
show etherchannel (id) (brief,detail,summary)	privileged	Lists information about state of EtherChannel
quit	privileged	exits IOS -system
reload	privileged	reboots the switch
copy tftp startup config	privileged	Copies tftp server configuration to startup-config
copy tftp running-config	privileged	Copies tftp server configuration to running-configuration
telnet (hostname)	privileged	Connects the CLI to another host using telnet
resume	privileged	Resumes connection to suspended host
disconnect	privileged	Disconnects connection to suspended host
vlan database	privileged	Moving to vlan datab. conf.mode also VTP.conf.mode
Cntr+Shift-6 (+) x	keyboard sc	Key sequence to suspend Telnet or SSH connection
show ip route	privileged	Shows routing table information
end	conf.mode	Exits in any conf. mode and goes user mode
exit	conf.mode	Moving back to the next higher mode
enable secret	conf.mode	Sets clear text- password

Command	Mode	Purpose
enable password	conf.mode	Sets automatically encrypted password
ip route 0.0.0.0 0.0.0.0 (+) d.address	conf mode	Defines default IP -route
hostname	conf.mode	Sets switch's hostname
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
line console 0	conf.mode	Moving to console line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
interface vlan (id)	conf.mode	Creates VLAN and moves to VLAN conf. mode
spanning-tree mst configuration	conf.mode	Moving to MST configuration mode
spanning-tree vlan (id) root primary	conf.mode	Changes switch to root switch. Priority is either 24,567 or 4096 lower than current root
spanning-tree vlan (id) root secondary	conf.mode	Changes switch base priority to 28,627
spanning-tree mode (mst, rapid-pvst,pvst)	conf.mode	Enables PVST+ ,PVRTS or MST protocol
username (value) (+) password (value)	conf.mode	Sets username and password required if the login local command is configured
ip routing	conf.mode	Enables IP Routing
no logging console	conf.mode	Disables IOS -logging information
ip default-gateway (+) d.address	conf.mode	Defines default-gateway
login local	line vty conf	Tell IOS to prompt for username and password
ip address (value) (+) mask (value)	line fa conf	Sets ip address and mask for interface
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
switchport mode trunk	line fa conf	Configures the trunking on the interface
switchport trunk allowed vlan (id)	line fa conf	Defines lists of allowed VLANs
switchport access vlan (id)	line fa conf	Configures defined interface into VLANs
switchport trunk encapsulation (dot1q)	line fa conf	Defines dot1q trunking encapsulation to interface
channel-group (id) mode (auto,desirable,on)	line fa conf	Enables EtherChannel on the interface
name (vlan name)	vlan conf	Gives name to specific VLAN
management	vlan conf	Set management VLAN interface
ip address (value) (+) mask (value)	vlan conf	Sets ip address and mask for VLAN
instance (id) (+) vlan (id)	mst conf	Set MST instances
name (value)	mst conf	Gives name to specific mst instance
revision (id)	mst conf	Gives revision number to specific mst instance
vtp domain	vtp.mode	Defines VTP domain name
vtp password	vtp.mode	Defines VTP password
vtp (server,client, transparent)	vtp.mode	Defines VTP mode

TASK 1 Boot up switch and router and make basic configurations for devices.

STEP 1

First task is to build up exam topology that matches topology with exam picture. Every group must show own coupling to administrator and check it is acceptable before continuing.

STEP 2

From your PC, Open connection to terminal server.

STEP 3

Take connection your switch. (Check terminal server IP address and port number with a picture included)

STEP 4

Configure switch IP address, Subnet Mask, enable password, VTY line password and hostname.

Use enable secret password "**cisco**", enable password "**sanfran**" hostname "**switch WG-?**" where "?" is your group number. You can use Cisco configuration dialog or configure settings manually. (Addresses and masks are in a picture)

STEP 5

When switch basic configurations are done, take other connection to your router and make router basic configurations. Configure router enable password, vty password and router hostname.

Use password "**cisco**" enable password "**sanfran**" hostname "**router WG-?**" where "?" is your group number. You can use Cisco configuration dialog or configure setting manually. (Addresses and masks are in a picture)

STEP 6

Configure IP routing for router

STEP 7

Enter command that disables console messages from switch and router IOS - screens.

TASK 2 Examine VTP (VLAN Trunk Protocol) information and VTP domains

STEP 1

Change to switch connection and show VTP information on your switch. What kind of information Cisco VTP gives you?

Collect information below:

VTP Domain name:

VTP VLAN Support:

VTP Operating Mode:

VTP password (if configured):

How switch get other switches VLAN information at present operating mode?

What is best operating mode, when doing lab exercises, where configurations are changing all the time?

STEP 2

Ensure that switch VLAN database is changed to that mode. If mode is some other go to VTP configuration mode and change switch operating mode to right mode. What is right command that changes switch VTP mode?

STEP 3

What is the meaning of VTP pruning? How VTP pruning improves network traffic?

TASK 3 Configure switch interfaces to trunk mode

STEP 1

Keep connection at your switch and move to interface configuration mode.

STEP 2

Move to FA interface 0/10 configure mode.

STEP 3

Set the port FA 0/10 to trunk mode. What is right command for that?

What is meaning of trunk port?

Set on port FA 0/10.

STEP 4

Go back to privileged mode and check trunk configuration from interface FA 0/10. What is trunk port encapsulation type?

STEP 5

Move to interface FA 0/10 configuration mode and change port FA 0/10 encapsulation type to “dot1q”.

What is right command for that?

STEP 6

Set the port FA 0/20 to trunk mode and set port encapsulation type to “dot1q” but don’t enable port keep it shut down. What is right command to disable port if it is set on?

STEP 7

Go back to privileged mode and check both interfaces trunk configuration.

What VLANs trunk port allowed, when it is configured with default settings?

STEP 8

There are four different trunking methods available. What are those trunking modes called?

STEP 9

When two switches are connected together and other switch trunk port is conconfigured for dynamic auto mode and other trunk port is configured for access mode. What is trunk configuration between switches at this kind of situation?

TASK 4 Configure VLANs on the switch

STEP 1

Keep connection at your switch and move to global configuration mode.

STEP 2

Using the exam VLAN chart create VLAN "?" on your switch, where "?" means VLAN number on the chart between "100-104".

What is right command to create VLAN on your switch?

STEP 3

Give description "WG?-VLAN to your created VLAN. Where "?" is your workgroup number.

STEP 4

Go back to privileged mode and show VLAN information on your switch?

What VLANs is configured on your switch?

What VLAN information "show vlan brief" command gives you?

What is default VLAN number?

Is there any ports configured to use default VLAN?

STEP 5

What is right command to configure management VLAN?

STEP 6

Go to interface FA 0/1 configure mode and set port FA 0/1 to use created VLAN. What is right command for that?

STEP 7

Move back to global configuration mode and move then to VLAN 8 configuration mode. When you are at the VLAN 8 configuration mode set IP address and mask for VLAN 8 (look at the picture) then set VLAN 8 interface to work management interface. Write commands below:

STEP 8

Go back to privileged mode and give instructor to verify your configurations.

STEP 9

Change connection to your router.

STEP 10

Go to interface FA 0/1 configuration mode.

STEP 11

Change interface FA 0/1 IP address and subnet mask to match with the given addresses in a picture.

STEP 12

Set on router port FA 0/1.

STEP 13

Add default route from your workgroup router to point core router address. What is right command to set default route from workgroup to core?

What is meaning of default route?

STEP 14

Add then default gateway from your workgroup switch to point core router address. What is right command to set default gateway?

STEP 15

Ensure that connections work and ping core router address from your workgroup router using ping command.

TASK 5 Configure and testing STP (Spanning Tree Protocol) on your switch

STEP 1

Change connection back to your switch.

STEP 2

Move to privileged mode.

STEP 3

Show switch running-configuration and ensure that switch interfaces FA 0/10 and FA 0/20 is property configured for trunking.

STEP 4

Move to interface FA 0/20 mode.

STEP 5

Set on port FA 0/20.

STEP 6

Go back to privileged mode.

STEP 7

Show spanning-tree information on your switch.

Which five operational states port has when STP is working?

STEP 8

Show spanning tree information on your VLAN?

Which ports are now in the forwarding state for the VLAN?

Which ports are now in the blocking state for the VLAN?

Which switch is functioning root bridge for the STP?

How STP chooses which switch is functioning root? What is priority of the root bridge?

STEP 9

Change connection to your router.

STEP 10

Move to privileged mode and ping core router address with extended ping command. (repeat count must be over 20000) What is right command for that?

_____

Is ping command successful? (if continuous ping replies are coming from the core router, ping command is successful)

_____

If the ping is successful, move to switch connection. (if not contact you instructor)

STEP 11

Move to interface FA 0/10 configuration mode and shutdown interface. What happened to the extended ping?

_____

If nothing happened, enable interface FA 0/10 and move to interface FA 0/20 configuration mode and shutdown that interface?

_____

Is the ping command successful after 30 seconds?

_____

How STP chooses which port to shutdown?

_____

_____

STP protocol -port roles are Root port and Designated Port.
RSTP (Rapid Spanning tree) Port roles differ from STP, what are RSTP protocol five port roles?

_____

_____

_____

_____

_____

STEP 12

What is MSTP protocol and STP protocol difference? How MSTP protocol areas must be configured?

STEP 13

What does STP optimal feature EtherChannel?

TASK 6 Saving switch and router configuration to TFTP server

STEP1

Keep connection at your switch and move to privileged mode.

STEP 2

Final task is copy router and switch configurations to TFTP server. In a privileged mode, type right command, that copies your configuration file to TFTP server.
(Image file name and IP address are found at the picture)

STEP 3

Change to switch connection.

STEP 4

Move to privileged mode.

Enter right copy command below.

Use following image file name: "**Ex5_SW_Group?"** where "?" is your workgroup number.

STEP 5

Change to router connection.

STEP 6

Move to privileged mode.

STEP 7

Copy router configuration from WG router to TFTP server using following image file name: "**Ex5_RO_Group?"** where "?" is your workgroup number.

STEP 8

At the final task is to remove interfaces VLAN configurations. Every group removes group own VLAN that is created earlier. What is right command to remove interface from using specific VLAN?

Week 5 Exam Revision Questions

1 Which of the following VTP modes allow VLANs to be configured on a switch?

a Client
b Server
c Transparent
d Dynamic
e None

2 Which of the following command list operationnal state of interface fa 0/1 in regard to VLAN trunking?

a show interfaces fa 0/1
b show interfaces fa 0/1 switchport
c show interfaces fa 0/1 trunk
d show trunks

3 Which of the terms best equates to the term VLAN?

a Collision domain
b Broadcast domain
c Subnet domain
d Single switch
e Trunk

4 Which of the following adds the trunking header for all VLANs expect one?

a VTP
b ISL
c 802.1Q
d Both ISL and 8021Q
e None

5 If switch has three configured VLANs. How many IP subnets are required assuming that all hosts in all VLANs want to use TCP/IP?

a 0
b 1
c 2
d 3
e you can't tell from the information provided

6 Which of the following are transitory IEEE 802.1d port states used only during the process of STP convergence?

a blocking
b forwarding
c listening
d learning
e discarding

7 Which of the following bridge ID would win election as root, assuming that the switches with these bridge Ids were in the same network?

a 32768:0200.1111.1111
b 32768:0200.2222.2222
c 200:0200.1111.1111
d 200:0200.2222.2222
e 25,000:0200.1111.1111

8 Which of the following RSTP port states have the same name as a similar port state in traditional STP?

a blocking
b forwarding
c listening
d learning
e discarding
f disable

Week 5 Exam Question Answers

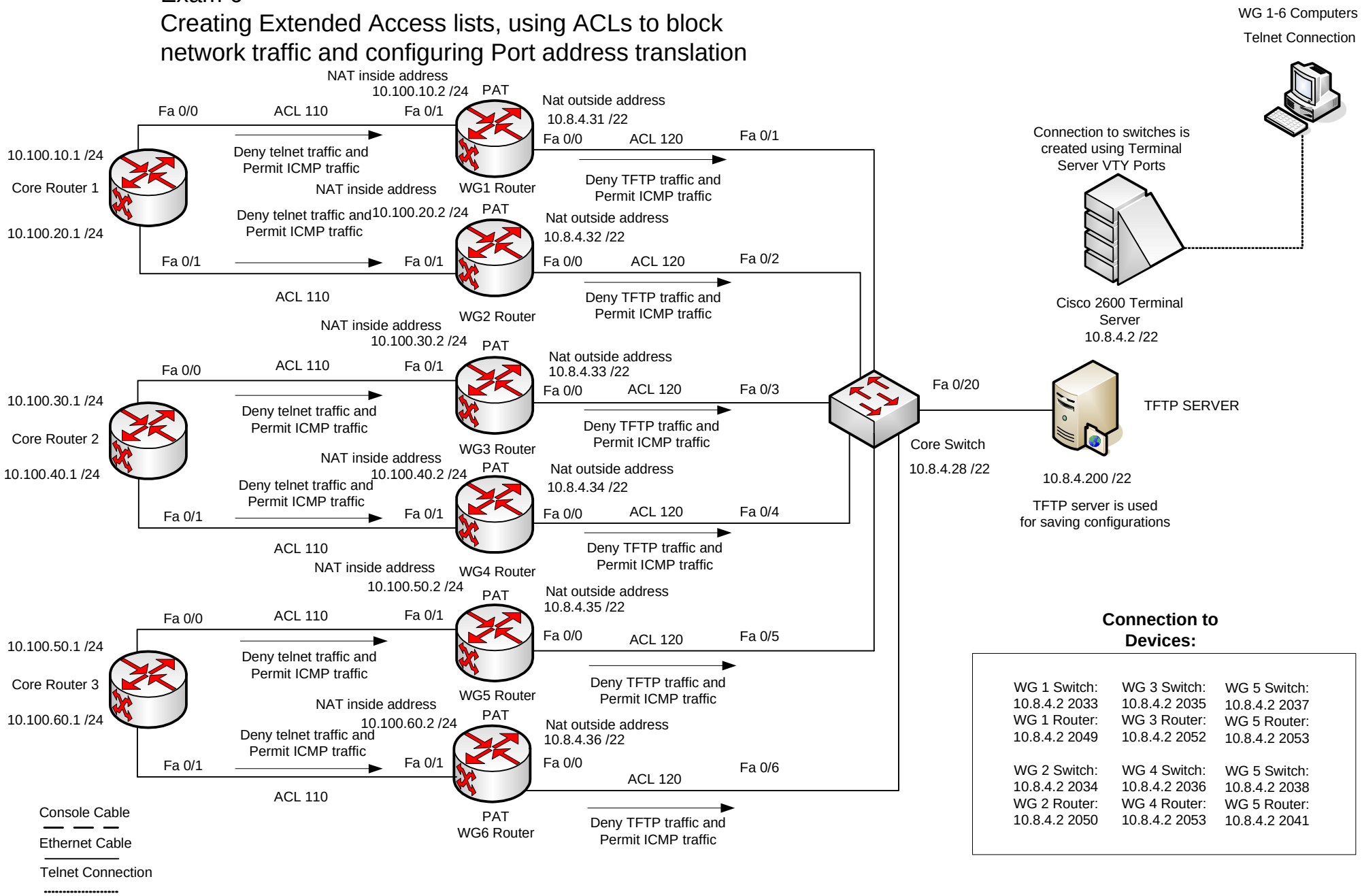
TASK	STEP	ANSWER
2	1	a)it shows trunking information between switches, how switches
2	1	advertises VLAN information
2	1	b) c) d) e) f)vtp server switch g)vtp transparent
2	2	vtp transparent
2	3	VTP pruning prevent broadcasting to switches that do not contain a VLANs
2	3	and it increase network available bandwidth by restricting flooded traffic
3	3	a)switchport mode trunk b)trunk port allowes all VLANs to go through,
3	3	specified VLANs can also configure separately c) no shutdown
3	4	-
3	5	switchport trunk encapsulation dot1q
3	6	switchport mode trunk, trunk encapsulation dot1q, disable
3	7	only VLAN 1 (default VLAN)
3	8	Access,Trunk,Dynamic desirable and Dynamic auto
3	9	Link is configured Access link mode
4	2	VLAN 100-104 (global configuration command) or just add port to
4	2	VLAN that user wants to use
4	3	name WG1-VLAN
4	4	a) b) c)default vlan is vlan 1 d)
4	5	management command (VLAN configure mode)
4	6	a) enable b) switchport access vlan 1
4	7	a) interface vlan 8 b)management
4	11	ip address example 10.100.0.1 WG 1
4	12	enable
4	13	ip route 0.0.0.0 0.0.0.0 "core router address"
4	13	with default route router knows where route to packet if address is
4	13	unknown
4	14	ip default gateway "core router ip address"
4	15	ping "core router ip address"
5	5	enable
5	7	a)show spanning-tree
5	7	b)blocking,listening,learning,forwarding,discarding
5	8	a)show spanning-tree vlan 100 >WG1 104> WG5
5	8	b) c) d) e)root port is port that has lowest bridge ID value
5	10	a)ping "core router address" repeat 20000
5	10	b)yes / no
5	11	a)shutdown, ping stops
5	11	b)shutdown
5	11	c)yes
5	11	d)spt blocs all ports that is not used for forwarding frames
5	11	e)root port,designated port,alternative port,backup port and disabled

TASK	STEP	ANSWER
5	**12**	MSTP -protocol uses separate ares to forward traffic
5	**12**	separate instances must be created for MSTP also
5	**12**	every instance must be configured to use specific mapped VLANs
5	**13**	etherchannel combines multiple paraller segments of equal speed
5	**13**	between the same pair of switches
6	**3**	copy running-configuration tftp > 10.8.4.200 >ex5_SW_Group1
6	**6**	copy running-configuration tftp > 10.8.4.200 >ex5_RO_Group1
6	**8**	no switchport access vlan id
Q	**1**	b,c
Q	**2**	b,c
Q	**3**	b
Q	**4**	c
Q	**5**	d
Q	**6**	c,d
Q	**7**	c
Q	**8**	b,d

Liite 14

Exam 6

Creating Extended Access lists, using ACLs to block network traffic and configuring Port address translation



Connection to Devices:

WG 1 Switch:	WG 3 Switch:	WG 5 Switch:
10.8.4.2 2033	10.8.4.2 2035	10.8.4.2 2037
WG 1 Router:	WG 3 Router:	WG 5 Router:
10.8.4.2 2049	10.8.4.2 2052	10.8.4.2 2053
WG 2 Switch:	WG 4 Switch:	WG 5 Switch:
10.8.4.2 2034	10.8.4.2 2036	10.8.4.2 2038
WG 2 Router:	WG 4 Router:	WG 5 Router:
10.8.4.2 2050	10.8.4.2 2053	10.8.4.2 2041

Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week6

Creating Extended Access lists, using ACLs to block network traffic and configuring Port address translation

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- Getting configurations from TFTP server
- Creating static routes between workgroup and core
- Creating Extended Access lists
- Configuring Access lists to block inside and outside traffic
- Configuring Port address translation
- Copy configurations to TFTP server

THEORY CONCEPTS

- Default route
- Static route
- Routing table
- Extended Access list
- Standard Access list
- Network address translation (NAT)
- Port address translation (PAT)

ADVANCE JOBS (exam instructor)

- Ensure that terminal server ports is cleared, when students take connections
- Ensure that connection to TFTP server is working before practise and server IP address is changed
- Ensure that configuration images are located from TFTP server and file names are correct
- Ensure that, Core Routers configurations are made before exam

EXAM JOBS (exam instructor)

- Ensure that connections between devices are working when testing connections using ping command
- Ensure that ACLs configurations are correctly made
- Ensure that ACLs 110 and 120 is placed right port and right direction
- Ensure that configuration files are saved to TFTP server after exam
- Troubleshooting purposes if needed

Week 6 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup-config	privileged	Copies running-configuration information
running config		from NVRAM to RAM
copy running-config	privileged	Copies running-configuration information
startup config		from RAM to NVRAM
erase startup-config	privileged	erase startup config file
ping (ip-address)	privileged	Used for troubleshooting purposes
quit	privileged	exits IOS -system
reload	privileged	reboots the switch
copy tftp startup config	privileged	Copies tftp server configuration to startup-config
copy tftp running-config	privileged	Copies tftp server configuration to running-configuration
copy running-config tftp	privileged	Copies configuration from running-config to tftp -server
copy startup config tftp	privileged	Copies configuration from startup config to tftp -server
telnet (+) hostname	privileged	Connects the CLI to another host using telnet
resume	privileged	Resumes connection to suspended host
disconnect	privileged	Disconnects connection to suspended host
show ip route	privileged	Shows routing table information
show access-lists	privileged	Shows details of configured access lists for all protocols
show ip access-list	privileged	Shows IP access lists
show ip nat statistics	privileged	List counters for packet and NAT table entries
show ip nat translations	privileged	Displays the NAT table
login local	line vty conf	Tell IOS to prompt for username and password
username (value)	conf.mode	Sets username and password required
password (value)		if the login local command is configured
exit	conf.mode	Moving back to the next higher mode
end	conf.mode	Exits in any conf. mode and goes user mode
line console 0	conf.mode	Moving to console line conf.mode
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
enable secret	conf.mode	Sets clear text- password
enable password	conf.mode	Sets automatically encrypted password
hostname	conf.mode	Sets switch's hostname
ip route 0.0.0.0 0.0.0.0 (+)	conf.mode	Defines default IP -route
d.address		

Command	Mode	Purpose
ip route(+)destination nw ip(+) source ip	conf.mode	Defines static route
access-list value(+)type(+) source ip (+)source wc mask (+)logging	conf mode	Creates standard access list use numbers 1-99 and 1300-1999
access-list value(+)type(+) protocol(+)source ip (+) source wc mask(+)destination ip (+) destination wc mask(+) logging	conf.mode	Creates extended access list use numbers 100-199 and 2000-2699
access-list value(+)type(+) source ip (+)source wc mask (+)logging	conf.mode	Creates standard access list use numbers 1-99 and 1300-1999
ip nat pool (+) name (+)1 addr (+)2 addr(+)mask	conf.mode	Defines IP NAT pool
ip nat inside source list (value) (+) interface (value) overload	conf mode	Enables NAT globally referencing to ACL that defines which source addresses to NAT and the interface or pool which to find global addresses
ip nat inside	line fa conf	Defines IP NAT inside interface
ip nat outside	line fa conf	Defines IP NAT outside interface
ip access-group value (+) in / out	line fa conf	Configures specific ACL to use that interface
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
ip address (+) mask	line fa conf	Sets ip address and mask for interface
ip access-group value (+) in / out	line fa conf	Configures specific ACL to use that interface
Cntr+Shift-6, x	keyboard sc	Key sequence to suspend Telnet or SSH connection

TASK 1 Getting exam configurations from TFTP server

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take connection your router. (Check terminal server IP address and port number with a picture included)

STEP 3

Go to privileged mode and copy router saved configuration image from TFTP server to router startup-configuration.

STEP 4

Boot up router. What is right command to boot-up router.

STEP 5

Show running-configuration from router and check if configuration is applied correctly?

STEP 6

Next task is to build up exam topology that matches topology with exam picture. Every group must show own coupling to administrator and check it is acceptable before continuing.

TASK 2 Create static routes between workgroups and core router

STEP 1

Change connection to WG router.

STEP 2

Move to privileged mode.

STEP 3

Show router routing table information.

STEP 4

What routes are listed on a table?

STEP 5

Move to interface FA 0/0 configuration mode.

STEP 6

Change interface IP address and subnet mask (check addresses for the picture)

STEP 7

Set on interface FA 0/0 if interface is shut down.

STEP 8

Move to interface FA 0/1 configuration mode.

STEP 9

Change interface IP address and subnet mask (check addresses for the picture)

STEP 10

Set on interface FA 0/1 if interface is shut down.

STEP 11

Move to privileged mode.

STEP 12

Show router routing table information.

What routes are listed on a table?

STEP 13

Move to global configuration mode.

STEP 14

What is right command to add default route.

STEP 15

Insert default route to Core router.

What is right command to add static route.

STEP 16

Insert static route to neighbouring workgroup router

STEP 17

Move to privileged mode and show router routing table information.

What routes are listed on a table?

STEP 18

Ping the neighbouring workgroup WG router. (check address for the picture)

Ping the core router. (check address for the picture)

Ping core switch address (check address for the picture)

Ping commands should work if static route and default router are configured correctly.

TASK 3 Configure access lists to control traffic in and out from router and saving configurations

STEP 1

Move to global configure mode.

STEP 2

Create IP extended access list 110 to deny telnet traffic and allow ICMP traffic from WG router to core router.

STEP 3

What is right command to show content of ACL 110? Show content of extended ACL 110.

STEP 4

What is difference between standard and extended list?

STEP 5

What is difference between creating ACL and applying ACL to interface?

STEP 6

Move to interface FA 0/1 configuration mode.

STEP 7

Apply created access list 110 to FA interface 0/1.

STEP 8

Should extended ACL 110 be applied as an input or output ACL?

STEP 9

Go back to privileged mode. Show running-configuration and verify that ACL 110 is applied to the FA 0/1 interface?

STEP 10

Ask parent group to ping your WG router FA 0/1 IP address? Did they get reply?

STEP 11

Ask parent group to take telnet connection your WG router FA 0/1 IP address? Can they get telnet connection work?

TASK 4 Configure Port address translation (PAT)

STEP 1

Move to global configuration mode.

STEP 2

Create extended access list 120 to deny TFTP traffic and allow ICPM traffic from parent WG router to TFTP server. Enable also information logging feature for access list 120.

STEP 3

Show content of extended ACL 120.

STEP 4

Move to FA 0/0 configure mode and configure interface to work NAT outside interface.

STEP 5

Move to FA 0/1 configure mode and configure interface to work NAT inside interface.

STEP 6

Move to global configuration mode.

STEP 7

Configure Port address translation (PAT) which uses ACL 120 and interface FA 0/0 to overloading addresses.

STEP 8

Move to global configuration mode

STEP 9

Ask parent group to ping TFTP server address, that you get traffic between PAT configured WG routers. Did you get reply?

Why ping command is successful or not?

STEP 10

Ask parent group to copy running configuration to TFTP server address, is copy process successful?

Why copy process is successful or not?

STEP 11

Show PAT table information and statistics. What is WG NAT inside local address, when PAT is configured?

What is WG NAT outside global address, when PAT is configured?

_____

TASK 5 Copy configuration files to TFTP server

STEP 1

Final task is copy your configurations to TFTP server. Type command that copy router configuration to TFTP server. (Image filename and IP address is found at the picture)

STEP 2

Copy configuration from router to TFTP server using following image file name: "**Ex6_RO_Group?"** where "?" is your workgroup number.

STEP 3

Enter right copy command below.

_____

Week 6 Exam Revision Questions

1 Which of the following must be true before IOS lists a route "S" in the input of as show ip route command?

a The ip address must be configured on an interface
b The router must receive a routing update from a neighboring router
c The ip route command must be added to the configuration
d The ip address command must be use the special keyword
e The interface must be up and up

2 Which of the following command correctly configures a static route?

a ip route 10.1.1.0 255.255.255.0 10.1.1.1
b ip route 10.1.1.0 fast ethernet 0
c ip route 10.1.1.0 /24 10.1.1.1.253
d ip route 10.1.1.0 /24 fast ethernet 0

3 Which of the following wildcard masks is most useful for matching all IP packe in subnet 10.1.128.0, mask 255.255.255.0?

a 0.0.0.0
b 0.0.0.31
c 0.0.0.240
d 0.0.15.0
e 0.0.248.255

4 Which of the following fields cannot be compared based on an extended IP ACL?

a Protocol
b Source IP address
c Destination IP address
d TOS byte
e URL
f filename for FTP transfers

5 Which of the following ACL commands permits traffic that matches packets from host 10.1.1.1 to all web servers whose ip address begin with 172.16.5?

a access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
b access-list 1950 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
c access-list 2550 permit ip host 10.1.1.1 eq www 172.16.5.0 0.0.0.255 www
d access-list 2550 permit tcp host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
e access-list 2550 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www

Week 6 Exam Question Answers

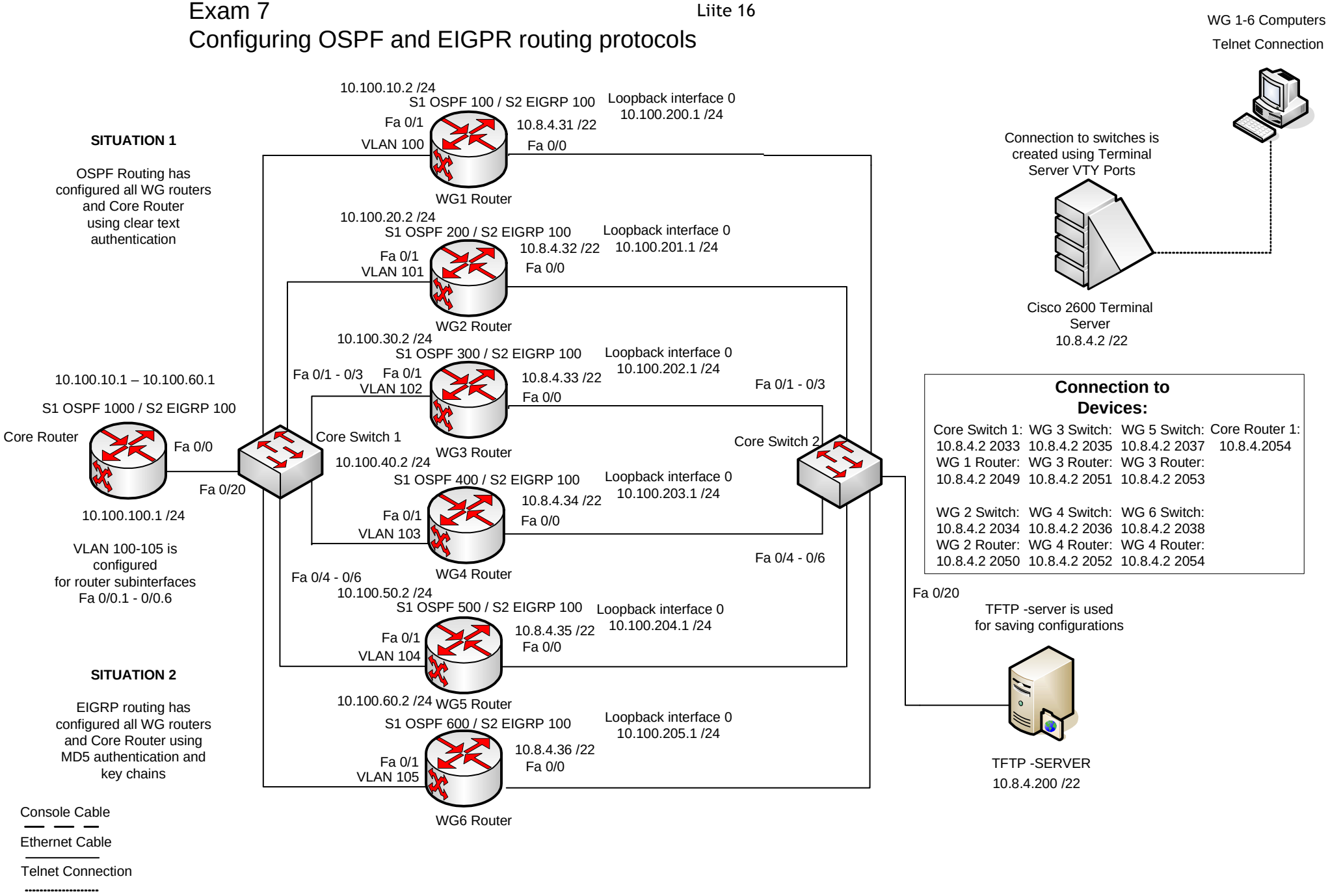
TASK	STEP	ANSWER
1	4	reload
1	6	show running-configuration
2	3	show ip route
2	4	only connected routes are listed on the table ("C") fa 0/1 (last exam)
2	12	interface fa 0/0 address and fa 0/1 address is connected ("C")
2	14	ip route 0.0.0.0 0.0.0.0 (+) "destination address"
2	15	a)ip route 0.0.0.0 0.0.0.0 (+) "core router ip address"
2	15	b)ip route(+)destination network address(+)subnet mask(+)source address
2	16	ip route other wg network address (+) network mask (+) wg router address
2	17	directly connected routes ("C") and new static routes ("S")
2	18	a)ping "wg router ip address"
2	18	b)ping "core router ip address"
2	18	c)ping "core switch ip address"
3	2	access-list 110 deny tcp wg router address(+)wg router wildcard mask(+)
3	2	core router address(+)core router wildcard mask(+) eq 23
3	2	access-list 110 permit icmp any any
3	3	show access lists 110
3	4	standard list is simplier than extended list in consist only target network
3	4	parameters extended list consist of source and destination network parameters
3	5	when creating ACL it consist only list rules and parameters
3	5	when list is applied to interface and target direction is defined
3	5	ACL start to block network traffic
3	7	ip access-group 110 in
3	8	inside traffic
3	10	ping "wg-router fa 0/1 ip address"
3	11	telnet "wg-router fa 0/1 ip address"
4	2	access-list 120 deny udp any host 10.8.4.200 eq 69 (+)log
4	2	access-list 120 permit icmp any any
4	3	show access lists 120
4	4	ip nat outside
4	5	ip nat inside
4	7	ip nat inside source list 120 interface FA 0/0 overload
4	9	ping "tftp server address"
4	9	ping process is succesfull, because ACL 120 permits icmp traffic
4	10	copy running-configuration tftp >10.8.4.200>test
4	10	copy process in not successfull, because ACL 120 denies TFTP traffic
4	11	show ip nat statistics / show ip nat translations
4	11	inside local address 10.100.10.2 - 10.100-60.2
4	11	outside global 10.8.4.31 - 10.100.10.36
5	3	copy running-configuration tftp >TFTP -server address>Ex6_RO-Group

Q	**1**	c
Q	**2**	a
Q	**3**	d
Q	**4**	e,f
Q	**5**	a,e

Exam 7

Liite 16

Configuring OSPF and EIGPR routing protocols



Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week7

Configuring Open Shortest Path First, OSPF and Enchanted Interior Gateway Routing Protocol, EIGRP

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- Getting configurations from TFTP server
- Removing old configurations
- Configuring OSPF routing
- Monitoring OSPF routing
- Configuring EIGRP routing
- Monitoring EIGRP routing
- Copy configurations to TFTP server

THEORY CONCEPTS

- EIGRP routing protocol
- OSPF routing protocol

ADVANCE JOBS (exam instructor)

- Ensure that terminal server ports is cleared, when students take connections
- Ensure that connection to TFTP server is working before practise and server IP address is changed
- Ensure that configuration images are located from TFTP server and file names are correct
- Ensure that, Core Router configurations are made before exam

EXAM JOBS (exam instructor)

- Ensure that OSPF routing protocol is configured correctly to WG routers
- Ensure that EIGRP routing protocol is configured correctly to WG routers
- Ensure that connections between devices are working when testing connections using ping command
- Ensure that configuration files are saved to TFTP server after exam
- Troubleshooting purposes if needed

Week 7 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup-config	privileged	Copies running-configuration information
running config		from NVRAM to RAM
copy running-config	privileged	Copies running-configuration information
startup config		from RAM to NVRAM
erase startup-config	privileged	Erase startup config file
ping (+) ip-address	privileged	Used for troubleshooting purposes
quit	privileged	Exits IOS -system
reload	privileged	Reboots the switch
show ip protocols	privileged	Show routing protocol parameters and timer values
show ip route ospf	privileged	Lists OSPF routes in the routing table
show ip ospf interface	privileged	Lists OSPF area interface information
show ip ospf neighbor	privileged	Lists interface neighbors status information
debug ip ospf events	privileged	Logs messages for each OSPF packet
debug ip ospf packet	privileged	Logs messages for content of all OSPF packets
debug ip ospf hello	privileged	Logs messages for Hello and Hello failures
show ip route eigrp	privileged	Lists OSPF routes in the routing table
show ip eigrp neighbors	privileged	Lists EIGRP neighbors and status
show ip eigrp topology	privileged	Lists content of the EIGRP topology table
show ip eigrp traffic	privileged	Lists statistics of the EIGRP send and receive messages
debug ip eigrp	privileged	Displays content of EIGRP packets specifally for IP
debug eigrp fsm	privileged	Displays changes to the EIGRP success and feasible successor routes
copy tftp startup config	privileged	Copies tftp server configuration to startup-config
copy tftp running-config	privileged	Copies tftp server configuration to running-configuration
copy running-config tftp	privileged	Copies configuration from running-config to tftp -server
copy startup config tftp	privileged	Copies configuration from startup config to tftp -server
telnet (hostname)	privileged	Connects the CLI to another host using telnet
resume	privileged	Resumes connection to suspended host
disconnect	privileged	Disconnects connection to suspended host
show ip route	privileged	Shows routing table information
Cntr+Shift-6, x	keyboard sc	Key sequence to suspend Telnet or SSH connection
exit	conf.mode	Moving back to the next higher mode
end	conf.mode	Exits in any conf. mode and goes user mode
line console 0	conf.mode	Moving to console line conf.mode
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
enable secret	conf.mode	Sets clear text- password
enable password	conf.mode	Sets automatically encrypted password

Command	Mode	Purpose
hostname	conf.mode	Sets switch's hostname
interface loopback	conf.mode	Defines loopback interface to OSPF -routing protocol
router ospf (+) id	conf.mode	Enters OSPF configuration mode
router eigrp (+) system number	conf.mode	Enters EIGRP configuration mode
ip route 0.0.0.0 0.0.0.0 (+) mask+destination address	conf.mode	Defines default IP -route
key chain (+) name	conf.mode	Create and name an authentication key chain
username (value)	conf.mode	Sets username and password required
password (value)		if the login local command is configured
interface fastethernet (+) sub interface	conf mode	Enters router subinterface configuration mode
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
ip address (+) mask	line fa conf	Sets ip address and mask for interface
swithport address vlan (+)value	line fa conf	Sets switch interface to use specific VLAN
login local	line vty conf	Tell IOS to prompt for username and password
network(+)interface address(+) wcmask(+)area id	OSPF conf	Enables OSPF interfaces matching the address and wcard combination and sets OSPF area
network(+)network address(+) wcmask	EIGRP conf	Enables EIGRP to all interfaces matching the address and wcard combination
ip ospf authentication(+)key password (value)	line fa conf	Sets OSPF authentication key if simple key authentication is used
ip authentication key-chain eigrp(+)value(+)chain-name	line fa conf	References the key chain used for MD5 authentication with EIGRP
ip authentication mode eigrp(+) value(+)md5	line fa conf	Enables EIGRP MD5 authentication for all neighbors reached on this interface
key(+)value	kchain mode	Create a new password key number
key-string(+)text	kchain mode	Creates the authentication key's value
accept lifetime(+)start time(+) end time	kchain mode	Set the time frame during which a router will accept the use of particular key
send lifetime(+)start time(+) end time	kchain mode	Set the time frame during which a router will send EIGRP messages using a particular key
encapsulation dot1q (+) vlan value	subinterface conf	attach subinterface for specific vlan
ip address (+) mask	subinterface conf	Sets ip address and mask for sub interface

TASK 1 Get exam configurations from TFTP server

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take connection your router. (Check terminal server IP address and port number with a picture included)

STEP 3

Go to privileged mode and copy router saved configuration image from TFTP server to router startup-configuration.

STEP 4

Boot up router. What is right command to boot-up router.

STEP 5

Show running-configuration from router and check if configuration is applied correctly?

STEP 6

Next task is to build up exam topology that matches topology with exam picture. Every group must show own coupling to administrator and check it is acceptable before continuing.

TASK 2 Remove old configurations from WG router and set up new IP addresses

STEP 1

Take connection to WG router.

STEP 2

Go to privileged mode.

STEP 3

Show router table information.

STEP4

What routes are marked on a table?

STEP5

Go to global configuration mode.

STEP6

Take off ACL 120 from router. What is right command to remove Access List?

STEP7

Remove Port Address Translation from router and PAT inside port and outside port settings.

STEP8

Take off all static routes that are marked with character ”S”. Go to global configuration mode and use command that removes static routes. Routes must be removed one by one. What is right command to remove static route?

STEP9

Go to interface FA 0/0 configuration mode and remove IP address from the interface.

STEP10

Set new IP address and mask to interface 0/0. Check right address from the picture.

STEP11

Set on interface.

STEP12

Go to interface FA 0/1 configuration mode and remove IP address from the interface.

STEP13

Set new IP address and mask to interface 0/1. Check right address from the picture.

STEP14

Insert default route from WG router to Core router workgroup VLAN sub interface

---

STEP15

Set on interface.

STEP16

Go back to privileged mode and show running-configuration from router.

TASK 3 Create route to other workgroup using OSPF routing protocol

STEP 1

Keep connection to WG router and move to global configuration mode.

STEP 2

Configure loopback interface for WG router.

STEP 3

What is right command to create loopback interface?

What is meaning of loopback interface?

STEP 4

Set IP address and subnet mask for loopback interface.

STEP 5

Set on loopback interface.

STEP 6

Configure OSPF routing protocol for WG router. Set OSPF protocol to advertise workgroup own network using interfaces FA 0/0, FA 0/1 and loopback interface. Interfaces must be configured to use OSPF area 0. When configuring subnet mask, it must be typed to wildcard mask format. (look for the picture to get right configurations)

Insert commands below:

STEP 7

Go back to privileged mode and show routing table information. What routes and routing protocols router is using now?

STEP 8

Show IP OSPF neighbours command to display neighbour information, what other routers are using OSPF protocol?

What different purpose of use is router that has configured Area Border router (ABR) or router that has configured internal router?

What is meaning of Backbone Area? (Area 0)

STEP 9

Take connection to Core-switch 1 and change interface that are connected to your group router for VLAN 100-105 depending your group number.

STEP 10

Take connection to Core-router and create sub interface FA 0/0.1 - FA 0/0.5 depending your group number.

STEP 11

Attach sub interface for your group VLAN and create IP address for sub interface (look at the picture for right address)

STEP 12

Switch connection back to WG router and show OSPF protocol parameters. What is right command for that?

What kind of packets OSPF protocols sends to each other? Find command that display this kind of information?

STEP 13

Configure OSPF authentication for interface FA 0/1 using Clear text. Use password “cisco” for authentication.

Show information about authentication. Find command that displays information about authentication method?

STEP 14

Change connection to core router and configure OSPF authentication also for your group network. (Core router interface FA0/0.?)

STEP 15

Change connection back to WG-router and ping the core router address. Did you get reply?

Ping other WG router address, is the ping command successful?

If workgroup 1 is using OSPF protocol and other workgroup is using other routing protocol. Can ping command get reply to other network?

STEP 16

Move to WG router interface configure mode and change OSPF protocol password to key-sanfran.

STEP 17

Ping the other workgroup router address. Did you get reply?

STEP 18

Disable OSPF routing for WG router and core router.

TASK 4 Create route to other workgroup using EIGRP routing protocol

STEP 1

Keep connection to WG router and move to global configuration mode.

STEP 2

Configure EIGRP routing protocol for WG router. Set EIGRP protocol to advertise workgroup own network. When configuring subnet mask, must be typed wildcard mask format. All groups must use same autonomous system number. (Look for the picture to get right configurations)

Insert commands below:

STEP 3

Go back to privileged mode and show routing table information. What routes and routing protocols router is using now?

STEP 4

Show IP EIGRP neighbours -command to display neighbours information what other routers are using EIGRP protocol?

STEP 5

Show content of the EIGRP topology table. What difference is successor and feasible successor routes?

STEP 6

Show EIGRP traffic. What is right command for that?

STEP 7

What kind of packets EIGRP protocols sends to each other? What are the right commands to find that?

STEP 8

Configure EIGRP authentication for interface FA 0/1 using key chain “basic keys”: Use following information:

Key Chain basic keys

key 1

key-string pete

accept -lifetime “this day” – “one week for this day”
send -lifetime “this day” – “one week for this day”

key 2

key-string john

accept lifetime “one week for this day – 1 day” – “one month for this day”
send -lifetime “one week for this day – 1 day” – “one month for this day”

Write command below to create authentication:

STEP 9

Change connection to core router and configure EIGRP authentication also for your group network. (Core router interface FA0/0.?)

STEP 10

Ping the core router address.

Ping the workgroup 2 router address, is the ping command successful?

STEP 11

Take off key-string pete for WG router and try then ping other WG router and core router. Did you get reply?

STEP 12

Notify instructor that authentication key is removed. Then instructor can check that EIGRP neighbourhood is not longer valid.

STEP 13

Disable EIGRP routing for WG router and core router

STEP 14

Which is the better way to configure authentication at a real life situation?

TASK 5 Copy configuration files to TFTP server

STEP 1

Final task is copy your configurations to TFTP server Type command that copy router configuration to TFTP server. (Image filename and IP address is found at the picture).

STEP 2

Move to privileged mode.

STEP 3

Copy configuration from router to TFTP server

Use following image file name: "**Ex7_RO_Group?"** where "?" is your work-group number.

Week 7 Exam Revision Questions

1 Which of the following affects the calculation of OSPF routes when all possible default values are used?

a Bandwidth
b Delay
c Load
d Reliability
e MTU
f Hop Count

2 Two OSPF routers connect the same VLAN using Fa 0/0 interfaces. Which of the following settings would prevent the two routers from becoming OSPF-neighbors?

a IP addresses of 10.1.1.1/24 and 10.1.1.254/25 respectively
b The addition of a secondary IP address on one router's interfac, but not the other
c Both router interfaces assigneted to area 3
d One router is configured to use MD5 authentication, and the other is not

3 Which of the following network commands, following the command router ospf 1, tells router to start using OSPF on interfaces whose IP addresses are 10.1.1.1,10.1.100.1 and 10.1.120.1

a network 10.0.0.0 255.0.0.0 area 0
b network 10.0.0.0. 0.255.255.255 area 0
c network 10.0.0.1 255.0.0.255 area 0
d network 10.0.0.1. 0.255.255.0. area 0

4 Which of the following affects the calculation of EIGRP routes when all possible default values are used?

a Bandwidth
b Delay
c Load
d Reliability
e MTU
f Hop Count

5 Which of the following network commands, following the command router eigrp 1, tells router to start using EIGRP on interfaces whose IP addresses are 10.1.1.1,10.1.100.1 and 10.1.120.1

a network 10.0.0.0
b network 10.1.1x.0
c network 10.0.0.0 0.255.255.255
d network 10.0.0.0 255.255.255.0

6 Which of the following must occur to configure MD5 authentication for EIGRP?

a Setting the MD5 authentication key via some interface subcommand
b Configuring at least one key chain
c Defining a valid lifetime for the key
d Enabling EIGRP MD5 authentication on an interface

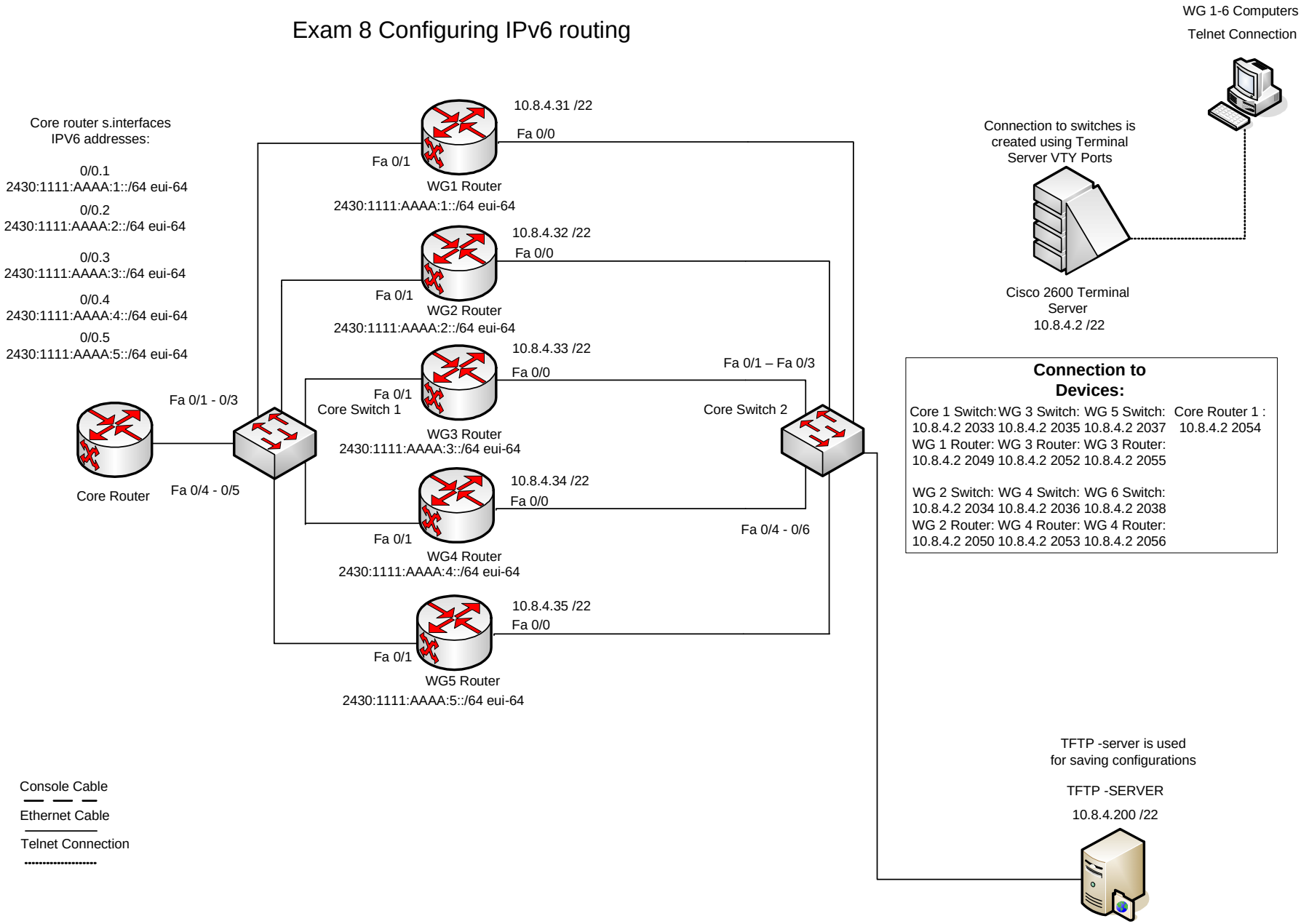
Week 7 Exam Question Answers

TASK	STEP	ANSWER
1	4	reload
1	5	show running-config
2	3	show ip route
2	4	connected routes marked with "C" and static routes marked with "S"
2	6	no access-list 120
2	7	no ip nat inside source list 120 interface FA 0/0 overload/no ip nat inside/no ip nat outside
2	8	no ip route (+) route source and destination addresses
2	9	no ip address
2	10	ip address(+)WG router fa 0/0 address
2	11	no shutdown
2	13	ip address(+)WG router fa 0/1 address
2	14	ip route 0.0.0.0 0.0.0.0 10.100.10.?
2	15	no shutdown
3	3	interface loopback
3	3	loopback interface is virtual interface that is always on and it should be configured for all
3	3	key routers
3	4	ip address(+)WG router loopback address
3	6	router ospf 100-600 >network fa 0/0 address(+)wildcard mask(+)area 0
3	6	>network(+)fa 0/1 address(+)wildcard mask(+)area 0
3	6	>network(+)loopback address(+)wildcard mask(+)area 0
3	7	connected routes marked with "C" and OSPF routes marked with "O"
3	8	a) WGs that is configured to use OSPF routing protocol to advertise routes
3	8	b) ABR router is places between two different areas example area 3 and backbone area 0
3	8	c) Backbone area is area which all other areas must be connect
3	9	configure terminal >interface fa ? > switchport access vlan ?
3	10	configure terminal > interface fa 0/0.?
3	11	encapsulation dot1q vlan ?
3	12	a) show ip protocols b) debug ip ospf events
3	13	a) ip ospf authentication > ip ospf authentication-key key-cisco b) show ip ospf
3	14	configure terminal > interface fa 0/0.? >ip ospf authentication > ip ospf authentication-key
3	14	key-cisco
3	15	a)ping (+) core router address, yes b)ping (+) wg? router address, yes c) no OSPF routing
3	15	must be configured to all routers
3	16	ip ospf authentication-key key-sanfran
3	17	ping (+) "wg? router address" no
3	18	no router ospf 1
4	2	router eigrp 100 >network address(+)wildcard mask
4	3	connected routes marked with "C" and EIGRP routes marked with "E"
4	4	WGs that is configured to use EIGRP routing protocol to advertise routes
4	5	successor is the main route to other router feasible successor is the alternative route
4	6	show ip eigrp traffic

4	**7**	debug eigrp packets or debug ip eigrp
4	**8**	ip authentication mode eigrp md5 >ip authentication key-chain eigrp 1 basic keys >
4	**8**	key chain basic keys > key 1 > key-string pete > accept-lifetime "example" 06:00:00 jun
4	**8**	27 2008 06:00:00 jul 4 2008 > send-lifetime "example" 06:00:00 jun 27 2008 06:00:00
4	**8**	jul 4 2008 > key 2 > key-string john > accept-lifetime "example" 06:00:00 jul 3 2008 >
4	**8**	jul 27 2008 send-lifetime "example" 06:00:00 jul 3 2008 jul 27 2008
4	**10**	a) ping (+) core router address, yes b) ping (+) WG router address, yes
4	**11**	a) key chain basic keys > no key 1
4	**11**	a) ping (+) "wg? router address" yes and no b) core router port 10.100.10.1 is connected
4	**11**	to WG-router other 10.100.20.1 port is using EIGRP md5 authentication
4	**13**	no router eigrp 100
4	**14**	using type 2 of authentication method that uses encyption called MD5
5	**3**	copy running-config tftp >ip address>ex7_RO_Group? > confirmation

Q	**1**	a
Q	**2**	a,d
Q	**3**	b
Q	**4**	a,b
Q	**5**	a,c
Q	**6**	b,d

Exam 8 Configuring IPv6 routing



Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week8

Configuring IPv6 routing

WORKING METHOD

1 people / workgroup max 5 groups

ACTIVITY OBJECTIVES

- Getting configurations from TFTP server
- Removing old configurations
- Configuring IPv6 address
- Configuring RIPng routing protocol
- Copy configurations to TFTP server

THEORY CONCEPTS

- RIPng routing protocol
- IPv6 address format
- IPv6 address prefix
- IPv6 address abbreviation
- IPv6 tunnelling methods

ADVANCE JOBS (exam instructor)

- Ensure that terminal server ports is cleared, when students take connections
- Ensure that connection to TFTP server is working before practise and server IP address is changed
- Ensure that configuration images are located from TFTP server and file names are correct

EXAM JOBS (exam instructor)

- Ensure that IPv6 address is configured correctly to interface
- Ensure that RIPng routing protocol is configured correctly to WG router
- Ensure that connections between devices are working when testingIPv6 connections using ping command
- Ensure that configuration files are saved to TFTP server after exam
- Troubleshooting purposes if needed

Week 8 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup-config	privileged	Copies running-configuration information
running config		from NVRAM to RAM
copy running-config	privileged	Copies running-configuration information
startup config		from RAM to NVRAM
erase startup-config	privileged	Erase startup config file
ping (+) ip-address	privileged	Used for troubleshooting purposes
quit	privileged	Exits IOS -system
reload	privileged	Reboots the switch
show ip protocols	privileged	Show routing protocol parameters and timer values
copy tftp startup config	privileged	Copies tftp server configuration to startup-config
copy tftp running-config	privileged	Copies tftp server configuration to running-configuration
copy running-config tftp	privileged	Copies configuration from running-config to tftp -server
copy startup config tftp	privileged	Copies configuration from startup config to tftp -server
telnet (hostname)	privileged	Connects the CLI to another host using telnet
resume	privileged	Resumes connection to suspended host
disconnect	privileged	Disconnects connection to suspended host
show ip route	privileged	Shows routing table information
show ipv6 route	privileged	Lists IPv6 routes
show ipv6 route (+) address	privileged	Lists IPv6 the routes that match for packets sent to listed address
show ipv6 interface	privileged	Lists IPv6 settings on an interface
show ipv6 interface brief	privileged	List IPv6 settings for each interface
Cntr+Shift-6, x	keyboard sc	Key sequence to suspend Telnet or SSH connection
exit	conf.mode	Moving back to the next higher mode
end	conf.mode	Exits in any conf. mode and goes user mode
line console 0	conf.mode	Moving to console line conf.mode
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
enable secret	conf.mode	Sets clear text- password
enable password	conf.mode	Sets automatically encrypted password
hostname	conf.mode	Sets switch's hostname
interface loopback	conf.mode	Defines loopback interface to OSPF -routing protocol
router ospf	conf.mode	Enters OSPF configuration mode
router eigrp	conf.mode	Enters EIGRP configuration mode

Command	Mode	Purpose
ip route 0.0.0.0 0.0.0.0 (+) mask (+) destination address	conf.mode	Defines default IP -route
ipv6 route		
ipv6 unicast-routing	conf.mode	Enables IPv6 routing
ipv6 router rip (+) tag	conf.mode	Enables RIPng routing protocol on the router
ipv6 rip (name) enable		Enables RIPng on the specific interface
ip route s.address (+) mask (+) null 0	conf.mode	Creates bogus route to interface null0 (it does not lead anywhere)
username (value) password (value)	conf.mode	Sets username and password required if the login local command is configured
ipv6 route(+)destination nw ip(+) destination wc mask(+)source ip	conf.mode	Defines ipv6 static route
ipv6 address (+) ipv6-address / prefix-lenght (+) eui-64	line fa conf	Set IPv6 /64 prefix address to interface
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
ip address (+) mask	line fa conf	Sets ip address and mask for interface
login local	line vty conf	Tell IOS to prompt for username and password
ipv6 rip (name) enable		Enables RIPng on the specific interface
ipv6 address (+) ipv6-address / prefix-lenght (+) eui-64	line fa conf	Configures either the entire interface IP address of / 64 prefix
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
ip address (+) mask	line fa conf	Sets ipv4 address and mask for interface
swithport address vlan (+)value	line fa conf	Sets switch interface to use specific VLAN
login local	line vty conf	Tell IOS to prompt for username and password
username (value)	line vty conf	Sets username and password required
password (value)		if the login command is configured
redistribute static subnets	ospf conf	distributes static routes to other routers
encapsulation dot1q (+) vlan value	subinterfac conf	Attach subinterface to specific vlan
ipv6 address (+) ipv6-address / prefix-lenght (+) eui-64	subinterface conf	Set IPv6 /64 prefix address to sub interface

TASK 1 Get router configuration from TFTP server

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take connection to your WG router. (Check terminal server IP -address and port number with a picture included)

STEP 3

Go to privileged mode and copy router saved configuration image from TFTP server to router startup-configuration.

STEP 4

Boot up router. What is right command to boot-up router.

_____

STEP 5

Show running-configuration from router and check if configuration is applied correctly?

STEP 6

Next task is to build up exam topology that matches topology with exam picture. Every group must show own coupling to administrator and check it is acceptable before continuing.

TASK 2 Remove old configurations from WG router

STEP 1

Take connection to WG router.

STEP 2

Move to privileged mode.

STEP 3

Show running-configuration.

STEP 4

Show router table information.

What routes are marked in the routing table?

STEP 5

Go to global configuration mode.

STEP 6

Take off all static routes from a table (if there are any). Routes must be removed one by one. What is right command to remove route from a table?

Show router table information and check, that there are no routes left.

STEP 7

Go to interface FA 0/0 configuration mode and remove IP -address from the interface.

STEP 8

Go to interface FA 0/1 configuration mode and remove IP -address from the interface.

STEP 9

Show running-configuration.

STEP 10

Check, that all interfaces IP -addresses are cleared.

STEP 11

Remove all IPv4 routing protocols, if there are any?

TASK 3 Configure IPv6 addresses and static routes between routers

STEP 1

Keep connection to WG router and move to global configuration mode.

STEP 2

Enable IPv6 routing. What is right command for that?

STEP 3

Move to interface FA 0/1 configure mode.

STEP 4

Set EUI-64 IPv6 address to interface FA 0/1. Look right address at the picture.

What is right command to add IPv6 address to interface?

STEP 5

Create static ipv6 route to other WG router.

Before route can be configured correctly you must now, what is other router Ethernet address and create static route to use that address. (look at the picture for right mac -address)

STEP 6

Move to privileged mode and show router routing table information.

What ipv6 routes are listed in a table?

STEP 7

Take connection to core switch and change interface that are connected to your group router for VLAN 100-105 depending your group number.

STEP 8

Take connection to core router and create sub interface FA 0/0.1 - FA 0/0.5 depending your group number.

Attach sub interface for your group VLAN and create IPv6 address for sub interface (look at the picture for right address)

STEP 9

Change connection back to WG router

STEP 10

Move to privileged mode and show router routing table information.

What ipv6 routes are listed in the table?

Are there any ipv6 static routes in the table?

STEP 11

Ping other WG router ipv6 interface FA 0/1 address. Did you get reply?

STEP 12

Remove all static ipv6 routes from a router

TASK 4 Configure IPv6 addresses and RIPng routing protocol

STEP 1

Keep connection to WG router and move to global configuration mode.

STEP 2

Enable routing protocol for IPv6. Use RIPng (next generation) routing protocol for that. Enter right command below:

There are also other routing protocols for IPv6. What are called EIGPR and OSPF routing protocol versions that supports IPv6 routing. What are those protocols called? Write answer below.

STEP 3

How many parts normal Pv6 address is composed?

What are those parts called?

How many bits one hexadecimal number represent?

Full IPv6 address consists 8 quarters of 4 hex digits separated by a colon. How many bits is full IPv6 address long?

How IPv6 address bits are shared between different parts?

STEP 4

IPv6 address is possibility to type abbreviated form. How abbreviated IPv6 address prefix is typed?

How IPv6 address 3000:1234:1234:5EFD:0000:0000:0000:0000/64 is typed abbreviated form.

What is binary form of the hexadecimal number 6?

What is binary form of the hexadecimal number E?

STEP 5

Enable IPv6 routing protocol on the interface FA 0/1. Insert command below:

STEP 6

Move to privileged mode.

STEP 7

Show IPv6 information for each interface. What is right command for that?

STEP 8

Enable IPv6 routing for Core-router sub interface (look at the picture for right address)

STEP 9

Move to global configuration mode.

STEP 10

Show routing table information. What IPv6 related routes did you find?

STEP 11

Try to ping some other WG router IPv6 address that is configured for IPv6 routing. Did you get reply?

STEP 12

IPv6 protocol can send IP packet different ways. What are those three categories to send IP packet?

STEP 13

IPv6 packet can also be send to existing IPv4 network if IPv6 packet is encapsulated inside IPv4 packet and later another device removes only IPv4 header revealing IPv6 packet inside. This is called IPv4 to IPv6 tunnelling, what different IPv6 tunnelling methods exists?

_____

_____

_____

_____

TASK 5 Copy router configuration files to TFTP server

STEP 1

Final task is copy your configurations to TFTP server. Type right command, that copies you configuration file to TFTP -server. (Image file name and IP -address is found at the picture).

STEP 2

Move to privileged mode.

STEP 3

Copy configuration from router to TFTP server

Use following image file name: "**Ex8_RO_Group?"** where "?" is your work-group number.

Enter right copy command below

_____

Week 8 Exam Revision Questions

1 Which of the following is the shortest valid abreviation for FE80:0000:0100:0000:0000:0000:0123?

a FE80::100::123
b FE8::1::123
c FE80::100:0:0:0:123:4567
d FE80:0:0:100::123

2 Which of the following are routing protocols that supports IPv6?

a RIPng
b RIP-2
c OSPFv2
d OSPFv3
e OSPFv4

3 If router has following MAC address 4444.4444.4444. Which of the following IPv6 addresses will the interface use?

a 3456::C444:44FF:FE44:4444
b 3456::1
c FE80::1
d FE80::6444:44FF:FE44:4444
e FE80:4444:4444:4444

4 Which of the following configuration commands would enable RIP on FA 0/0?

a network 3456::/64
b network 3456::/16
c network 3456::1/128
d ipv6 rip enable
e ipv6 rip tag1 enable

5 Which tunneling method use host to create and encapsulate packet?

a Dynamic 6to4 tunnel
b MCT
c Teredo
d ISATAP

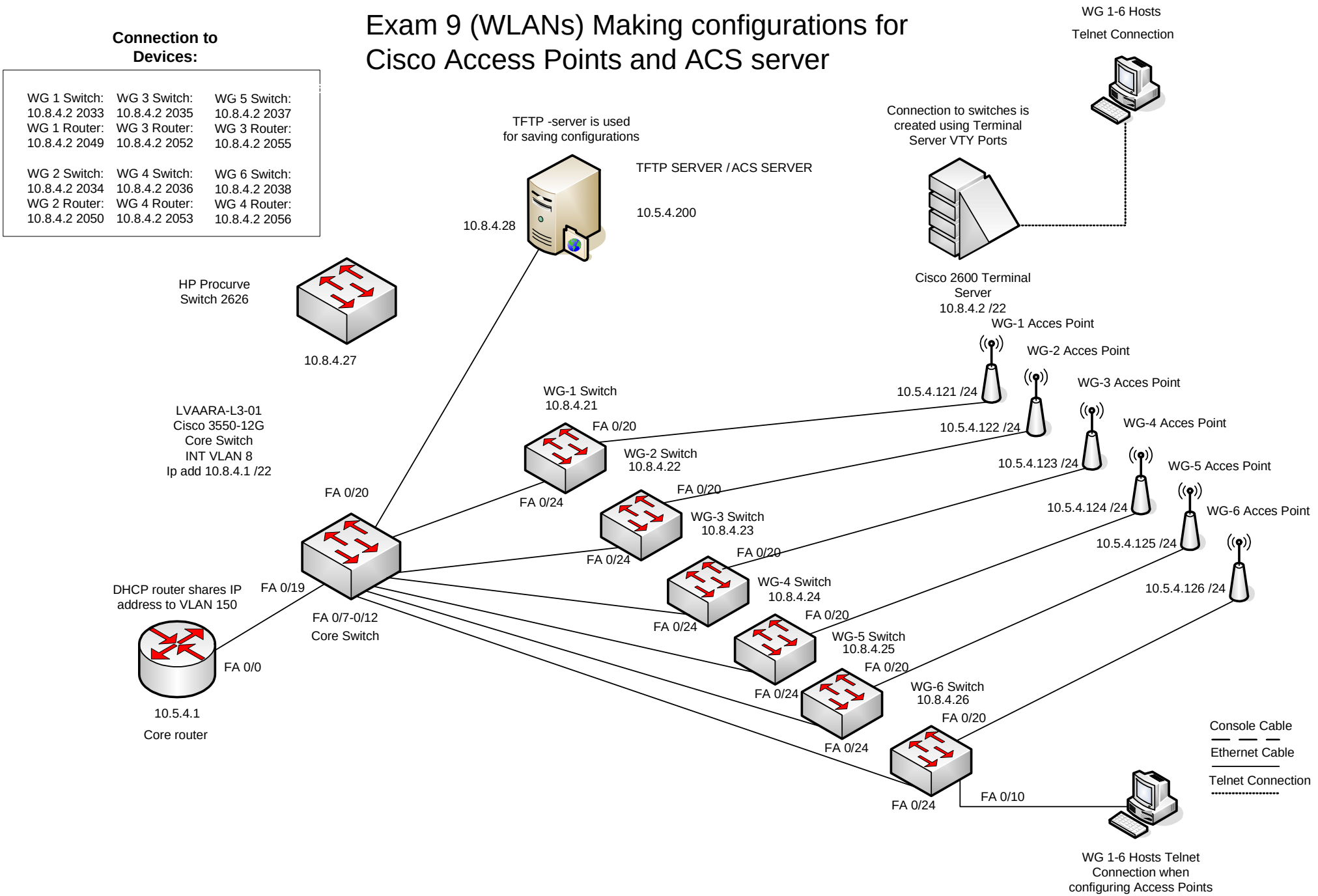
Week 8 Exam Question Answers

TASK	STEP	ANSWER
1	4	reload
2	3	show running-config
2	4	a) show ip route b) only connected routes "c"
2	5	configure terminal
2	6	no ip route (+) source address mask (+) destination address mask
2	7	a) interface fastethernet 0/0 no ip address / ip address 10.8.4.? /22
2	8	a) interface fastethernet 0/1 no ip address
2	10	show interfaces / show running-config
2	11	no router rip / no router eigrp / no router ospf
3	2	ipv6 unicast routing
3	4	ipv6 address (+) ipv6 address /prefix lenght (+) eu1-64
3	5	a) show ipv6 route b) only connected routes should be in a table
3	6	switchport access vlan 100-105
3	7	a)interface fa 0/0.01 - 0/0.05
3	7	b)encapsulation dot1q vlan 100-105
3	8	ipv6 route 2430:1111:aaaa:? (+) router ethernet address (next hop address)
3	10	show ipv6 route >static and connected routes should be in a table
3	11	ping should get reply if static routes are configured correctly
3	12	no ipv6 route (+) destination address (+) next hop address
4	2	a) ipv6 router rip (+) id b) RIPng,OSPFv3,MP-BGP4 and EIGRP for IPv6
4	3	a) two parts b) Prefix and Host c) 4 bits d) 128 bits e) 48 bits subnet prefix part
4	3	that includes 16 subnet part and 64 bits for host part
4	4	a) :: abbreviation means that one or more quarters of address bits is zeros "0"
4	4	:: abreviation is possibility to use only one time per address
4	4	b) 3000:1234:1234:5EFD:: /64 c) 0110 d) 1110
4	5	ipv6 rip (id) enable
4	7	show ipv6 interface brief
4	8	interface fa 0/0.01 - 0/0.05 ipv6 > rip (id) enable
4	10	show ip route
4	11	ping (+) ipv6 address >all ipv6 configured address shoud answer to ping command
4	12	unicast, multicast, anycast
4	13	Manually configured tunnels (MCTs), Dynamic 6to4 tunnels, Intra site Automatic Tunnel
4	13	addressing Protocols (ISATAP) and Teredo tunnels
5	3	copy running-config tftp > TFTP server address >EX9_RO_Group?
Q	1	d
Q	2	a,d
Q	3	b,d
Q	4	e
Q	5	c

Exam 9 (WLANs) Making configurations for Cisco Access Points and ACS server

Connection to Devices:

WG 1 Switch:	WG 3 Switch:	WG 5 Switch:
10.8.4.2 2033	10.8.4.2 2035	10.8.4.2 2037
WG 1 Router:	WG 3 Router:	WG 3 Router:
10.8.4.2 2049	10.8.4.2 2052	10.8.4.2 2055
WG 2 Switch:	WG 4 Switch:	WG 6 Switch:
10.8.4.2 2034	10.8.4.2 2036	10.8.4.2 2038
WG 2 Router:	WG 4 Router:	WG 4 Router:
10.8.4.2 2050	10.8.4.2 2053	10.8.4.2 2056



Laurea Data communication laboratory CCNA network exam

Pvm

Name Student number

Name Student number

Week9

Configuring WLAN networks and Access Points

WORKING METHOD

1 people / workgroup max 6 groups

ACTIVITY OBJECTIVES

- Getting configurations from TFTP server
- Removing old configurations
- Configuring Access Points with different VLANs
- Configuring APs settings
- Configuring ACS server settings
- Testing WLAN -networks
- Copy configurations to TFTP server

THEORY CONCEPTS

- WLAN
- Cisco Access Point
- Cisco Secure Access Control Server
- SSID
- Native VLAN
- Authentication
- Encyption

ADVANCE JOBS (exam instructor)

- Ensure that terminal server ports is cleared, when students take connections
- Ensure that connection to TFTP server is working before practise and server IP address is changed
- Ensure that configuration images are located from TFTP server and file names are correct
- Ensure that APs is configured correctly with default configurations
- Ensure that connections to APs are working
- Ensure that ACS server is turned on and connected to right VLAN

EXAM JOBS (exam instructor)

- Help students learn to use Cisco Access Point GUI commands
- Help students configuring computer network settings
- Help student to configure ACS-server (other instructor must be check that all groups get help to configure ACS-server settings)
- Ensure that configuration files are saved to TFTP server after exam
- Troubleshooting purposes if needed

Week 9 Exam Command List

Command	Mode	Purpose
enable	user	Moving to privileged mode
disable	privileged	Moving to user mode
configure terminal	privileged	Moving to configuration mode
show running-config	privileged	Show content of running-configuration
show startup-config	privileged	Show content of startup-configuration
copy startup-config	privileged	Copies running-configuration information
running config		from NVRAM to RAM
copy running-config	privileged	Copies running-configuration information
startup config		from RAM to NVRAM
erase startup-config	privileged	erase startup config file (NVRAM)
ping (ip-address)	privileged	Used for troubleshooting purposes
quit	privileged	exits IOS -system
reload	privileged	reboots the switch, router or Access Point
copy tftp startup config	privileged	Copies tftp server configuration to startup-config
copy tftp running-config	privileged	Copies tftp server configuration to running-configuration
copy running-config tftp	privileged	Copies configuration from running-config to tftp -server
copy startup config tftp	privileged	Copies configuration from startup config to tftp -server
telnet (hostname)	privileged	Connects the CLI to another host using telnet
resume	privileged	Resumes connection to suspended host
disconnect	privileged	Disconnects connection to suspended host
show ip route	privileged	Shows routing table information
show vlan (brief,name, summary)	privileged	Displays VLAN information
Cntr+Shift-6, x	keyboard sc	Key sequence to suspend Telnet or SSH connection
ip route 0.0.0.0 0.0.0.0 (+) mask+destination address	conf.mode	Defines default IP -route
exit	conf.mode	Moving back to the next higher mode
end	conf.mode	Exits in any conf. mode and goes user mode
line console 0	conf.mode	Moving to console line conf.mode
line vty (1st-vty 2nd-vty)	conf.mode	Moving to virtual line conf.mode
interface fastethernet	conf.mode	Moving to interface conf.mode
enable secret	conf.mode	Sets clear text- password
enable password	conf.mode	Sets automatically encrypted password
hostname	conf.mode	Sets switch's hostname
username (value)	conf.mode	Sets username and password required
password (value)		if the login local command is configured
login local	line vty conf	Tell IOS to prompt for username and password
shutdown	line fa conf	Shutdown interface
no shutdown	line fa conf	Enable interface
ip address (+) mask	line fa conf	Sets ip address and mask for interface
switchport mode trunk	line fa conf	Configures the trunking on the interface
switchport trunk allowed vlan (id)	line fa conf	Defines lists of allowed VLANs
switchport access vlan (id)	line fa conf	Configures defined interface into VLANs

Command	Mode	Purpose
switchport trunk encapsulation (dot1q)	line fa conf	Defines dot1q trunking encapsulation to interface
swithport trunk native	line fa conf	Defines native VLAN

TASK 1 Getting switch configurations from TFTP server

STEP 1

From your PC, Open connection to terminal server.

STEP 2

Take new connection to your WG? Switch.

STEP 3

Go to privileged mode and copy switch saved configuration image from TFTP -server to switch startup -configuration.

STEP 4

Boot up switch.

STEP 5

Show running-configuration from switch and check if last exam configuration is applied correctly?

STEP 6

Next task is to build up exam topology that matches topology with exam picture. Every group must show own coupling to administrator and check it is acceptable before continuing.

STEP 7

Clear all switch configured VLANs and trunk port settings. Keep management VLAN 8.

TASK 2 Make switch VLAN configuration to Access Point

STEP 1

Move to privileged mode.

STEP 2

Show information about switch VLANs below:

How many VLANS switch database consists of?

_____

What VLAN is working at the switch administrative VLAN?

_____

STEP 3

Move to interface FA 0/20 configuration mode.

STEP 4

Set interface FA 0/20 to trunk port mode.

STEP 5

Set on interface FA 0/20, if interface is disabled.

STEP 6

Allow trunk port to transmit vlans 8, 26 and 150.

STEP 7

Set vlan 150 to native vlan mode.

STEP 8

What is right command to set vlan 150 to native mode?

_____

STEP 9

What is meaning of Native VLAN?

_____

STE 10

Move to interface FA 0/10 configuration mode.

STEP 11

Define interface FA 0/10 to allow VLAN 150.

STEP 12

Set on interface FA 0/10, if interface is disabled.

STEP 13

Move to interface FA 0/24 configuration mode.

STEP 14

Set interface to trunk mode

STEP 15

Set on interface FA 0/24, if interface is disabled.

STEP 16

Show running-configuration and check if the VLANs are correctly configured

STEP 17

Connect WG computer to switch interface FA 0/10 and check computer set ups:

IP Address:

Subnet Mask:

Default gateway:

DHCP server:

TASK 3 Configure WLAN Access Point settings with graphical user interface (GUI)

STEP 1

Open internet browser and take connection to Workgroup Access Point. Check Access Point IP address with picture.

STEP 2

Give username: admin and password: cisco, when login screen is displayed

STEP 3

Every group must configure Access Point basic settings and two networks one secure and one common network. After step, fill right command and location where command must be entered (right form and line for the GUI)

STEP 4

General Settings: Give Access Point hostname: WG?-AP

Cisco GUI location:

Command:

STEP 5

User and password settings: Add new user: WG-? and user password: cisco. Check that password is configured to Local User list only and user has possibility to read and write configurations.

Cisco GUI location:

Command:

STEP 6

VLAN settings: Add VLAN 8 and VLAN 26

Cisco GUI location:

Command:

STEP 7

VLAN settings: Add VLAN 150 and set VLAN 150 to native VLAN

Cisco GUI location:

_____

Command:

_____

STEP 8

Encryption settings: Set VLAN 8 to use encryption Cipher TKIP

Cisco GUI location:

_____

Command:

_____

STEP 9

ACS Server settings: Add Radius Cisco ACS server. Get IP address from the picture, set password WG-? when connecting server.

Cisco GUI location:

_____

Command:

_____

STEP 10

Add priority 1 EAP -authentication server. Use ACS server IP address.

Cisco GUI location:

_____

Command:

_____

STEP 11

SSID Settings: Add two networks WG?-common and WG?-secure. Networks configurations are following:

WG?-common:
SSID: WG?-common
VLAN: 26
Interface: Radio0-802.11g

WG?-secure:
SSID: WG?-secure
VLAN: 8
Interface: Radio0-802.11g

Open Authentication: With EAP
Network EAP: <nothing>
Customize, Priority 1: AP-address
Key management: Mandatory (WPA)

Add specific radio channel to each group. Use following channels:

Radio channel 1 for WG 1 and Radio channel 6 for WG6

Cisco GUI location:

Commands:

Cisco GUI location:

Commands:

Radio Channels:

Cisco GUI location:

Commands:

TASK 4 Make Access Control Server (ACS) configurations

STEP 1

Every group must configure ACS server configurations. Instructor shows computer where ACS server is installed. Configurations must be made for that computer.

STEP 2

Open Cisco Secure ACS server program

STEP 3

Every group must add their own workgroup configurations.

Network configuration: Client Hostname: WG?-AP, Client IP Address: “Action Point 1-6 IP address” KEY: WG-? Authentication: RADIUS (Cisco Aironet)

Command 1:

_____

Cisco GUI location:

_____

Command 2:

_____

Cisco GUI location:

_____

Command 3:

_____

Cisco GUI location:

_____

STEP 4

User configurations: Every group must add their usernames and passwords. Username: WG1-WG6 and password: WG-1-WG-6

Command:

_____

Cisco GUI location:

_____

STEP 5

Why Cisco WLAN action points needs Cisco ACS server?

_____

_____

_____

Why ACS server is needed for this exam?

TASK 5 Make WLAN configurations to PC

STEP 1

Open network connection settings from a group computer. Check IP configurations:

IP Address:

Subnet Mask:

Default gateway:

DHCP server:

STEP 2

Change network connection to use wireless network card.

STEP 3

Add new wireless network: **WG?-common**, use open authentication and disable all encryption settings.

STEP 4

Check now changed IP configurations:

IP Address:

Subnet Mask:

Default gateway:

DHCP server:

Did VLAN 26 DHCP server give you new network settings?

STEP 5

Clear SSID WG1-common configurations.

STEP 6

Add new wireless network: **WG?-secure**, use **WPA authentication**, encryption **TKIP** and EAP TYPE **Protected EAP**

STEP 7

Remove selections for all authentications.

STEP 8

Use server certificate validation.

STEP 9

Remove logon when windows starts.

STEP 10

Create connection to AP and insert username and password, when prompted

STEP 11

Check now changed IP configurations:

IP Address:

_____

Subnet Mask:

_____

Default gateway:

_____

DHCP server:

_____

STEP 12

Did VLAN 8 DHCP server give you new network settings?

_____

STEP 13

What differences two connections has? What is the main difference?

_____

_____

_____

STEP 14

Clear configurations.

TASK 6 Copy APs configuration files to TFTP server

STEP 1

Take telnet connection to WG switch and move to privileged mode.

STEP 2

Final task is copy your configurations to TFTP server. Type command that copy router configuration to TFTP server. (Image file name and IP address are found at the picture).

STEP 3

Enter right copy command below

Use following image file name: "**Ex9_SW_Group?"** where "?" is your work-group number.

STEP 4

Take telnet connection to Access point.

STEP 5

Move to privileged mode.

STEP 6

Copy Access Point running-configuration to Access Point startup-configuration.

STEP 7

Check if copy operation succeeded.

STEP 8

Copy startup-configuration from Access Point to TFTP server.

Use following image file name: "**Ex9_ACS_Group?"** where "?" is your work-group number.

STEP 9

Clear Access Point NVRAM memory.

STEP 10

Copy new default configuration (ap-config_?) from TFTP server to NVRAM memory.

STEP 11

Check if copy operation succeeded.

STEP 12

Reload Access Point.

Week 9 Exam Revision Questions

1 Which of the following IEEE wireless LAN standards uses only the U-NII band of frequencies (around 5.4GHz)?

a 802.11a
b 802.11b
c 802.11g
d 802.11i

2 When configuring a wireless access point, which of the following are typical configurations choices?

a SSID
b Speed of use
c wireless standard to use
d size of the desired coverage area

3 Which of the following is true about an ESS's connections to the wired Ethernet LAN?

a The AP connects to the Ethernet switch using a crossover cable
b The various APs in the same WLAN need to be assigned to the same VLAN by the switches
c The Aps must have an IP address configured to forward traffic
d The APS using mixed 802.11g mode must connect via a Fast Ethernet or faster connection to an Ethernet switch

4 Which of the following WLAN security standards refer to the IEE standard?

a WPA
b WPA2
c WEP
d 802.11i

5 Which of the follwing security features not in the original WEP security standard but are true now in the WPA 2 security standard?

a Dynamic key exhange
b Preshared Keys (PSK)
c 801.1x authentication
d AES encyption

Week 9 Exam Question Answers

TASK	STEP	ANSWER
1	5	show running-config
1	7	no switchport mode trunk, no switchport access vlan ?
2	2	a)- b)vlan 8
2	8	switchport trunk vlan 150 native
2	9	native VLAN does not get trunk encapsulation they would on a native ethernet
2	9	hence native vlan.
2	17	a) b) c) d)
3	4	a) express setup > hostname b) WG?-AP
3	5	a) security > admin access b) Username: wg? Password: cisco local user list only:x r/w:x
3	6	a) services > VLAN b) vlan 8 , vlan 26
3	7	a) services > VLAN b) vlan 150 , native VLAN
3	8	a) security > encyption b) vlan 8, encryption > CIPHER: TKIP
3	9	a) security > server manager / radius ACS b) address: "server ip address" , password: wg-1
3	10	a) security > server manager / radius ACS b) server: priority 1, authentication: EAP,
3	10	address: "server ip address"
3	11	a) security > SSID manager: b)SSID:wg1-common, vlan:vlan 26, interface:radio 0-802.11g
3	11	c) security > SSID manager: d)wg1-secure, vlan:vlan 8, radio0-802.11g,
3	11	open authentication: With EAP,
3	11	network EAP: - customize priority 1: "AP-address" key management: mandatory (WPA)
3	11	e) network interface > radio: f)radio ch: wg=ch1 wg6=ch6
4	3	a) general setup / client settings b) client name: WG-1AP - WG6-AP
4	3	c) general setup / client settings d) ap address: 10.5.4.121 - 10.5.4.126
4	3	e) general setup / client settings f) Authentication: Cisco Aironet
4	4	a) general setup / user configuration b) username: wg1-wg6 password: wg1-wg6
4	5	a) ACS -server shares network information to APs and manages networks encryption
4	5	it is also simplier to make configurations for many APs using ACS -server
4	5	b) that students is able to practise making configurations for ACS -server
4	5	ACS -server is used for this exam because it manages enctyption for SSID network
4	5	wg1-6 -secure
5	1	ip config /all
5	4	ip config /all
5	4	yes
5	11	ip config /all
5	12	yes
5	13	wg-common is basic network without any secure settings
5	13	wg-secure is using TKIP encryption and WPA authentication protocol
6	3	copy running-config TFTP > "ip address" >Ex9_SW_Group1-6
6	9	clear nvram
6	10	copy TFTP startup-config >ap-config1-6
6	12	reload

Q	**1**	a
Q	**2**	a,c
Q	**3**	b
Q	**4**	b,d
Q	**5**	a,c,d