Satakunnan ammattikorkeakoulu

Petri Luojus

LANGATTOMAN VERKON TIETOTURVASTA

Tekniikka Pori

Tietotekniikan koulutusohjelma

Tietoliikennetekniikan suuntautumisvaihtoehto

2008

LANGATTOMAN VERKON TIETOTURVASTA

Luojus, Petri
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Toukokuu 2008
Valvoja: Holm, Hannele
UDK: 004.056, 004.73, 621.395:621.371
Sivumäärä: 88

Asiasanat: WLAN, WEP, WPA, WPA2, IEEE 802.11, Langaton verkko

---

Tämä opinnäytetyö keskittyi IEEE 802.11-standardin mukaisten, radiotaajuuksilla toimivien langattomien lähiverkkojen tietoturvan kulmakiviin.

Tässä työssä käytiin aluksi läpi IEEE 802.11-standardiin perustuvien verkkojen toimintaa sekä verkkojen fyysisiin osiin kohdistuvia standardin laajennuksia. Standardin esittelyn jälkeen suoritettiin nopea katsaus tuleviin standardeihin.

Työssä tutustuttiin tietoturvan yhteydessä käytettyihin peruskäsitteisiin ja yleisiin tietoturvaa parantaviin menetelmiin.

Tietoturvan peruskäsitteistä siirryttiin langattomissa verkoissa tapahtuvaan käyttäjän todentamiseen, jossa luotiin katsaus EAP-protokollaan sekä EAP:n käyttämiin sisäisiin todentamismenetelmiin.

Todentamismenetelmistä siirryttiin datan suojaamiseen fyysisellä siirtotiellä, eli radioaalloilla. Tässä kappaleessa pureuduttiin standardissa määritellyn WEP:n tietoturvaongelmiin ja tarkasteltiin, miten WEP:n aukkoja on korjattu TKIP:llä. Kappaleen viimeisenä asiana käytiin läpi tehokas suojausmenetelmä, CCMP

Lopussa luodaan mielikuva langattomia verkkoja kohtaan kohdistuvista erilaisista uhkakuvista. Hyökkäyksien yhteydessä kerrotaan verkkoon tunkeutumiseen tarvittavien tietojen hankkimisesta, salausavaimen murtamisesta, Man-in-the-Middle-hyökkäyksestä sekä todentamismekanismia vastaan tehtävistä hyökkäyksistä.

Tietoturvan tutkimista varten rakennettiin koulun tietoliikennelaboratorioon viiden koneen testiverkko. Verkossa käytettiin Cisco Systemsin langattomia laitteita, reitittimiä sekä kytkimiä. Testiympäristössä tutkittiin tietojen hankkimista passiivisesti salakuuntelemalla, jotta verkkoon voitaisiin tunkeutua. Testiverkossa tutkittiin myös WEP-salauksen murtamista sekä WPA2:n avaintenvaihtoa ja salausalgoritmien neuvottelua.

WIRELESS NETWORK SECURITY

Luojus, Petri
Satakunta University of Applied Sciences
Degree Programme in Information Tehcnology
May 2008
Instructor: Holm, Hannele
UDC: 004.056, 004.73, 621.395:621.371
Number of Pages: 88

Key Words: WLAN, WEP, WPA, WPA2, IEEE 802.11, Wireless network

---

This thesis concentrated on the keystones of wireless LAN security in accordance with the IEEE 802.11 standard.

This thesis first took a look in the basic functions and physical entities of IEEE 802.11 networks. The same chapter covers also physical extensions for IEEE 802.11 standard and mentions also something about new, upcoming standards.

After familiarizing oneself with the wireless standards, some basic concepts of overall data security are covered. User authentication is next in line after the basic data security concepts. Focus in this chapter is on the EAP authentication protocol and on its inner authentication methods.

From authentication methods, focus was moved to the ways of securing data transfer over physical transmission paths, which in this case were radio waves. This chapter gets its teeth into the security mechanisms specified by the original wireless standard, IEEE 802.11. After taking a look in WEP's security holes and flaws, one will see how TKIP have fixed these problems. The last subject in this chapter is CCMP, a powerful security mechanism used in today's modern and secure wireless networks.

At the end, this thesis addressed some vulnerabilities and basic attacks against wireless networks. Formerly mentioned attacks consist of some basic steps for gathering enough required information to join the network. After collecting the information, one will hear about breaking the encryption key. This chapter will also cover Man-in-the-Middle attacks and assaults, which are possible to make against authentication methods.

To investigate wireless LAN security, a five computer network was built to a data communications laboratory for testing purposes. The network was built on Cisco Systems equipment and to be more precise, the network consisted of wireless devices, routers and switches. In this testing environment, data was gathered passively by eavesdropping for the purpose of infiltrating the network. In this same network, cracking on the WEP encryption was examined. Key exchange and encryption algorithm negotiation was investigated from WPA2.

SISÄLLYS

1 LYHENNELUETTELO

ACS	Access Control Server
ADHP	Authenticated Diffie-Hellman Protocol
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSS	Basic Service Set
CCK	Complementary Code Keying
CCMP	Counter Mode/CBC-MAC Protocol
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CTS	Clear To Send
DCF	Distributed Coordination Function
DSSS	Direct Sequence Spread Spectrum
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
GMK	Group Master Key
GPS	Global Positioning System
GTK	Group Transient Key
IBSS	Independent Basic Service Set
IEEE	The Institute of Electrical and Electronic Engineers
ICV	Integrity Check Vector
IP	Internet Protocol
ISM	Industrial Scientific Medical
ISR	Integrated Services Router

IV	Initialization Vector
MAC	Medium Access Control
MIC	Message Integrity Check
MSDU	MAC Service Data Unit
NAS	Network Access Server
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PAC	Protected Access Credential
PAN	Personal Area Network
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
PMK	Pairwise Master Key
PN	Packet Number
PoE	Power over Ethernet
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
QoS	Quality of Service
RADIUS	Remote Address Dial-In User Service
RC4	Rivest Cipher 4
RSC	Recieve Sequence Counter
RF	Radio Frequency
RTS	Request To Send
SHA	Secure Hash Algorithm
SSID	Service Set Identifier
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TEK	Temporal Encryption Key
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TSC	TKIP Sequence Counter

UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller

2 JOHDANTO

Langattomat verkot ovat laajalti käytössä niin yrityksissä kuin kotiverkoissakin. Valitettavan usein löytyy langattomia verkkoja, jotka tarjoavat suoran pääsyn kaikkiin sisällä pitämiinsä palveluihin. Yksinkertaiset salausmenetelmät tiedonsiirron turvaamiseksi eivät ole vaikeita käyttöönotettavia, mutta usein sekin jää kokonaan tekemättä.

Langattomia verkkoja on jo lähes kaikkialla. Monissa kaupungeissa on rakennettu julkinen, kaikille avoin verkko pienimuotoiseen Internetin käyttöön. Yrityksissä luodaan vierailijoita varten avoimia verkkoja, joista on pääsy Internetiin. Liikkuvuuden helpottamiseksi tehdään myös verkkoja yrityksen sisäiseen käyttöön, joista on pääsy kaikkiin verkon palveluihin. Tietoturvan merkitystä langattomien verkkojen suojaamiseksi ei voida koskaan korostaa liikaa. Tietoturvan pettäessä voidaan menettää paljon tietoja, jotka voivat olla tärkeitä yrityksen menestymisen kannalta.

Langattomien verkkojen suojaamiseksi on viimeisen kymmenen vuoden aikana kehitetty suuri määrä erilaisia tekniikoita. Nykyaikaisilla menetelmillä voidaan langaton verkko pitää turvallisena, mutta negatiivisena puolena asiassa on kustannuksien nousu. Kustannuksien noustessa voidaan ruveta säästämään kuluissa ja aletaan tinkiä tietoturvasta, joka taas saattaa kostautua myöhemmin.

3 LANGATON LÄHIVERKKO

Langattoman lähiverkon toteuttamiseksi on olemassa useita vaihtoehtoja eri käyttötarkoituksiin. PAN (Personal Area Network) on yhden ihmisen läheisyydessä oleva verkko, jonka toteutukseen on pääasiassa käytetty IrDA tai Bluetooth teknologioita. MAN (Metropolitan Area Netrowk) toteutukseen on usein käytetty niin WLAN kuin WiMAX teknologioita.

3.1 IEEE 802.11

IEEE 802.11-standardi hyväksyttiin vuonna 1997 ja sen paranneltu versio julkaistiin vuonna 1999. Standardi määrittelee toiminnot OSI-mallin kerroksilla 1 (Fyysinen kerros) ja 2 (Siirtoyhteyskerros).

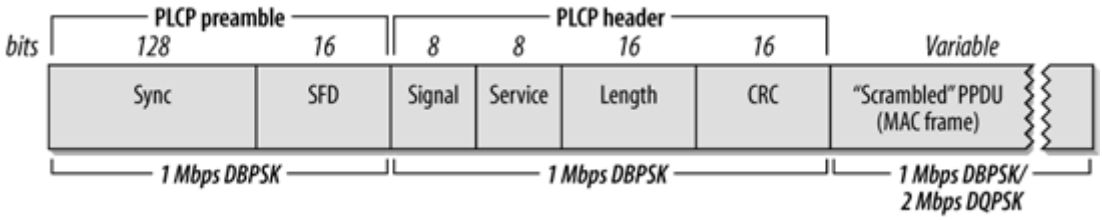
3.1.1 Fyysinen kerros

Fyysinen kerros jakautuu kahteen pääryhmään. Yleisimmin käytetty ratkaisu on 2,4 GHz ISM-alueella toimiva RF (Radio Frequency). Radiotiellä IEEE 802.11 käyttää sekä suorasekvenssihajaspektriä DSSS (Direct Sequence Spread Spectrum) että taajuushyppelyä FHSS (Frequency Hopping Spread Spectrum). Radioaaltoja käytetään, koska ne läpäisevät seiniä ja muita fyysisiä esteitä. Tällä saavutetaan se etu, ettei tukiaseman ja työaseman välillä tarvitse olla näköyhteyttä, joten verkkoa voidaan käyttää myös muista huoneista käsin. Toiseksi siirtotavaksi standardi määrittelee 850–950 nm aallonpituudella toimiva IR:n (Infra Red). IR vaatii näköyhteyttä tukiaseman ja työaseman välillä ja tästä johtuen sen käyttö on jäänyt marginaaliseksi radioon verrattuna. /3/

Fyysinen kerros jakautuu kahteen alikerrokseen, ylempänä olevaan PLCP (Physical Layer Convergence Procedure) kerrokseen sekä alempana sijaitsevaan PMD (Physical Medium Dependent) kerrokseen. Näistä PMD-kerroksen toiminnot jakautuvat useammalle alemmalle kuljetusteknologialle, mutta PLCP-kerroksen tehtävät ovat samoja kaikille toteutuksille. Hajaspektritekniikassa jokainen käyttäjä

levittää lähetteensä koko taajuusalueelle, jolloin kukaan ei voi hallita koko kaistaa. Vapaat alueet ovat 2,400 – 2,485 GHz sekä 5,725 – 5,825 GHz, mutta näille on erilaisia maakohtaisia laajennuksia ja rajoituksia. /3/

Suorasekvenssihajaspektri- eli DSSS-tekniikassa lähete levitetään laajalle kaistalle, jolloin menetelmän häiriönsietokyky kasvaa. Hyvän häiriönsietokyvyn saaminen 20 MHz kaistalle mahdollistaa vain pienen siirtonopeuden. 20 MHz taajuuskaistaa käytettäessä samalle kuuluvuusalueelle mahtuu vain kolme eri järjestelmää. Euroopassa on käytössä 13 kanavaa, joille voidaan asettua, sillä rinnakkaisten järjestelmien keskitaajuuksien tulee olla vähintään 25 MHz jotta ne eivät häiritsisi toisiaan. Suurin sallittu lähetysteho on 100mW EIRP. /3/



Kuva 3-1. DS PLCP–kehys */2/*

3.1.2 Siirtotie

IEEE 802.11-verkossa kanavanvarauksen toteuttamista varten on kaksi mahdollista menetelmää, PCF (Point Coordination Function) ja DCF (Distributed Coordination Function).

Keskeisenä ajastimena toimii NAV (Network Allocation Vector). Tämän ajastimen ollessa viritettynä laite ei saa lähettää mitään sanomia siirtotielle. Kaikissa linjalla siirtyvissä sanomissa on kerrottuna tapahtuman kesto ja NAV viritetään asettamalla tämä kesto ajastimeen. Käytössä on myös 4 erilaista viivettä.

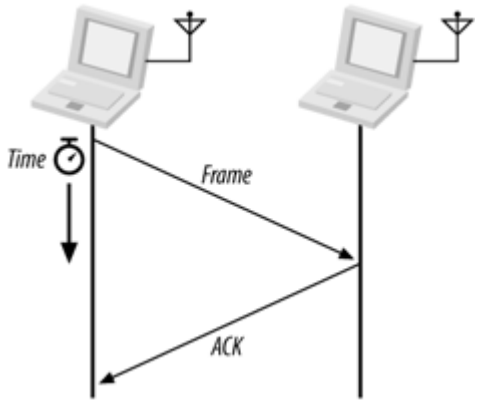
1. SIFS (Short InterFrame Space). Viiveen pituus on 28 µs ja sitä käytetään tapahtuman sisällä. Vastaus sanomaan pitää tulla tämän 28 µs aikana tai sanoman odotetaan törmänneen tai vääristyneen.

2. PIFS (Point Coordination IFS) on tukiaseman käyttämä viive. Viiveen pituus on 78 μs, joten tukiasema pystyy aina ottamaan siirtotien haltuunsa ennen verkon muita laitteita.
3. DIFS (Distributed IFS) on viive, jonka asema joutuu odottamaan ennen sanoman lähettämistä siirtotielle. DIFS on SIFS + 2 aikaväliä.
4. EIFS (Extended IFS) on viive, jota käytetään siinä tapauksessa kun asema ei osaa tulkita saamaansa sanomaa. Tämä viive estää työasemaa lähettämästä sanomia kesken tapahtuman siinä tapauksessa, että se on tulkinnut verkossa olevan tilanteen väärin. EIFS on viiveistä pisin ja se kestää useiden aikavälien ajan.

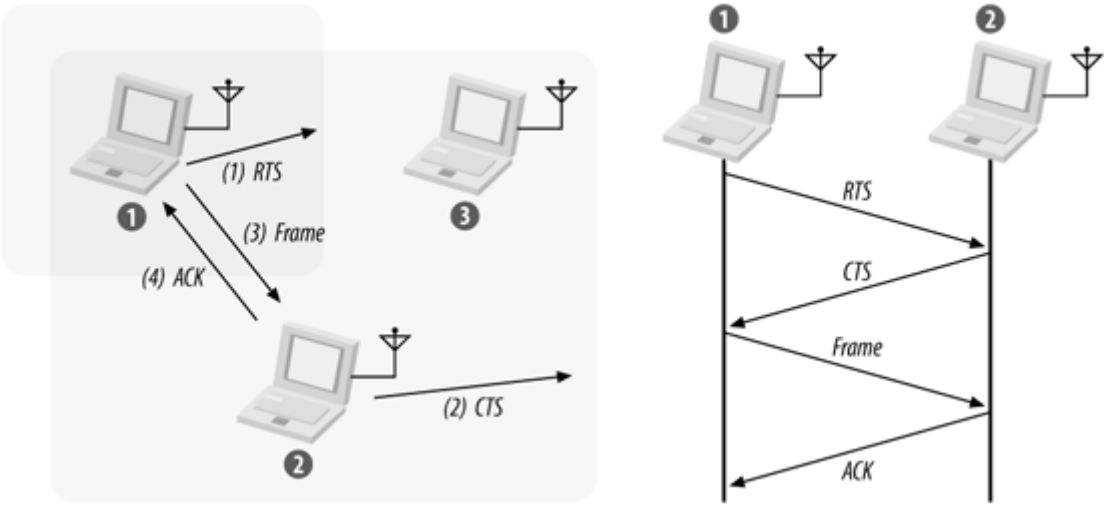
Törmäyksiä CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)-protokollaa käytettäessä tapahtuu, vaikka niitä pyritään välttämään. Törmäyksistä toipuminen onnistuu, kunhan vastapuolet toimivat eri tavoin. Jos vastapuolet toimisivat törmäyksen jälkeen samalla tavalla, uusi törmäys olisi väistämätön. IEEE 802.3-verkoissa on käytössä CSMA/CD (Carrier Sense Multiple Access / Collision Detection), josta tuttua ns. eksponentiaalista toipumista käytetään myös 802.11-verkoissa. Uudelleenlähetyksen ajankohta (n) valitaan satunnaisesti lukujen 0 ja i-1 väliltä. Kun n aikaväliä on kulunut, laite voi lähettää uudestaan. Aikavälin pituus on 50 μs, joka on sellainen aika, että laite kuulee, jos toinen osapuoli on aloittanut lähettämisen edellisellä aikavälillä. Aluksi i:n arvoksi asetetaan 1, jolloin ensimmäisen törmäyksen jälkeen on valittavana toinen aikaväleistä 0 ja 1. Toisen törmäyksen jälkeen valittavana taas on yksi 0-3 aikavälistä, ja tätä toistetaan niin kauan, kunnes lähetys saadaan onnistumaan tai törmäysten maksimimäärä täyttyy. 802.11-verkoissa jokainen toimitettu kehys tulee kuitata (Kuva 3-2). /3/

Hajautetussa hallinnassa kanavan varaus alkaa kuuntelemalla kanavaa DIFS -viiveen ajan. Jos kanava on vapaa tämän ajan, voidaan sanoma lähettää, jos taas kanavalla on liikennettä, siirrytään eksponentiaaliseen toipumiseen. Vapaalle siirtotielle lähetetään RTS (Request To Send)-sanoma, johon odotetaan vastausta CTS (Clear To Send) SIFS-viiveen ajan. Jos vastausta ei kuulu, oletetaan törmäyksen tapahtuneen ja siirrytään eksponentiaaliseen toipumismenettelyyn. Datan lähettämisen jälkeen kuittausta odotetaan SIFS-viiveen ajan, jos kuittausta ei tule, siirrytään

eksponentiaaliseen toipumismenetelmään. Lähetyksen päätteeksi suoritetaan vielä eksponentiaalinen toipumismenettely (Kuva 3-3). /3/



Kuva 3-2. 2-vaiheinen tapahtuma */2/*



Kuva 3-3. 4-vaiheinen tapahtuma */2/*

Keskitetyssä hallinnassa (PCF) tukiasema varaa liikennettä esim. sen mukaan, jos verkossa tarvitaan vapaata siirtotietä puheen tai videon siirtämistä varten. Tukiasema ottaa siirtotien haltuunsa lähettämällä beacon -sanomassa tiedotteen keskitetyn hallinnan alkamisesta ja kestosta. Tämän keston asiakkaat lisäävät omiin NAV-ajastimiinsa. Yhden kyselykierroksen aikana tukiasema ja työasema voivat vaihtaa yhden datasanoman. Jokaista datasanomaa varten tarvitaan siis uusi kyselykierros. /3/

3.1.3 Komponentit

Asiakkaat. Verkot rakennetaan siirtämään dataa asiakkaiden välillä. Tyypillisesti asiakkaat ovat kannettavia laitteita, kuten kannettavia tietokoneita, matkapuhelimia ja PDA-laitteita. Myös pöytäkoneita liitetään langattomasti verkkoon kun halutaan välttyä kaapelin vetämiseltä.

Tukiasemat. Tukiasemien tärkeimpänä tehtävänä on hoitaa siltaaminen langattoman ja langallisen verkon välillä. Tukiasemien tehtäväksi jää myös tiedon salaaminen ja purkaminen sen liikkuessa langattomaan verkkoon ja sieltä pois.

Siirtotie. Liikennöintiin käytetään pääasiassa radiotaajuuksilla toimivaa langatonta siirtotietä. Myös infrapuna on käytetty siirtotie.

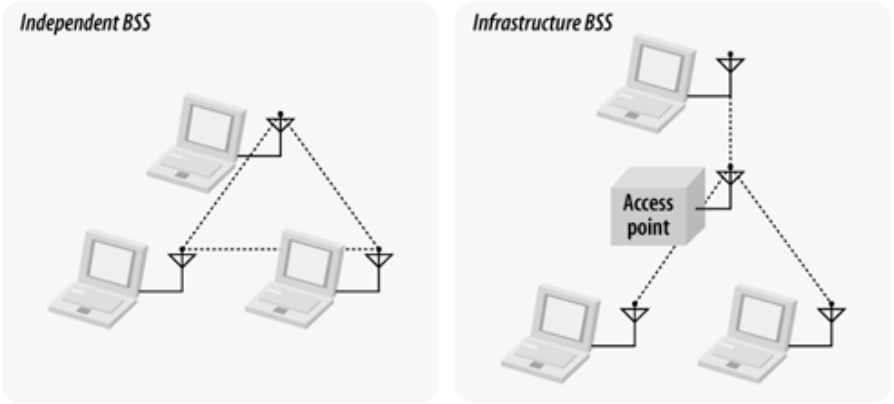
Jakelujärjestelmä. Useiden tukiasemien verkossa tukiasemien pitää pystyä kommunikoimaan keskenään jäljittäessään liikkuvan asiakkaan liikkeitä. 802.11 standardi ei määrittele tarkemmin käytettävää jakelujärjestelmää, mutta yleensä jakelujärjestelmänä toimii olemassa oleva fyysinen verkko, jossa on käytössä Ethernet teknologia.

3.1.4 Verkkotopologiat

IEEE 802.11-verkot koostuvat ns. peruspalveluryhmistä (BSS, Basic Service Set). Langattomat verkot erotellaan toisistaan palveluryhmätunnuksilla (SSID, Service Set Identifier). SSID on verkkonimi, jonka avulla tunnistetaan samaan loogiseen verkkoon kuuluvat laitteet. Standardissa määritellään kolme verkkotopologiaa, IBSS, Infrastructure BSS sekä ESS.

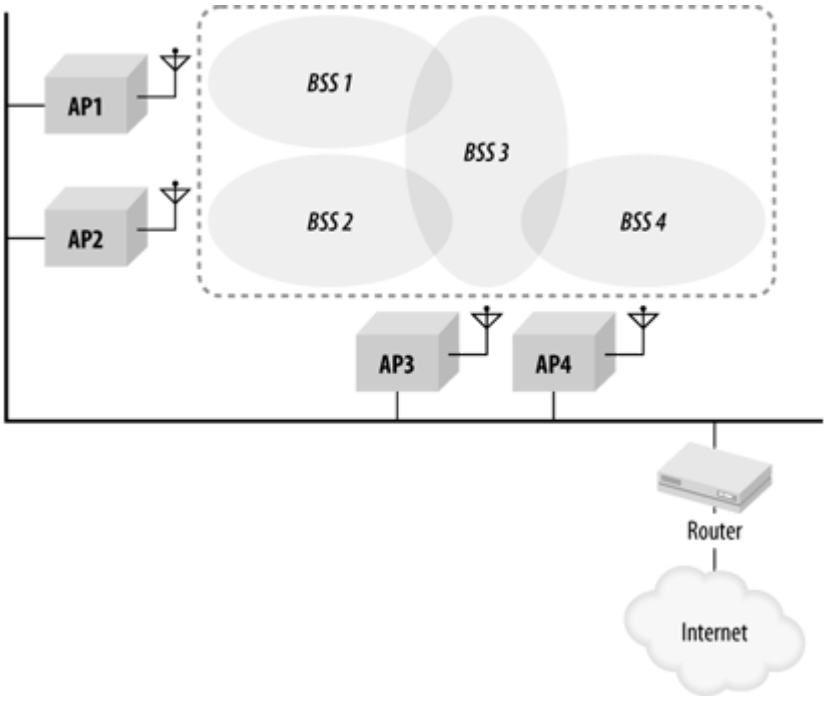
IBSS tunnetaan myös nimellä Ad-Hoc (Kuva 3-4). IBSS-verkossa asiakkaat kommunikoivat suoraan toistensa kanssa. Pienin mahdollinen IBSS-verkko koostuu vain kahdesta asiakaslaitteistosta. Tyypillisesti IBSS-verkko koostuu pienestä määrästä laitteita ja se perustetaan yleensä vain lyhyeksi ajaksi. /2/

Infrastructure BSS (Kuva 3-4) on yleisin pienissä verkoissa käytetty verkkotopologia, joka pitää sisällään vain yhden tukiaseman, johon kaikki asiakaslaitteet yhdistyvät. Kaikki verkossa liikennöity data kulkee tukiaseman kautta, meni se sitten samassa langattomassa verkossa olevalle toiselle asiakkaalle tai jakelujärjestelmän puolelle kiinteään verkkoon. Verkon alueella asiakaslaitteiden ei tarvitse olla toistensa kantamalla liikennöidäkseen keskenään, mutta molempien on oltava tukiaseman kantamalla. Verkkoon yhdistäessä asiakaslaitteet assosioituvat tukiaseman kanssa saadakseen verkon palvelut käyttöönsä. /2/



Kuva 3-4. IBSS- ja Infrastructure BSS-verkot /2/

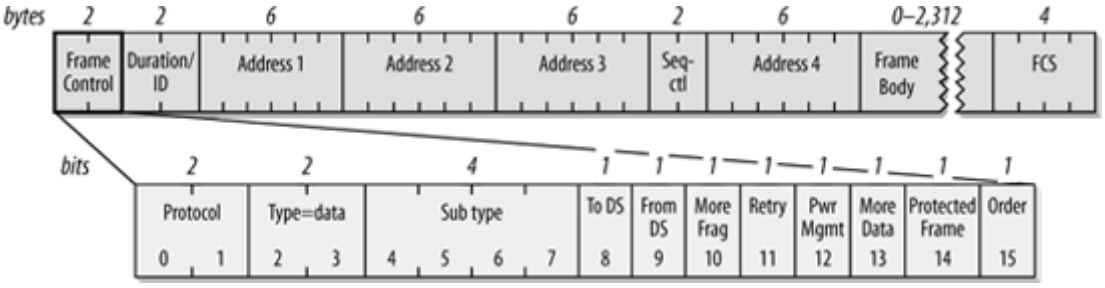
ESS-verkkoon (Kuva 3-5) kuuluu vähintään kaksi infrastruktuuriverkkoa, jotka molemmat on sidottu samaksi loogiseksi verkoksi saman SSID:n kanssa. ESS-verkon kaikki tukiasemat on kytketty samaan runkoverkkoon, jonka kautta liikenne kulkee eri tukiasemiin yhdistäneiden asiakkaiden välillä. Verkosta liikennöidään ulos runkoverkossa sijaitsevan reitittimen kautta. /2/



Kuva 3-5. ESS */2/*

3.1.5 Verkon sanomat

Fyysisellä tasolla siirrettävät kehykset kuljettavat hyötykuormassaan MAC PDU-sanomia (Medium Access Control Protocol Data Unit) (Kuva 3-6). Käytössä on neljä sanomatyyppiä, Datasanoma, RTS-sanoma, CTS-sanoma sekä ACK-sanoma.



Kuva 3-6. MAC -kehys ja Frame Control-kenttä */2/*

Datasanoman sisällä kehyksen hyötykuormassa siirretään dataa laitteelta toiselle. Datasanoman suurin sallittu pituus on 2346 tavua ja minimissään se on 29 tavua.

Duration-kenttä kertoo sanoman keston mikrosekunneissa sanoman alkamisesta sanoman kuittaamiseen. Tämä kesto siirretään NAV–ajastimeen, ja sen tulee kattaa koko sanoman toimitus & kuittaus.
Address 1-kenttä sisältää vastaanottajan MAC-osoitteen tai AP:n kattaman solun tunnisteen BSSID (Basic Service Set ID).
Address 2-kenttä pitää aina sisällään sanoman lähettäjän MAC-osoitteen tai AP:n kattaman solun BSSID-tunnisteen.
Address 3-kentän sisältö on sanoman alkuperäinen lähettäjä siinä tapauksessa, jos kenttien ToDS ja FromDS arvo on 1
Address 4-kenttä on käytössä vain silloin, kun kaksi tukiasemaa yhdistetään toisiinsa langattomasti. Tällöin osoitekentät 1 ja 2 sisältävät vastaanottavan ja lähettävän tukiaseman tunnukset ja osoitekentät 3 ja 4 sisältävät lopullisen vastaanottajan ja lähettäjän MAC-osoitteet.
Seq-ctl-kenttä pitää kirjaa lähetetyistä MAC-sanomista, sanoman yksilöivä osa on 4-bittinen sekä toinen, 12-bittinen, osa kasvaa järjestyksessä jokaisen sanoman lähettämisen jälkeen, näin voidaan havaita puuttuvat sanomat.
FCS-kehystarkiste lasketaan CRC-jakojäännösmenetelmällä, ja siihen sisällytetään sekä MAC-otsikko että hyötykuorma. /3/

RTS-sanoma kertoo vastaanottajalle alkavasta tiedonsiirrosta ja ohjaustiedon lisäksi se sisältää myös seuraavat kentät: sanoman kesto, vastaanottajan tunnus, lähettäjän tunnus sekä FCS-kehystarkiste.

CTS-sanomaa käytetään vastaamaan RTS-sanomaan. Sanoma kertoo lähettäjälle, että RTS-sanoma on vastaanotettu ja samalla se kertoo lähetyksen alkamisesta sellaisille laitteille, jotka eivät ole RTS-sanoman lähettäjän kuuluvuusalueella. Tästä sanomasta löytyy seuraavat kentät: kesto, vastaanottajan tunnus sekä FCS -kehystarkiste.

ACK–sanomalla kuitataan vastaanotettu sanoma. Sanomassa ilmoitetaan sanoman kesto, joka on tavallisessa sanomassa 0. Siirrossa, jossa on dataa fragmentoitu kenttä "More Fragments" saa arvon 1, jolloin ACK-sanoman kestoon asetetaan yhden datasanoman kesto, kuittauksen kesto sekä kaksi SIFS-viivettä. Näin lähettäjä voi lähettää toisen sanoman samalla varauspyynnöllä ilman uutta kanavanvarausta. ACK-sanomassa on myös vastaanottajan tunnus sekä FCS-kehystarkiste. /3/

3.1.6 Palvelut

IEEE 802.11-standardi määrittelee yhdeksän palvelua. Näistä palveluista kolmea käytetään tiedon siirtämiseen. Jäljelle jääneet kuusi palvelua on tarkoitettu hallinnollisiin operaatioihin. Palvelut jaetaan kahteen pääryhmään, asemapalveluihin ja jakelujärjestelmäpalveluihin.

Asemapalveluita tulee jokaisen 802.11-yhteensopivan aseman tarjota. Palvelut on toteutettu langattomassa asemassa ja tukiasemien langattomassa rajapinnassa. Asemapalveluihin luetaan neljä palvelua, MSDU (MAC Service Data Unit) toimitus, todentaminen (Authentication), todennuksen purkaminen (Deauthentication) sekä luottamuksellisuus (Confidentiality). /2/

MSDU toimitus on peruspalvelu, jonka vastuulla on tiedon toimittaminen vastaanottajalle.
Todentaminen on tärkeässä roolissa langattomien verkkojen tietoturvassa. Langalliseen verkkoon liittyminen voidaan estää pelkästään estämällä pääsy verkon liityntäpisteisiin, mutta langattoman verkon ollessa kyseessä tämä ei onnistu. Tästä johtuen langattomissa verkoissa on käytettävä erilaisia todentamismenetelmiä varmistamaan käyttäjän oikeus käyttää langatonta verkkoa.
Todennuksen purku päättää todennetun ja assosioidun yhteyden.
Luottamuksellisuus oli alun perin määritelty yksityisyydeksi, jonka WEP:n (Wired Equivalent Privacy) oli määrä tarjota. Fyysinen yhteys langattomaan verkkoon on verrattavissa oikean antennin ja modulaatiomenetelmän käyttämiseen. /2/

Jakelujärjestelmäpalvelut yhdistävät tukiasemat jakelujärjestelmään. Tukiasemien päärooli on ulottaa langallisen verkon palvelut langattoman verkon puolelle. Tämä on toteutettu tuottamalla jakelu- ja yhdistämispalvelut langattomalle puolelle. Yhteyksien ylläpitämiseen ja langattomien asemien paikantamiseen jakelujärjestelmä tarjoaa assosioinnin (Association), uudelleen assosioitumisen (Reassociation), assosioinnin purkamisen (Disassociation), jakelun (Distribution) sekä yhdistämisen (Integration). /2/

Jakelupalvelua käytetään joka kerta, kun lähetetään dataa infrastruktuuri-verkossa. Kun tukiasema on ottanut kehyksen vastaan, se käyttää jakelupalvelua hyväksi toimittaakseen kehyksen vastaanottajalle. Jakelupalvelua käytetään aina, kun tukiaseman läpi liikennöidään, vaikka kyseessä olisi kaksi asiakasta saman tukiaseman kantamalla.

Yhdistämispalvelu on jakelujärjestelmän tuottama palvelu, joka mahdollistaa yhdistämisen muihin kuin IEEE 802.11-verkkoihin. Yhdistämispalvelua ei ole määritelty standardissa muuten, kuin että se on pakko tarjota.

Assosiointi on asiakkaan rekisteröinti tukiaseman kanssa. Jakelujärjestelmä voi rekisteröinnin jälkeen käyttää rekisteröintitietoja hyväkseen asiakkaan yhdistämisessä tiettyyn tukiasemaan.

Uudelleenassosiointi tapahtuu liikuttaessa ESS:n sisällä tukiasemalta toiselle. Uudelleenassosiointi on asiakkaan aloittama tapahtuma, kun signaalin vahvuus sitä edellyttää.

Assosioinnin purku on käytössä olevan yhteyden purkamista varten. Assosioinnin purkamisen yhteydessä jakelujärjestelmästä poistetaan kaikki tiedot assosioituneesta asiakkaasta ja purkamisen jälkeen asiakas ei ole enää liittyneenä verkkoon. /2/

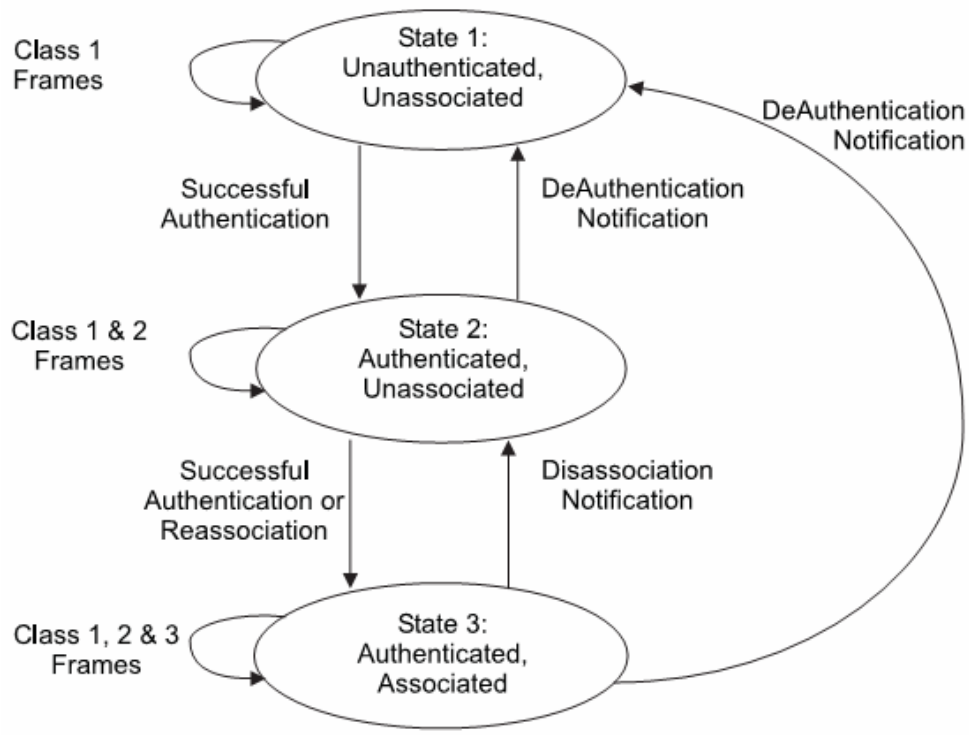
3.1.7 Palveluiden väliset riippuvuudet

Kuvassa (Kuva 3-7) on esitettynä langattoman aseman tilakaavio. Tilakaavion tilojen välinen vaihtelu tapahtuu eri palveluiden (Authentication, Deauthentication, Association, Reassociation, Deassociation) käytön perusteella.

Asema aloittaa todentamattomasta ja assosioimattomasta tilasta (State 1). Ensimmäinen askel on todentaa asema käyttämällä todentamispalvelua. Todentamisen eri vaiheet vaihtelevat tukiaseman ja jakelujärjestelmän käyttämän todentamismenetelmän vaatimusten mukaisesti. Onnistuneen todentamisen jälkeen asema siirtyy tilaan 2 (State 2), jossa edessä on assosiointi. Assosioinnin tapahduttua asema on täydessä toimintakunnossa.

Tilasta 3 (State 3) vaihdetaan pois tapahtumilla assosioinnin purku sekä todennuksen purku. Nämä kaksi tapahtumaa ovat huomautuksia, jotka on pakko hyväksyä.

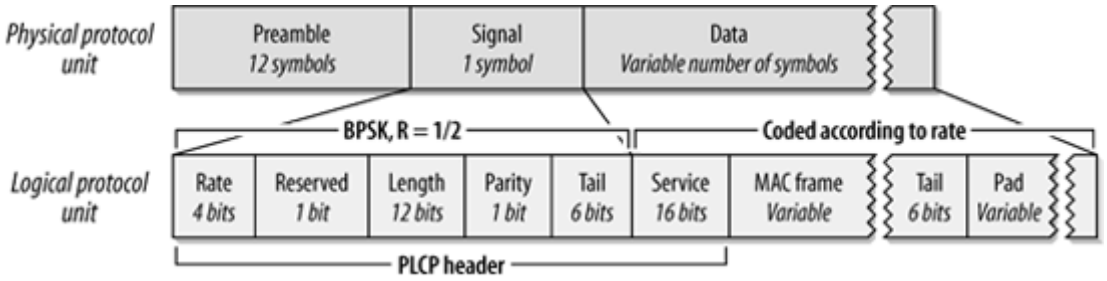
Kuvassa (Kuva 3-7) on kerrottu kehyksille (Frames) eri luokkaa, 1, 2 ja 3. Jokaisessa tilassa voidaan vaihtaa assosiointikehyksiä. 1. luokan kehykset pitävät sisällään välttämättömiä tiedotteita, kuten tiedustelusanomia (Probe), majakkasanomia (Beacon), todentamiseen käytettäviä sanomia (Authentication, Deauthentication). 2. luokassa sijaitsevat kaikki assosioitumiseen liittyvät sanomat (Association, Disassociation, Reassociation). 3. luokassa on vain datakehyksiä. /1/



Kuva 3-7. Aseman tilakaavio */6/*

3.2 IEEE 802.11a

IEEE 802.11-standardiin lisättiin laajennus vuonna 1999. IEEE 802.11a on fyysisen tason laajennus, joka sallii 5 GHz taajuusalueella siirtonopeudeksi 54 Mbps. Laajennus perustuu OFDM-tekniikkaan, jossa suuritaajuuksinen kanava jaetaan useisiin alakanaviin. Jokaista alikanavaa käytetään tiedon siirtämiseen. Kaikki hitaat alikanavat niputetaan yhteen yhdeksi nopeaksi kanavaksi. Jokainen 20 MHz kanava koostuu 52 rinnakkaisesta apukantoaallosta, joista 48 on käytettävissä datan siirtoon.



Kuva 3-6. IEEE 802.11a-kehys */2/*

Otsikko siirtyy aina 6 Mbps nopeudella, kun taas PLCP-otsikon nopeus (Rate)-kenttä kertoo hyötykuorman nopeuden. Eri nopeuksilla on käytössä myös eri modulaatiot. 6 - 9 Mbps – BPSK, 12 - 18 Mbps – QPSK, 24 - 36 Mbps – 16QAM, 48 - 45 Mbps – 64 QAM. /3/

3.3 IEEE 802.11b

Vuonna 1999 IEEE 802.11 sai laajennuksen 802.11b, joka on fyysisen tason laajennus. Laajennus tukee siirtonopeuksia 5,5/11 Mbps. Suositus määrittelee myös tavan pudottaa nopeutta 802.11-perussuosituksen mukaisiin nopeuksiin 1 Mbps ja 2 Mbps. Linjalla siirrettävä sanoma on identtinen DSSS -peruskehyksen kanssa, mutta signaali (Signal)-kentän arvojoukkoa on laajennettu tukemaan uusia siirtonopeuksia. 5,5 ja 11 Mbps nopeudet käyttävät CCK (Complementary Code Keying)-modulointia. /3/

3.4 IEEE 802.11g

Kesäkuussa 2003 hyväksyttiin laajennus 802.11g. Laajennus ei muuta vanhoja spesifikaatioita, eikä oikeastaan ole vain yksi fyysisen tason laajennus lisää. Standardissa on monta eri fyysistä laajennusta yhteensopivuuden aikaansaamiseksi vanhempien järjestelmien kanssa. Tässä laajennuksessa tuetut siirtonopeudet ovat 1, 2, 5.5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48 ja 54 Mbps. Standardi määrittelee käytettäviksi modulaatiomenetelmiksi DSSS, CCK sekä OFDM riippuen siitä, missä verkossa toimitaan. /9/

3.5 Tulevat standardit

IEEE-työryhmällä on tällä hetkellä standardointityön alla suuri määrä eri standardeja liittyen 802.11-standardin laajennuksiin. /4/ Mainitsen näistä nyt 802.11n-laajennuksen, joka on myös fyysinen tason laajennus. Tulevalla laajennuksella pyritään saamaan läpäisykyky jopa 100 Mbps asti. /5/ Standardi on määrä saattaa hyväksyttäväksi kesäkuussa 2009.

4 TIETOTURVA

4.1 Tietoturvan käsitteitä

Perustavanlaatuisia tietoturvan käsitteitä on luottamuksellisuus (Confidentiality), eheys (Integrity) sekä saatavuus (Availability). Langattomien verkkojen ollessa kyseessä pitää laskea mukaan myös todentaminen (Authentication), oikeuttaminen (Authorization) sekä pääsyn valvonta (Access Control). Usein saatavuus mielletään siirron laadun takaamisena (QoS) eikä tietoturvaongelmana. Salaustekniikka on keino saavuttaa nämä edellä mainitut tietoturvatavoitteet. /1/

Luottamuksellisuus on kyky lähettää ja vastaanottaa tietoja kenenkään asiaankuulumattoman niitä näkemättä. Tämä saavutetaan salauksella, symmetrisellä sekä epäsymmetrisellä.

Eheys on kyky lähettää ja vastaanottaa tietoja ilman, että kukaan asiaankuulumaton on päässyt muokkaamaan siirrettävää dataa lähettäjän tai vastaanottajan sitä huomaamatta. Dataa voidaan muokata jos pelkästään eheys on ainoa tarkkailtava asia, mutta eheyden tarkistaminen paljastaa datan muokkaamisen. Eheyden tarkastus suoritetaan digitaalisilla allekirjoituksilla ja yhteen suuntaan toimivilla tiivistefunktioilla. /1/

Saatavuus on tässä yhteydessä kyky lähettää ja vastaanottaa tietoa. Siirtotien ylimääräinen kuormitus voi aiheuttaa sen, ettei tietoja voida enää lähettää. Erilaisilla siirron laadun varmistavilla työkaluilla tai palvelunestohyökkäykset tunnistavilla työkaluilla voidaan tätä ongelmaa helpottaa. /1/

Todentaminen on vastapuolen tunnistamista, että vastapuoli on todellakin se, kuka hän väittää olevan. Eheyden tarkastamiset ovat usein merkityksettömiä jos vastapuolen henkilöllisyyttä ei pystytä todentamaan. IEEE 802.11-verkoissa voidaan käyttää monia erilaisia protokollia käyttäjän todentamista varten. Tähän

tarkoitukseen voidaan käyttää esim. 802.1x, RADIUS, EAP, PAP/CHAP, MS-CHAP jne. /1/

Oikeuttaminen on sidottu yhteen todentamisen kanssa. Oikeuttaminen kertoo todentamisen jälkeen mitä saat tehdä. Oikeuttaminen ei aina vaadi todentamista, mutta käytännössä nämä yleensä kulkevat käsi kädessä.

Pääsyn hallinta on kyky hallita käyttäjän pääsyä resursseihin erilaisten ominaisuuksien perusteella. Erilaisia keinoja tämän toteuttamiseen on useita.

Salakirjoitus tai salaus on keino muuttaa tieto jollakin algoritmilla sekalaiseksi joukoksi bittejä. Salattua tietoa kutsutaan salatekstiksi. Salauksen purkaminen on päinvastainen operaatio salaukselle, jolla sekalaisesta salatekstistä saadaan taas luettavaa tietoa. Tiedon salaamista varten on olemassa tehottomia ja vähän tehokkaampia salausalgoritmeja. Ongelmia muodostuu todentamisen yhteydessä, kun pitäisi olla varma osapuolen henkilöllisyydestä. Jos todentamiseen halutaan luottaa, salaus on välttämätön. /1/

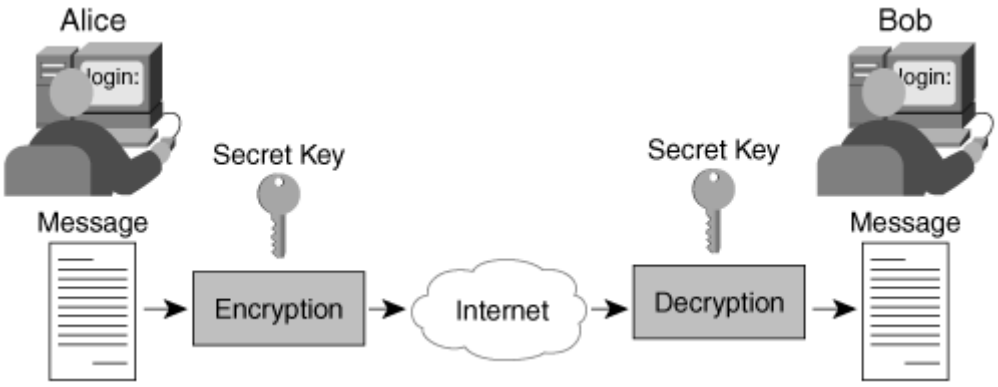
Avainten hallinta on osana salakirjoitusta. Avain on digitaalinen koodi, jota voidaan käyttää tiedon salaamiseen, salauksen purkamiseen ja tiedon allekirjoittamiseen. Joitakin avaimia säilytetään yksityisinä, toiset avaimet taas kerrotaan julkisesti kaikille, joilla voidaan salata vastaanottajalle lähetettävät tiedot. Avaimet toimivat pareina, tietyllä julkisella avaimella salattu tieto voidaan avata vain tietyllä yksityisellä avaimella. Turvallinen avaintenhallinta on langattomissa verkoissa haaste, ja sen pitää samalla myös toimia automaattisesti. /1/

4.2 Salakirjoitus

Salakirjoituksessa salattava tieto ajetaan tietyn algoritmin läpi, jolloin ulos saadaan sekalainen jono merkkejä, jotka eivät ole luettavissa selkokielellä. Erilaisia salausalgoritmeja on olemassa suuri määrä. Salausalgoritmit voidaan jakaa kahteen pääryhmään: symmetrisiin ja epäsymmetrisiin salausmenetelmiin. /1/

Symmetriset salausmenetelmät käyttävät samaa avainta tiedon salaamiseen ja salauksen purkamiseen. Symmetriset salausmenetelmät ovat huomattavasti epäsymmetrisiä salausmenetelmiä nopeampia. Symmetriset salausmenetelmät voidaan jakaa vielä kahteen ryhmään: lohkosalaimiin sekä jonosalaimiin. Lohkosalaimilla salattava tieto jaetaan lohkoihin, jotka jokainen salataan erikseen, jonosalaimissa tieto salataan periaatteessa tavu kerrallaan. /1/

Kuvassa (Kuva 4-1) on kaksi henkilöä, Alice ja Bob. He ovat sopineet käytettävästä salausmenetelmästä etukäteen ja samaa algoritmia käytetään niin tiedon salaamiseen, kuin purkamiseen. Molemmilla on myös tiedossa käytettävä salausavain, jolla tieto salataan ja puretaan. /1/



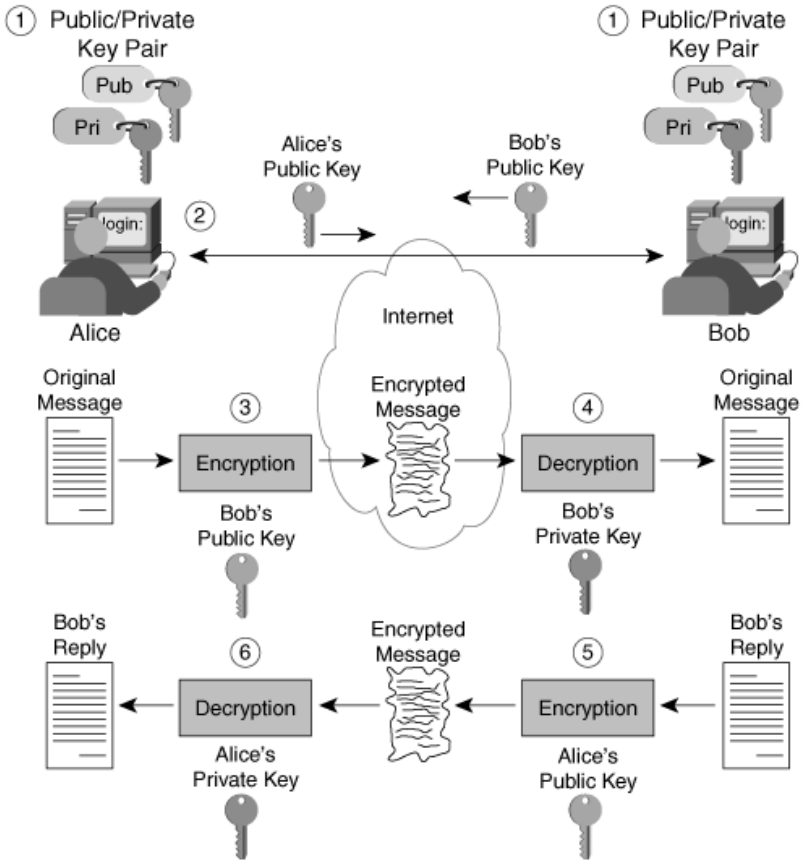
Kuva 4-1. Symmetrinen salaus */1/*

Yleisimmin käytössä olevat symmetriset salausmenetelmät ovat AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES), RC4 (Rivest Cipher 4) ja IDEA (International Data Encryption Algorithm). Näistä AES sekä RC4 otetaan tarkempaan tarkasteluun kappaleessa 5.2, koska näitä kahta käytetään IEEE 802.11-verkoissa salausalgoritmeina. /1/

Epäsymmetrisiä salausmenetelmiä kutsutaan yleisesti myös julkisen avaimen menetelmäksi. Epäsymmetrisessä salauksessa käytetään kahta avainta, kaikille jaettavissa olevaa julkista avainta ja varmasti tallessa pidettävää yksityistä avainta. Näillä avaimilla on riippuvuus toisiinsa, tietyllä julkisella avaimella salattu tieto voidaan avata vain saman avainparin yksityisellä avaimella. /1/

Epäsymmetriset menetelmät ovat yleensä käytössä tiedon eheyden säilyttämisessä, tiedon luottamuksellisuuden säilyttämisessä, lähettäjän kiistämättömyydessä sekä lähettäjän todentamisessa.

Kuvassa (Kuva 4-2) ovat Alice ja Bob vaihtamassa tietoja keskenään. Koko operaatio lähtee liikkeelle yksityisten ja julkisten avainten luonnilla. Tämän jälkeen osapuolet vaihtavat keskenään toistensa julkisia avaimia. Alice kirjoittaa Bobille viestin ja käyttää tämän viestin salaamiseen Bobin julkista avainta. Salaamisen jälkeen viesti lähetetään vastaanottajalle, jossa Bob pystyy purkamaan viestin omalla yksityisellä avaimellaan. Bob kirjoittaa vastauksen Alicelle ja salaa kirjoittamansa viestin Alicen julkisella avaimella ja lähettää Alicelle. Viestin vastaanotettuaan Alice voi käyttää omaa yksityistä avainta purkaakseen viestin. /1/



Kuva 4-2. Eheyden ja luottamuksellisuuden varmistaminen */1/*

Vasta tällä menetelmällä voidaan saavuttaa tiedon eheys ja luottamuksellisuus, koska viestin purkamiseksi ulkopuolinen hyökkääjä tarvitsisi myös vastaanottajan yksityisen avaimen tietoonsa. Ongelmia aiheuttaa se, kun ulkopuolinen henkilö voi

lähettää Bobille tietoja salaamalla ne Bobin julkisella avaimella. Tästä syystä Alicen henkilöllisyys pitää jotenkin varmistaa, jotta voidaan olla varmoja, että ollaan tekemisissä juuri Alicen kanssa. /1/

Todentaminen onnistuu kuvan 4-2 kaltaisella järjestelyllä, jossa ensimmäisen viestin lähettäjänä toimiva Alice salaa viestin käyttäen omaa yksityistä avaintaan. Tämän jälkeen Bob voi purkaa viestin Alicen julkisella avaimella. Tämä todistaa, että viesti todellakin on Alicelta lähtöisin – hänen julkisella avaimella se saadaan auki. Avainten ollessa julkisia, kuka tahansa voisi purkaa nämä viestit julkisten avainten avulla. Jotta eheys ja luottamuksellisuus saadaan säilytettyä sekä halutaan varmistua lähettäjän tunnistamisesta, pitää viesti salata kahteen kertaan. Ensimmäisen kerran salaus suoritetaan vastaanottajan julkisella avaimella ja tämän jälkeen vielä lähettäjän yksityisellä avaimella. Jokainen siis pystyy purkamaan ensimmäisen salauksen, mutta ei enää toista salausta, joka aukeaa vain vastaanottajan yksityisellä avaimella. /1/

Julkisen avaimen menetelmiä käytetään salaamaan symmetristä salausta varten vaihdettavat salausavaimet. Yleisiä julkisen avaimen algoritmeja ovat RSA (Ron Rivest, Adi Shamir, Leonard Adleman) sekä El Gamal. /1/

4.3 Digitaaliset allekirjoitukset ja tiivistefunktiot

Tiivistefunktioita käytetään laskemaan kiinteämittainen tarkistesumma tiivistealgoritmiin syötetystä viestistä. Tiivistealgoritmin pitää täyttää muutamia ehtoja sopiakseen tiivisteiden laskemista varten. Tiivistealgoritmin pitää tuottaa samasta syötteestä aina sama vaste. Funktiossa pitää olla myös sattumanvaraisuutta estääkseen alkuperäisen viestin arvauksen. Tiivisteen pitää myös olla uniikki, kaksi eri viestiä ei saa tuottaa samaa tiivistettä. Tiivistefunktiot ovat yksisuuntaisia, eli niiden tuottamaa tiivistettä ei saa laskettua takaisin alkuperäiseen viestiin. Tarkoituksena olisi myös, että pieni muutos alkuperäiseen viestiin tuottaisi suuren muutoksen laskettuun tiivisteeseen. /1/

Tiivistefunktiolla lasketaan viestistä sormenjälki, joka on uniikki tunniste luodulle viestille. Viestistä laskettu tiiviste voidaan toimittaa viestin mukana vastaanottajalle,

joka myös laskee viestistä tiivisteen ja vertaa sitä vastaanotettuun tiivisteeseen. Jos tiivisteet vastaavat toisiaan, viestiä ei ole peukaloitu matkan varrella. Vaarana tässä on Man-in-the-Middle-hyökkäys, jossa ulkopuolinen hyökkääjä kaappaa alkuperäisen viestin, lisää oman sisältönsä viestiin ja laskee uuden tiivisteen. Vastaanottajalle saapuisivat tässä tapauksessa muutettu viesti sekä siitä laskettu tiiviste, joka tietenkin vastaisi vastaanottajan itsensä laskemaa tiivistettä. /1/

Yleisiä käytössä olevia tiivistefunktioita ovat esim. MD5 (Message Digest 5) sekä SHA (Secure Hash Algorithm). MD5 tuottaa 128-bittiä pitkän tiivisteen, kun taas SHA tuottaa 160-bittisen tiivisteen.

Digitaalinen allekirjoitus on salakirjoitettu tiiviste. Digitaalinen allekirjoitus saadaan aikaiseksi laskemalla ensin viestistä yksisuuntainen tiiviste. Tiiviste salataan lähettäjän luomalla julkisella avaimella. Salauksen jälkeen digitaalinen allekirjoitus on valmis. /1/

Vastaanottopäässä paketista erotetaan itse viesti ja digitaalinen allekirjoitus erikseen. Allekirjoituksen salaus puretaan lähettäjän julkista avainta käyttäen ja ulos saadaan lähettäjän laskema tiiviste viestistä. Viesti ajetaan tiivistefunktion läpi, jolloin tästä saatua tiivistettä voidaan verrata salattuna olleeseen tiivisteeseen, jos ne täsmäävät, lähettäjä on tunnistettu ja myös viesti on saapunut muuttumattomana perille. /1/

4.4 Digitaaliset varmenteet ja avaintenhallinta

Avainten vaihtamiseksi turvattoman siirtotien yli käytetään Diffie-Hellman algoritmia. Diffie-Hellman algoritmilla muodostettua avainta voidaan käyttää tietojen salaukseen. /7/

Esimerkissä otetaan avaimia vaihtaviksi osapuoliksi taas Alice ja Bob. Molemmat päättävät keskenään käyttävänsä alkulukua p ja primitiivistä alkiota g. Todellisuudessa luvuksi p valittaisiin huomattavasti suurempi luku, esim. 300 numeroinen luku. Luvuiksi a ja b valittaisiin myös paljon suurempi luku. Luvun g ei tarvitse olla kovinkaan iso. Alkuluvuksi p he valitsevat 23 ja primitiiviseksi alkioksi g luvun 5. /7/

Toisena vaiheena Alice valitsee itselleen salaisen luvun $a=6$ ja lähettää Bobille alkion ja luvun a jakojäännöksen (g^a mod p).

· 5^6 mod 23 = 8.

Myös Bob valitsee itselleen salaisen luvun $b=15$ ja lähettää Alicelle alkion ja luvun b jakojäännöksen (g^b mod p).

· 5^{15} mod 23 = 19.

Näiden vaiheiden jälkeen Alice voi laskea itselleen (g^b mod p)^a mod p.

· (5^{15} mod 23)^6 mod 23 = 2.

Samoin Bob laskee (g^a mod p)^b mod p.

· (5^6 mod 23)^{15} mod 23 = 2.

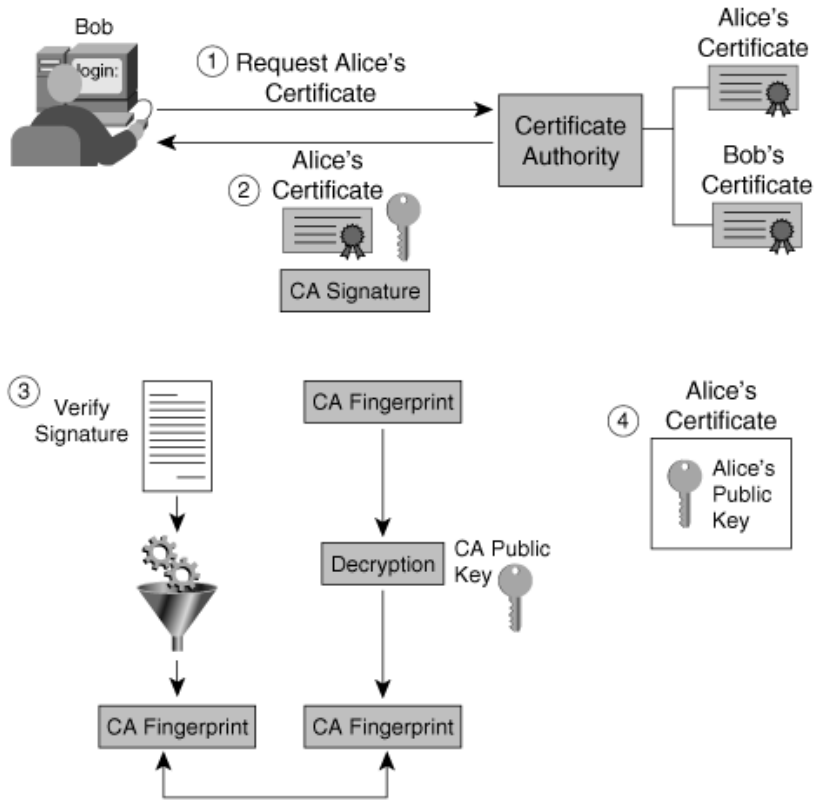
Tässä tapauksessa käytettäväksi salausavaimeksi muodostuu 2. Tätä lukua ei missään vaiheessa siirretä turvattoman siirtotien yli. Salassa pidettäviä lukuja ovat siis a, b ja $g^{ab} = g^{ba}$. Kaikki muu voidaan siirtää selkokielisenä. Ilman osapuolten todentamista tämäkin menetelmä on haavoittuvainen Man-in-the-Middle-hyökkäykselle jossa osapuolten väliin asettuu vihamielinen hyökkääjä, joka neuvottelee molempien osapuolten kanssa avaimet ja voi näin purkaa kaikki osapuolten välillä lähetetyt paketit. /7/

Digitaalisilla varmenteilla on oma standardinsa, ITU-T X.509. Digitaalisilla varmenteilla voidaan todistaa julkisen avaimen haltijan henkilöllisyys. Varmenteesta löytyvät seuraavat tiedot: versionumero, sarjanumero, varmenteen myöntäjä, myöntäjän käyttämän julkisen avaimen algoritmin tiedot, voimassaoloaika, haltijan julkinen avain, julkisen avaimen haltijan käyttämä algoritmi, varmenteen myöntäjän digitaalinen allekirjoitus ja mahdolliset laajennukset. /1/

Varmenteen myöntävä viranomainen (Certificate Authority, CA) on luotettava kolmas osapuoli, joka takaa varmenteen aitouden. Varmenneviranomainen pitää kirjaa varmenteista, jakaa varmenteet sekä kumoaa vanhentuneet tai epäkelvot varmenteet. /1/

Varmenneviranomaisten julkiset avaimet jaetaan yleensä turvallista reittiä pitkin, esim. ohjelmistojen mukana. Kuvassa (Kuva 4-3) käyttäjä Bob noutaa

varmenneviranomaiselta Alicen varmenteen, joka on allekirjoitettu varmenneviranomaisen julkisella avaimella. Bobilla on tiedossa turvallista reittiä saatu varmenneviranomaisen julkinen avain, jolla hän purkaa sormenjäljen suojaamiseen käytetyn salauksen. Bob vertaa hänellä jo olevaa sormenjälkeä varmenteen mukana saatuun sormenjälkeen, jos ne täsmäävät, voidaan olettaa, että Alicen varmenteen sisältävä julkinen avain on aito ja luotettavan tahon takaama. /1/



Kuva 4-3. Varmenteen noutaminen. */1/*

Langattomissa verkoissa IEEE 802.11i esittelee avainten hallintaa varten järjestelmän, joka sallii erillisen todentamisprosessin hoitaa avainten jakelu. Käyttäjän todentamista käydään tarkemmin läpi kappaleessa 5.1. Prosessissa on kaksi vaihetta, ensimmäisenä avaimen muodostaminen sekä toisena uusien avainten vaihtaminen. Ensimmäinen avain syötetään joko käsin tai se saadaan 802.1x protokollan kautta EAP:lla.

802.11i pitää sisällään kahden tyyppisiä avaimia, PMK (Pairwise Master Key) sekä GMK (Group Master Key). PMK on juurena muille, väliaikaisille, unicast-lähetyksissä käytössä oleville avaimille. GMK taas on käytössä, kun luodaan

multicast-lähetyksissä käytettävää avainta, GTK:ta. Avainten pituus vaihtelee käytettävästä salausalgoritmista riippuen. /1/

Jokaista istuntoa varten luodaan erikseen tilapäiset avaimet prosessilla, jota kutsutaan 4-vaiheiseksi kättelyksi. Kättely on neljän EAPOL-sanoman vaihto, jossa varmistetaan, että molemmat osapuolet jakavat saman PMK:n tilapäisten nonce-arvojen vaihtamista varten. 4-vaiheinen kättely alkaa tukiaseman lähettämällä nonce-arvolla, jota ei ole käytetty aikaisemmin saman PMK:n kanssa. Tämän viestin saatuaan asiakas luo oman nonce-arvonsa ja käyttää molempia nonce-arvoja PMK:n kanssa luodakseen väliaikaisen PTK:n (Pairwise Transient Key).
Asiakas vastaa ensimmäiseen viestiin omalla nonce-arvollaan ja todistaa samassa viestissä MIC:llä omistavansa PMK:n. Tukiasema varmistaa asiakkaan kättelyn toisessa toimitetussa vietissä saamansa MIC:n.
Mikäli viestin aitous on varmistettu, tukiasema luo GTK:n (Group Transient Key) multicast-lähetyksiä varten ja lähettää kolmannessa viestissä asiakkaalle luomansa GTK:n, oman nonce-arvonsa, MIC:n sekä RSC:n (Recieve Sequence Counter), joka on GTK:n järjestysluku. RSC:llä pyritään tunnistamaan uudelleen lähetetyt broadcast-viestit.
Asiakas varmistaa tukiaseman toimittavan MIC:n ja asentaa uudet avaimet sekä kuittaa tukiasemalle avainten asennuksen neljännessä viestissä omalla MIC:llä. /1/

Multicast-lähetyksiä varten avaimet luodaan prosessissa, jossa tukiasema lähettää asiakkaalle salattuna uuden avaimen EAPOL-Key viestillä. Samassa viestissä toimitetaan myös tukiaseman laskema MIC sekä RSC. Asiakas kuittaa viestin omalla MIC:llä, jonka jälkeen molemmat asentavat uuden GTK:n käyttöön.

5 TIETOTURVA IEEE 802.11-VERKOISSA

5.1 Käyttäjän todentaminen

Todentamisella voidaan viitata kahteen asiaan, joko laitteen tunnistamiseen tai käyttäjän todentamiseen. Järkeväähän on hoitaa kumpikin operaatio. Jos pelkkä laite todennetaan, ei voida taata varmuutta käyttäjän laillisuudesta. Yleisesti ottaen pääsynhallinta on sitä, että verkkoon joko on pääsy tai sitten ei ole.

IEEE 802.11-standardissa on määritelty kaksi erilaista tapaa autentikointiin, avoin todentaminen ja jaetun avaimen todentaminen. Avoimessa autentikoinnissa ei käyttäjää varsinaisesti edes todenneta mitenkään, mutta kuten kuvasta (Kuva 3-7) nähdään, todennettu tila on edeltävänä tilana ennen assosioitua tilaa, joten tämä tila käydään aina läpi.

Avoimeen autentikointiin voidaan liittää MAC-osoitteen perustuvalla tapahtuva verkkokorttien suodattaminen, mutta kuten kohdassa 5.3.2 on kerrottu, MAC-osoitteiden perusteella suoritettu laillisten korttien suodattaminen ei ole mitenkään luotettava toimenpide. MAC-osoitteiden perusteella tapahtuva valinta on tukiaseman sisäinen toimenpide, jossa tukiasemalla on taulu, johon on talletettu sallitut MAC-osoitteet.

Jaetun avaimen todentamisessa standardi luottaa WEP-infrastruktuuriin. Kappaleessa 5.2.1 käydään tarkemmin läpi WEP ja sen heikot kohdat. Jaetun avaimen todentamista ei voida sanoa käyttäjän autentikoinnin suorittavaksi mekanismiksi, koska sillä voidaan varmistaa vain se, että molemmat osapuolet tietävät salaisen avaimen. Usein WEP-salasana talletetaan koneelle, jolloin sitä ei tarvitse syöttää joka kerta uudelleen. Mikäli esim. kannettava tietokone varastettaisiin, pääsisi hyökkääjä talletetun salasanan turvin verkkoon sisälle varastamallaan koneella.

EAP/802.1x-konseptissa on kolme osapuolta käytössä todentamisen yhteydessä: pääsyä hakeva taho (Supplicant), pääsyn myöntävä taho (Authenticator) sekä pääsyluvan myöntävä taho (Authentication Server). Langattomien verkkojen tapauksessa yleensä pääsyä hakeva taho on WLAN-asiakas, pääsyn myöntävä taho on tukiasema ja pääsyluvan myöntävä taho on todentamispalvelin. Monissa ratkaisuissa tukiasema palvelee niin todentajana kuin todentamispalvelimena. /1/

Pääasiassa pääsyä hakeva taho aloittaa todentamisprosessin aloitusviestillä. Todentamista hoitava tukiasema aloittaa tämän viestin perusteella EAP-viestien vaihdon todentamispalvelimen kanssa. EAP-viestien vaihdon yhteydessä todentamispalvelin päättää todentamisessa käytettävän protokollan. Viestien vaihtamisen jälkeen todentamispalvelin lähettää joko hyväksytty-viestin tai kielletty-viestin. Näiden viestien perusteella todentamista hoitava tukiasema säätää sen, päästetäänkö pääsyä hakeva asiakas verkkoon vai ei. /1/

5.1.1 EAP - Extensible Authentication Protocol

RFC 3748 on nykyään korvannut alkuperäisen RFC 2284:n. /18/ EAP ei ole yksittäinen todentamismekanismi, EAP on todentamista varten rakennetut puitteet, jonka sisäisenä metodina voidaan käyttää useita eri todentamismetodeja. Todentamiseen käytettäviä metodeita löytyy tällä hetkellä n. 40 kappaletta, joista vain muutama käydään läpi. EAP pitää sisällään neljä viestityyppiä: pyynnön (Request), vastauksen (Response), onnistumisen (Success) ja epäonnistumisen (Failure). /19/ /1/

Ennen EAP-viestien vaihtoa pitää pääsyä hakevan ja todentajan muodostaa välilleen yhteys. Viestit vaihdetaan sillä periaatteella, että jokaiseen kyselyyn tulee vastaus ja uutta kyselyä ei toimiteta ennen, kuin edelliseen on vastattu. Yhteyden muodostuksen jälkeen voi esiintyä identiteetin vaihto. RFC ei suosittele luottamaan tähän identiteetin vaihtoon, vaan todentamismekanismien tulisi käyttää omaa, sisäistä tunnistamista. Näiden vaiheiden jälkeen todentaminen suoritetaan jollakin todentamismekanismilla. Viestien vaihdon jälkeen pääsyä vaativalle asiakkaalle toimitetaan viesti joko onnistumisesta (Success) tai epäonnistumisesta (Failure). /1/

5.1.2 EAP-TLS – EAP-Transport Layer Security

EAP-TLS käyttää molemminpuolista todentamista, jossa todentamispalvelin todentaa asiakkaan ja asiakas todentamispalvelimen. Liikenne on myös salattua osapuolten välillä sekä avainten vaihto voidaan hoitaa dynaamisesti. EAP-TLS käyttää digitaalisia varmenteita, joten näiden ylläpitämiseen tarvitaan oma infrastruktuurinsa.

TLS – Transport Layer Security on lähes samanlainen edeltäjänsä SSL:n (Secure Sockets Layer) kanssa. TLS:n avulla voidaan kommunikoida verkon yli estäen samalla salakuuntelu, pakettien sormeilu sekä viestien väärentäminen. Asiakas aloittaa TLS-kättelyn pyytämällä palvelimelta suojattua yhteyttä.

Asiakas toimittaa ClientHello-viestissä korkeimman tukemansa TSL-versionumeron, satunnaisluvun, sekä tukemansa salausalgoritmit ja tiivistefunktiot. Asiakkaan toimittamasta listasta palvelin valitsee tehokkaimman salausmenetelmän ja tiivistefunktion, ja ilmoittaa ne asiakkaalle ServerHello-viestissä.
Palvelimen lähettämän ServerHello-viestin jälkeen palvelin toimittaa digitaalisen varmenteen sekä pyytää myös asiakasta lähettämään oman varmenteensa. Palvelimen päättäessä oman osuutensa kättelystä, se lähettää ServerHelloDone-viestin.
Asiakas luo satunnaisluvun ja salaa sen sovitulla salausalgoritmilla käyttäen palvelimen julkista avainta. Tämä voidaan purkaa vain palvelimen omalla yksityisellä avaimella. Tästä satunnaisluvusta palvelin ja asiakas luovat itselleen käytettävän MasterSecret-luvun, josta kaikki muut avaimet johdetaan.
Asiakas lähettää palvelimelle ChangeCipherSpec-viestin, joka kertoo, että tästä lähtien kaikki toimitetut viestit ovat salattuja. Lopuksi asiakas lähettää palvelimelle Finished-viestin, jossa on sisällä edellisistä viesteistä laskettu tiiviste sekä MAC (Message Authentication Code). Palvelin purkaa asiakkaan lähettämän Finished-viestin ja vertaa sitä laskemiinsa arvoihin, jos ne eivät täsmää, yhteys puretaan. Viimeisinä viesteinä palvelin lähettää myös ChangeCipherSpec-viestin sekä Finished-viestin, jotka asiakas varmistaa edellä mainituin keinoin. /20/

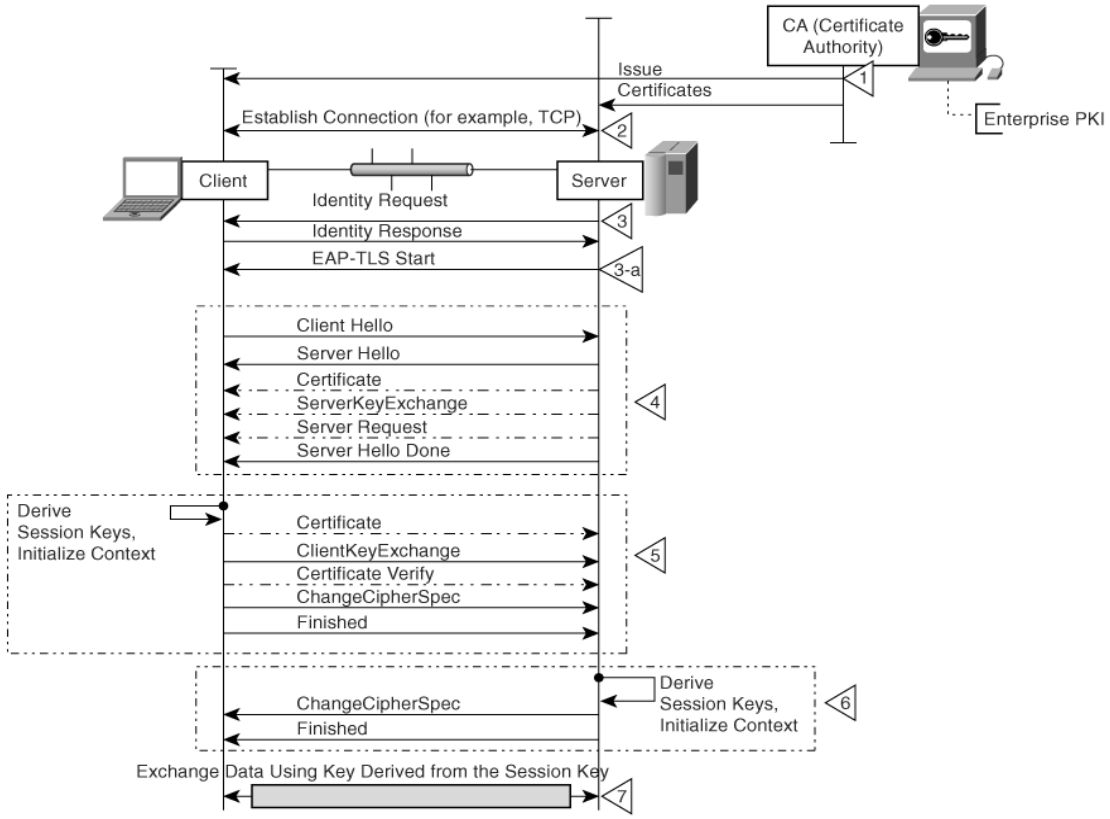
TLS määrittelee kaksi kerrosta käyttöön, ns. tietuekerros ja viestikerros. Tietuekerroksessa siirretään viestejä, jotka käsittelevät asioita kuten pirstoutuminen,

viestin todentaminen sekä salaus. Viestikerroksessa kuljetetaan neljää erityyppistä viestiä, ChangeCipherSpec, Alert, Handshake protokolla sekä sovellusten data.

Kuvassa (Kuva 5-1) on kuvattu EAP-TLS-viestien vaihto, joka on lähes samanlainen TLS:n viestejä vaihdettaessa.

EAP-TLS käyttää TLS:stä hyväkseen mm. molempien osapuolten todentamista, salaukseen käytettävän menetelmän neuvottelua sekä istunnon avainten johtamista. Identiteetin vaihdon jälkeen TLS-Start lähetetään palvelimelta todennettavalle asiakkaalle, jolla ilmoitetaan, että asiakkaan tulisi aloittaa viestien vaihto ClientHello-viestillä. EAP-TLS ei kuitenkaan käytä TLS:n tietueprotokollia. /1/

EAP-TLS on turvallinen ratkaisu, koska myös todennettavalla asiakkaalla on oma digitaalinen varmenne käytössä. Tätä tietoturvaa voidaan kohentaa käyttämällä digitaalisia varmenteita sirukortilta, jolloin hyökkääjän pitäisi saada fyysisesti kortti haltuunsa. Kortin kadotessa varmenne voidaan mitätöidä hyvinkin nopeasti. Salasanan leviäminen ulkopuolisten tietoon ei välttämättä käy ilmi heti.



Kuva 5-1. EAP-TLS viestien vaihto */1/*

5.1.3 PEAP – Protected EAP

PEAP on edelleen kehitetty EAP-TLS:stä langattomien verkkojen käyttöä ajatellen. PEAPista puhuttaessa viitataan usein PEAPv0/EAP-MSCHAPv2-toteutukseen, joka on toiseksi suosituin EAP-toteutus tällä hetkellä käytössä olevista menetelmistä. Cisco on kehittänyt myös PEAPv1/EAP-GTC-toteutuksen, mutta se ei ole läheskään niin laajalti käytössä, kuin PEAPv0/EAP-MSCHAPv2. /19/

PEAP vaatii vain palvelimen puolelta digitaalista varmennetta, käyttää TLS:ää suojatun tunnelin luomiseen ja jatkaa vielä EAP-TLS:n jälkeen suorittaakseen asiakkaan todentamisen ja avaintenvaihdon. Tämä asiakkaan todentaminen voidaan suorittaa oikeastaan millä tahansa EAP-metodilla. PEAP vaatii palvelimille infrastruktuurin digitaalisten varmenteiden käyttöä varten. /1/

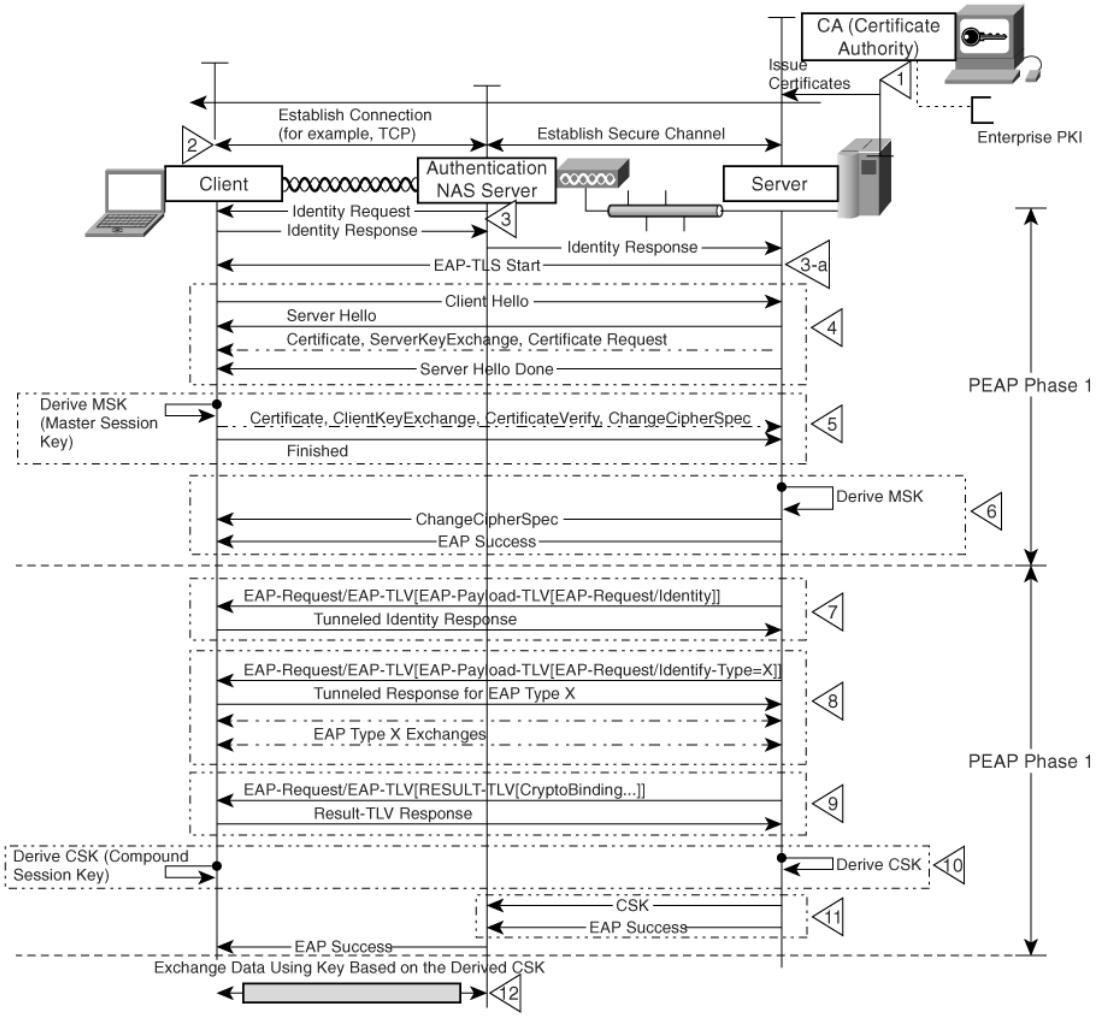
PEAP:lla on kaksi vaihetta käytössä. Ensimmäinen vaihe on suojatun tunnelin muodostaminen käyttäen EAP-TLS:ää. Toisena vaiheena on asiakkaan todentaminen valitulla EAP-metodilla käyttäen ensimmäisessä vaiheessa luotua tunnelia. Kuvassa (Kuva 5-2) on PEAP-keskustelu, joka käydään EAP-palvelimen ja EAP-asiakkaan välillä, todentajana oleva tukiasema toimii suurelta osin vain viestien välittäjän asemassa. Uudempien EAP-ratkaisujen käyttöönotto helpottuu, koska koko infrastruktuuria ei tarvitse uusia, pelkkä asiakkaan ja todentamispalvelimen päivittäminen riittää. /1/

PEAP TLV-mekanismia käytetään vapaasti määritettävissä olevien tietojen vaihtoon. Tämä mekanismi on käytössä PEAP vaiheessa 2, jossa voidaan siirtää EAP Payload TLV:ssä EAP-metodeita suojatun tunnelin sisällä. /1/

Kuvassa (Kuva 5-2) näkyvässä keskustelussa kohdassa 3 tapahtuvaa identiteetin vaihtoa käytetään yleensä palvelimen valintaan. Se lähetetään selväkielisenä, joten sitä ei tulisi käyttää mihinkään tietoturvan kannalta ratkaisevaan operaatioon. PEAP-

vaiheessa 2 vaihdetaan identiteetit, jonka avulla asiakas tunnistetaan. Kohdissa 4, 5 ja 6 on normaali EAP-TLS operaatio, jolla suojattu tunneli muodostetaan. /1/

Kohdasta 7 alkaa vaihe 2. EAP-TLV-mekanismin sisällä tapahtuu normaali EAP identiteetin vaihto. Kohdassa 8 asiakas todennetaan käyttämällä saatavilla olevaa EAP-mekanismia. Kohdassa 10 luodaan käytettävät avaimet. Kohdassa 11 käytettävä avain toimitetaan todentamispalvelimelta tukiasemalta, jonka jälkeen kohdassa 12 aloitetaan tietojen vaihto tukiaseman ja asiakkaan välillä edellisessä kohdassa luotuja avaimia käyttäen. /1/



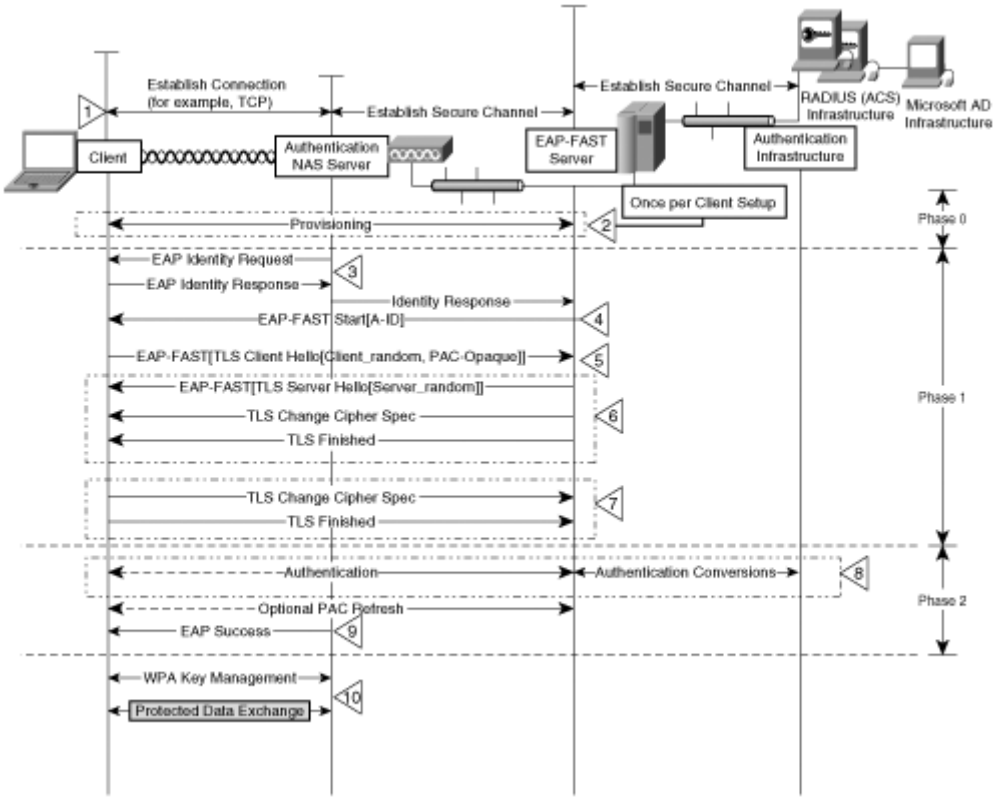
Kuva 5-2. PEAP viestien vaihto */1/*

5.1.4 EAP-FAST – EAP-Flexible Authentication via Secure Tunneling

Esillä olleisiin metodeihin verrattuna EAP-FAST on toistaiseksi kaikista kattavin ja turvallisin langattomien verkkojen käyttöä ajatellen. EAP-FAST on määritelty RFC 4851:ssä /25/. EAP-FAST pienentää passiivisten sanakirjahyökkäysten riskiä, kuten myös MitM-hyökkäysten riskiä samalla luoden mahdollisuuden turvalliseen todentamiseen jo käytössä olevien todentamismenetelmien avulla. EAP-FAST on kolmivaiheinen protokolla, jonka aikana muodostetaan PAC-avain (Protected Access Credential) suojatun tunnelin luomista varten, käyttäjän todentaminen tapahtuu vasta suojatun tunnelin sisällä. /1/

EAP-FAST pitää sisällään neljä toiminnallista yksilöä. Pääsyä pyytävä asiakas, todentajana oleva tukiasema, EAP-FAST palvelin sekä sisäisen todentamismenetelmän käyttämä palvelin. Näistä toiminnallisuuksista useampi voi sijaita fyysisesti yhdessä laitteessa.

Kuvassa (Kuva 5-3) nähdään EAP-FAST-protokollan käyttämä viestien vaihto ja käytössä olevat 3 vaihetta (Phase 0, 1 & 2).
Vaiheessa 0 tapahtuu avaintenvaihto käyttäen ADHP (Authenticated Diffie-Hellman Protocol)-protokollaa. Vaihe 0 on itse asiassa EAP-TLS vaihto.
Vaihe 1 käsittää suojatun tunnelin luomisen.
Vaiheessa 2 tapahtuu varsinainen käyttäjän todentaminen. Vaiheessa 2 todentamiseen käytettävä EAP siirretään EAP-TLV:n sisällä. Sisäinen metodi voi olla EAP-SIM, EAP-OTP, EAP-GTC tai MSCHAPv2. Tapahtuma loppuu EAP-Success-viestiin, jonka jälkeen WPA:ssa voidaan käyttää aikaisempien kolmeen vaiheen aikana luotuja avaimia. /1/



Kuva 5-3. EAP-FAST viestien vaihto */1/*

5.1.5 802.1x/EAPOL – EAP Over LAN

EAP on pääasiassa kehitetty soittosarjayhteyksien käyttöä varten, joten niitä varten ei ole siirtoyhteyskerroksen protokollia 802-verkoissa. Kuten aikaisemmista kuvista on nähty, EAP tarvitsee esim. TCP-yhteyden toimimaan ensimmäiseksi. Tätä tarkoitusta varten 802.1x tarjoaa yhteydet, tilakoneet ja EAP:n LAN:n yli (EAPOL). 802.1x on laajalti käytössä langallisissa verkoissa. 802.1x lähtee konseptista, jossa yhdelle asiakkaalle on yksi paikka liittyä verkkoon. Tämä toimii myös 802.11-verkoissa, jossa asiakas voi olla assosioituneena vain yhteen tukiasemaan kerrallaan, joka on siis asiakkaalle yhdellä kertaa yksi ainoa kohta verkkoon liittymiseksi. EAPOL siirtää EAP paketit asiakkaan ja todentamista hoitavan tukiaseman välillä MAC-palveluiden avulla. Ennen todentamista, asiakas ei pääse liikennöimään tukiaseman kautta mitään muita paketteja, kuin todentamista varten tarkoitettuja paketteja. /1/

5.1.6 RADIUS

RADIUS (Remote Address Dial-In User Service) (RFC 2865) on asiakas-palvelin asetelmalla toimiva protokolla, jossa asiakkaana toimii esim. tukiasema tai langattoman verkon tukiasemia hallitseva ohjain. Palvelin on usein UNIX tai NT koneessa prosessina pyörivä palvelu. RADIUS on yhteydetön palvelu, joka käyttää UDP:tä siirtoprotokollana, jolloin uudelleenlähetykset ja aikakatkaisut hoitavat RADIUS-palvelua pyörittävät laitteet siirtoprotokollan sijasta. /21/

RADIUS on AAA-protokolla (Authentication, Authorization, Accounting). Authentication puoli hoitaa käyttäjän todentamisen, Authorization antaa luvan käyttää tiettyjä palveluita tai määrää käyttäjälle Access-Accept-viestin parametreina käytettävät osoitteet. Accounting-ominaisuudella voidaan pitää kirjaa käyttäjän toimista muodostetun session aikana esim. laskutustietojen muodostamiseksi.

RADIUS-asiakas sekä RADIUS-palvelin käyttävät jaettua salasanaa tunnistukseen, tätä salasanaa ei siirretä koskaan siirtotien yli. Käyttäjien salasanat toimitetaan salattuina. Huomionarvoinen asia on se, että osa liikenteestä salataan ja sekin vain RADIUS-osapuolten välillä, eli esim. tukiaseman tai RADIUS-palvelimen välillä. Pääsyä vaativan asiakkaan yhdistäessä verkkoon, NAS (Network Access Server) kysyy asiakkaalta tunnistetietoja, ja lähettää ne RADIUS-palvelimelle salattuna. RADIUS-palvelin vastaa NAS:lle viestillä Accept, Reject tai Challenge. /1/

5.1.7 TACACS+

TACACS+ on edelleen kehitetty alkuperäisestä TACACS-protokollasta. TACACS+ käyttää TCP:tä siirtoprotokollana ja kuuntelee portissa 49. Kuten RADIUS, TACACS+ on asiakas-palvelin protokolla, joka käyttää samoja verkon elementtejä, kuin RADIUS.

TACACS+ on AAA-protokolla, mutta käyttäjän todentamista varten suunnattu Authentication on tässä tarkastelun kohteena. TACACS+ sallii minkä tahansa todentamismekanismin käyttämisen (PAP, CHAP, EAP, jne). TACACS+ käyttää kolmea erityyppistä pakettia, joista asiakkaan lähettämiä ovat START ja

CONTINUE, palvelin lähettää vain REPLY-paketteja. Todentamisprosessi alkaa START-viestillä, jossa ilmoitetaan käytettävä todennusmetodi ja voi sisältää myös todentamiseen käytettäviä tietoja. START-paketti lähetetään vain ensimmäisenä viestinä TACACS+ session yhteydessä ja sillä on järjestysnumero aina 1. Palvelin vastaa aina REPLY-paketeilla, jossa se ilmoittaa, että päättyykö todentamisprosessi vai pitäisikö sitä vielä jatkaa. Jos todentamista jatketaan, samassa REPLY-paketissa toimitetaan myös vaatimukset todentamisen jatkamista varten tarvittavista tiedoista. Asiakas palauttaa uudet tiedot palvelimelle CONTINUE-viestillä, ja tätä prosessia jatketaan niin kauan, kunnes kaikki tiedot todentamista varten on kerätty. /1/

TACACS+ käyttää myös asiakkaan ja palvelimen päässä jaettua salaista avainta, jota ei siirretä koskaan verkon yli. TACACS+ salaa kaiken liikenteen asiakkaan ja palvelimen välillä. /1/

5.2 Käytössä olevat salausmenetelmät

WEP käydään yksityiskohtaisemmin läpi seuraavassa kappaleessa. WPA on Wi-Fi Alliancen luokitus langattomien verkkojen suojaamiseksi. WPA oli väliaikainen, nopea ratkaisu WEP:n korvaamiseksi ennen IEEE 802.11i-standardin julkaisemista. WPA käyttää hyväkseen IEEE 802.11i-työryhmän kehittämää TKIP-suojausta, jossa on 128 bittiä pitkä avain ja 48 bittiä pitkä alustusvektori. WPA2 on toinen Wi-Fi Alliancen myöntämä luokitus. WPA2 käyttää samoja tekniikoita, kuin IEEE 802.11i-standardi, eli CCMP-protokollaa, joka käyttää salaukseen AES-algoritmia. WPA2 vaatii rautatasolta tukea AES-algoritmille, joten vanhemmilla laitteilla ei välttämättä ole mahdollista saada WPA2:sta käyttöön.

5.2.1 WEP - Wired Equivalent Privacy

IEEE 802.11-standardissa määritellyn salausmenetelmän tarkoituksena oli saavuttaa kolme tavoitetta. WEP:n oli tarkoitus estää siirrettävien pakettien paljastuminen ja muuttaminen sekä tarjota pääsyn hallintaa verkon käyttöön. WEP:n nimessä jo ilmenee sen tarkoitus, joka oli siis tarjota langattomaan verkkoon samantasoinen tietoturva, kuin langallisessa verkossa on käytössä. Suunniteltaessa tiedettiin jo

mahdollisista epäkohdista ja ne hyväksyttiin olettaen, että verkkoon pääsy olisi tehty yhtä vaikeaksi, kuin fyysisesti lankaverkkoon kiinni pääseminen. /1/

WEP salaa siirrettävän tiedon RC4-algoritmia käyttävällä jonosalaimella, jota ei ole tarkoitettu käytettäväksi uudestaan samalla avaimella. Jokaista pakettia varten muutetaan käytettyä salausavaitan lisäämällä WEP-avaimen alkuun 24 bittiä pitkä alustusvektori IV (Initialization Vector). WEP-avain on joko 40 tai 104 bittiä pitkä ja siihen lisätään 24 bittiä pitkä alustusvektori, jolla koko WEP-siemenen pituudeksi saadaan 64 tai 128 bittiä. Salausavaimen uusiutumista ei estetä mitenkään, joten alustusvektorien tahattomat uusiutumiset ja siten RC4:ää vastaan tehtävät hyökkäykset ovat mahdollisia. Paketin vastaanottajalla on WEP-avain tiedossaan, joten tämän lisäksi tarvitaan alustusvektori, joka sen takia toimitetaan selväkielisenä jokaisessa WEP-salatussa paketissa. Alustusvektori muodostaminen tapahtuu siten, että otetaan joku satunnainen luku tai 0 ja lisätään tämän arvoon yksi arvo lisää jokaisella kerralla, kun IV muodostetaan. 24 bittiä pitkän IV:n arvoalue on rajattu, joten väistämättä joskus laskuri palaa takaisin lähtöarvoonsa ja salausavaimeksi muodostuu jo aikaisemmin käytetty arvo. /1/

Eheyden tarkistamiseen WEP käyttää eheyden tarkistusvektoria ICV (Integrity Check Vector). ICV on 4 tavua pitkä tarkistussumma, joka lasketaan paketin selväkielisestä hyötykuormasta ja sisällytetään salattuun hyötykuormaan. ICV käyttää CRC-32-algoritmia tarkistussumman laskemiseen. Tarkistussumman tarkoituksena on paljastaa paketin muokkaaminen. Mikäli vastaanotetun paketin tarkistussumma ei täsmää ennen lähetystä laskettua summaa, on pakettia muutettu.

CRC-32:n käyttäminen lineaarisen tarkistussumman laskemiseen jonosalaimen yhteydessä oli huono valinta, koska jonosalaimet sallivat joidenkin bittien muuttamisen ilman vaikutusta muuhun viestiin. Lineaarisen tarkistussumman muuttuminen voidaan ennustaa, jos jotakin tiettyä osaa viestistä muutetaan. Hyökkääjä voi täten laskea, mitä bittiä voi muuttaa tarkistussumman tästä muuttumatta. Hyökkääjän ei edes tarvitse tietää ICV:tä, vaan pelkästään sen, mitä bittiä pitää muuttaa salatusta ICV:stä. /1/

RC4 on symmetrinen jonosalain, joka tuottaa selkotekstin kanssa samanmittaisen salatekstin. Jonosalaimissa ei ole tarkoitus käyttää samaa salausavainta uudelleen, ja tätä ohjesääntöä noudattamalla voidaan RC4 luokitella turvalliseksi salausalgoritmiksi. Symmetrinen salaus viittaa siihen, että salaus ja salauksen purkaminen hoidetaan samaa avainta käyttäen. RC4-salauksessa on kaksi vaihetta, tietovirran muodostaminen ja salaus. Tietovirran luonnissa käytetään erilaisia operaatioita, joilla saadaan järjesteltyä bitit näennäisesti satunnaiseen järjestykseen. Salaus itsessään on oikeastaan XOR-operaatio satunnaiseksi muokatun bittivirran ja salausavaimen välillä. RC4 käyttää S-laatikoita bittien uudelleen järjestämiseen. S-laatikot sisältävät valikoiman arvoja, joita käytetään korvaamaan tietovirran bitit. S-laatikossa on 256 arvoa. /1/

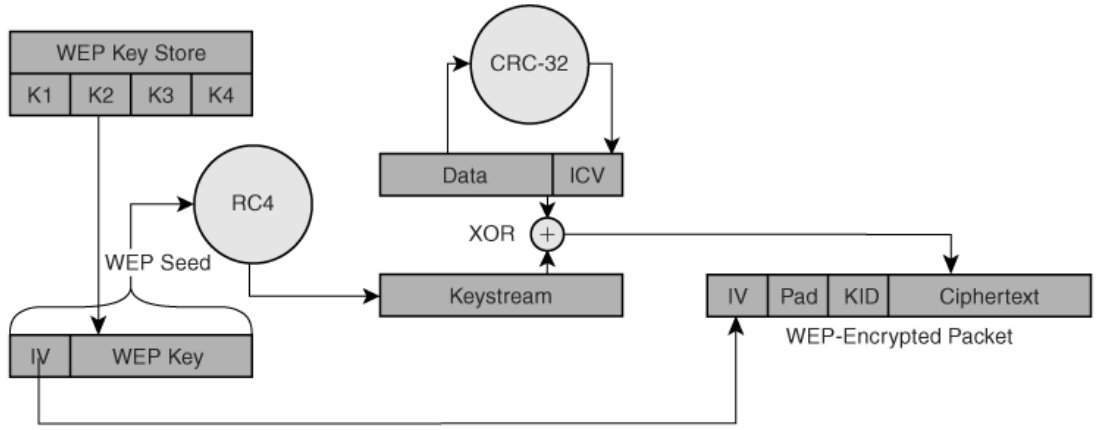
Kapselointi on operaatio, jolla data kääritään alemman verkkokerroksen käyttöön sopivaksi. Prosessiin kuuluu aiemmin mainittu salaus, tarkistussumman laskeminen sekä otsikkotietojen lisääminen. Kuvassa (Kuva 5-4) on esitettynä WEP-paketin muoto.

Kuva 5-4. WEP-paketti */1/*

Paketissa on alussa MAC-kerroksen otsikkotiedot, jonka kentät on käyty tarkemmin läpi kappaleessa 3.1.5. MAC otsikon jälkeen löytyy 3 tavua pitkä alustusvektori IV selvätekstisenä. Key ID-kenttä ilmoittaa, mitä neljästä mahdollisesta avainindeksistä käytetään WEP-avaimena. Paketissa kokonaan salattua osuutta on vain hyötykuorma sekä selkokielisen hyötykuorman tarkistussumma.

Kapseloinnin ensimmäisenä vaiheena valitaan alustusvektori IV, jonka alkaminen aloitetaan yleisimmin nollasta aina sen jälkeen, kun kortista katkaistaan virta. Toinen vaihtoehto voisi olla satunnaisesti valittujen alustusvektorien käyttäminen, mutta tämä vaatisi paljon muistia käytettyjen alustusvektoreiden tallentamiseen. Valittu IV

lisätään WEP-avaimeen ja näistä kahdesta saadaan muodostettua salausavaimena käytetty WEP-siemen. WEP-siemen syötetään RC4 algoritmiin ja sotketaan sekaisin S-laatikossa. Samalla, kun tietovirtaa muodostetaan, hyötykuormasta lasketaan 4 tavua pitkä ICV. Selkokielisen datan perään lisätään laskettu tarkistussumma. Datan ja tarkistussumman muodostama bittijono ajetaan XOR-operaation läpi tietovirran kanssa ja tästä operaatiosta saadaan tulokseksi salateksti. Koko operaatio on nähtävissä alla olevassa kuvassa (Kuva 5-5).



Kuva 5-5. WEP kapselointi */1/*

XOR on looginen bittioperaattori, jonka totuustaulu on näkyvissä taulukossa (Taulukko 5-1). Totuustaulusta voidaan nähdä, että XOR operaatio suoritettuna samoilla arvoilla johtaa nollaan, eli tuloksen bitit ovat nollia. Salauksen purkamisen yhteydessä tätä voidaan käyttää siten, että XOR operaatiolla saatu salateksti ajetaan uudestaan XOR operaation läpi avaimen kanssa, jolloin saadaan alkuperäinen selväteksti XOR-operaation tuloksena. /1/

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

Taulukko 5-1. XOR totuustaulu

Kapseloinnin purkaminen on päinvastainen operaatio kapselointiin nähden. Operaatiossa poistetaan ensin MAC otsikko, erotellaan IV ja käytettävän avainindeksin identifioiva arvo. Avainindeksin arvolla osoitetaan purkamiseen

käytettävän avaimen sijainti ja avainindeksin osoittamasta paikasta löytyvä WEP-avain ynnätään yhteen paketista irrotetun alustusvektorin kanssa. Tälle WEP siemenelle suoritetaan sama RC4 operaatio, kuin salauksen yhteydessä. Tämä tietovirta ajetaan XOR-operaation läpi salatekstin kanssa, josta tulokseksi saadaan selväteksti ja ICV. ICV lasketaan selvätekstistä ja verrataan paketista purettuun ICV:hen, jos ne täsmäävät, data siirretään ylemmän kerroksen käsiteltäväksi.

5.2.2 TKIP – Temporal Key Integrity Protocol

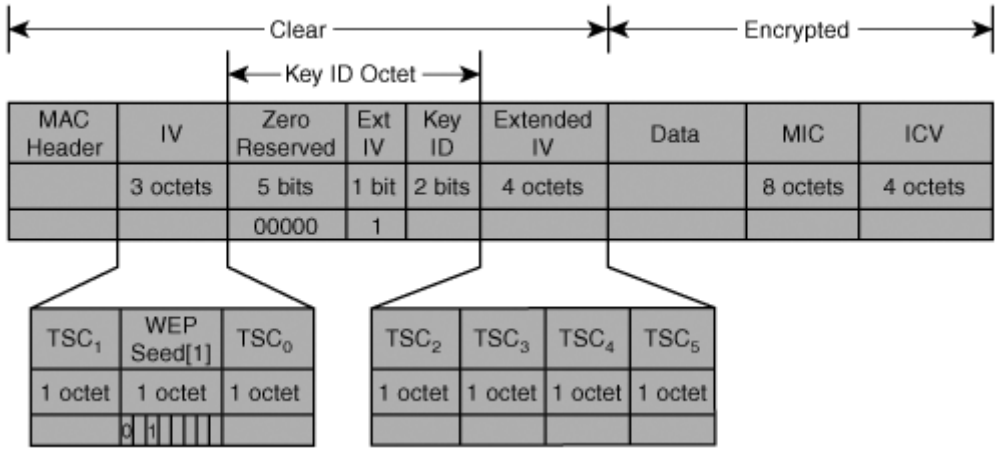
WEP:n haavoittuvuuden löydyttyä piti kehittää uusi menetelmä tiedon suojaamiseksi ilman, että miljoonista jo myydyistä laitteista tulisi jätettä. 802.11i-työryhmä kehitti TKIP:n ja CCMP:n korjaamaan puutteet WEP-protokollassa sillä välin, kun 802.11i-standardia kehitettiin. Koska suurimmat ongelmat johtuivat RC4-avaimista, oli parasta vaihtaa pohjalla olevaa WEP-avainta jokaista pakettia varten. TKIP sisältää kolme protokollaa, MIC:n (Message Integrity Check), avainten sekoitukseen käytettävän algoritmin sekä laajennetun alustusvektorin.

WEP:n käyttämä ICV on lineaarinen ja luottaa laskennassa vain paketissa olevaan sisältöön. TKIP käyttää tiivistefunktiota, johon on laskettu mukaan myös molempien osapuolten tietämä avain. Tiivistefunktiota käytettäessä seuraavien bittien arvoja ei voida päätellä, ja viestissä yhden bitin muuttamisen pitäisi aiheuttaa tiivisteessä suuren muutoksen. SHA1 on tehokas tiivistealgoritmi, joka on nykyisellään käytössä useassa salausalgoritmissa, mutta vanhojen laitteistojen laskentatehon puutteen takia päädyttiin yksinkertaisempaan algoritmiin, Michaeliin. Michael laskee tiivisteen ns. pehmustetusta MSDU:sta (MAC Service Data Unit), joka sisältää normaalin MSDU:n sekä lisäosan, jossa on lähettäjän ja vastaanottajan MAC-osoitteet, erilaisia varattuja oktetteja sekä prioriteetti-kenttä. Michaelista saadaan ulos kaksi 32-bittiä pitkää avainta, jotka yhdistetään 64-bittiseksi tiivisteeksi. /1/

Tiivistefunktion tavoitteena on luoda tiiviste, jollaista samanlaista ei ole olemassa erilaisesta datasta laskettuna. Ilman avainta hyökkääjä joutuu arvailemaan MIC:n oikeita bittejä. Arvailemisen kautta löydetty tulos ei ole mahdoton, mutta erittäin epätodennäköinen. IEEE 802.11i-suositus kertoo, että Michael ei tarjoa vahvaa

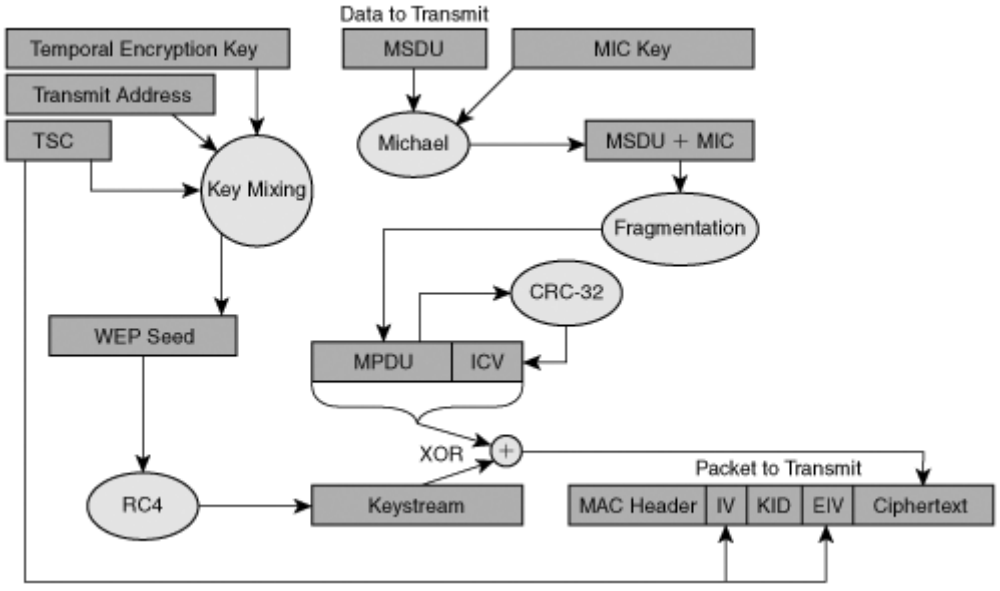
suojautumista aktiivisia hyökkäyksiä vastaan. Nämä heikkoudet johtuvat aiemmin kerrotusta syystä, jossa valittiin Michael suorittamaan tiivistefunktion virkaa SHA1:n tilalle. Ennen Michael-arvon tarkastamista tarkastetaan ICV:n arvo. ICV:n tarkastuksella pyritään vähentämään tarkoituksenmukaisia Michael-algoritmin tarkistuksen epäonnistumisia. Suojamekanismina toimii menetelmä, jossa minuutin sisällä kahden Michael-tarkistuksen epäonnistuminen lopettaa kaikkien pakettien vastaanottamisen ja lähettämisen. Samassa yhteydessä tukiaseman pitäisi purkaa kaikkien asiakkaiden yhteydet ja neuvotellut turvallisuusassosioinnit. Tämä vaihe kestää 60 sekunnin ajan, jonka jälkeen voidaan aloittaa uusien avainten neuvottelu. /1/

Avainten uusiutumista vastaan TKIP käyttää TSC:tä (TKIP Sequence Counter). WEP ei tarkista missään vaiheessa sitä, onko jollakin alustusvektorilla muodostettu avain käytetty vai ei, joten salausavainten uusiutumisia tulee esiintymään. Avaintenhallintaa WEP:ssä ei ollut, joten vaikka alustusvektoreiden uusiutuminen olisi estetty, vapaana olevien alustusvektoreiden määrä olisi loppunut. TSC on 48-bittinen laskuri, joka aloittaa nollasta ja kasvaa yhdellä jokaista pakettia kohden. Jokainen paketin vastaanottaja pitää kirjaa korkeimmasta TSC:n arvosta ja paketin lähettäjän MAC-osoitteesta. Mikäli TSC:n arvo on pienempi, kuin laskurista löytyvä arvo, paketti hylätään. ICV ja MIC estävät hyökkääjää muuttamasta TSC:n arvoa ja lähettämästä pakettia uudestaan. Kapseloinnin yhteydessä tapahtuva ICV:n tarkistus paljastaa muuttuneen avaimen ja hylkää paketin ennen sen pääsemistä edes MIC tarkistukseen asti. TSC on yhtenä arvona salauksen purkamisessa, joten vaikka TSC:n arvoa muutettaisiin ja paketti pääsisi ohittamaan eheyden tarkastukset, salauksen purkaminen epäonnistuisi. TSC toimitetaan paketissa selväkielisenä. Toisena mahdollisena skenaariona hyökkääjä voisi lähettää paketteja kasvattaen TSC arvoa viimeisestä tunnetusta arvosta ylöspäin. Vastaanottaja näkisi alkuperäisen lähettäjän paketit uudelleenlähetyksinä ja hylkäisi ne. Spesifikaatio tekee kuitenkin myös tämän mahdottomaksi, koska TSC-laskuria ei päivitetä ennen, kuin MIC-tarkistus on onnistuneesti mennyt läpi. Kuvassa (Kuva 5-6) näkyy TKIP-paketin muoto. /1/



Kuva 5-6. TKIP paketti */1/*

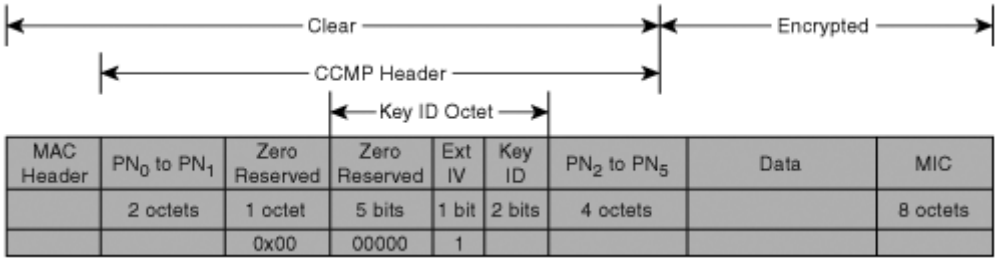
Avainten luontiin TKIP käyttää algoritmia, jolla on tarkoitus suojata TEK (Temporal Encryption Key). TEK on väliaikainen avain, joka voidaan vaihtaa avainten vaihtoon tarkoitetulla algoritmilla. TEK:n päälle rakennetaan jokaista pakettia varten vaihtuva salausavain. Lähtötilanteessa molemmilla osapuolilla on tiedossaan sama TEK, johon yhdistetään TSC ja lähettäjän MAC-osoite. Näistä kolmesta muodostuu jokaista pakettia varten uniikki 128 bittiä pitkä WEP siemen, jota WEP algoritmi käyttää salausavaimena. Kuvassa (Kuva 5-7) näkyy TKIP kapselointiprosessi.



Kuva 5-7. TKIP kapselointi */1/*

5.2.3 CCMP – Counter Mode/CBC-MAC Protocol

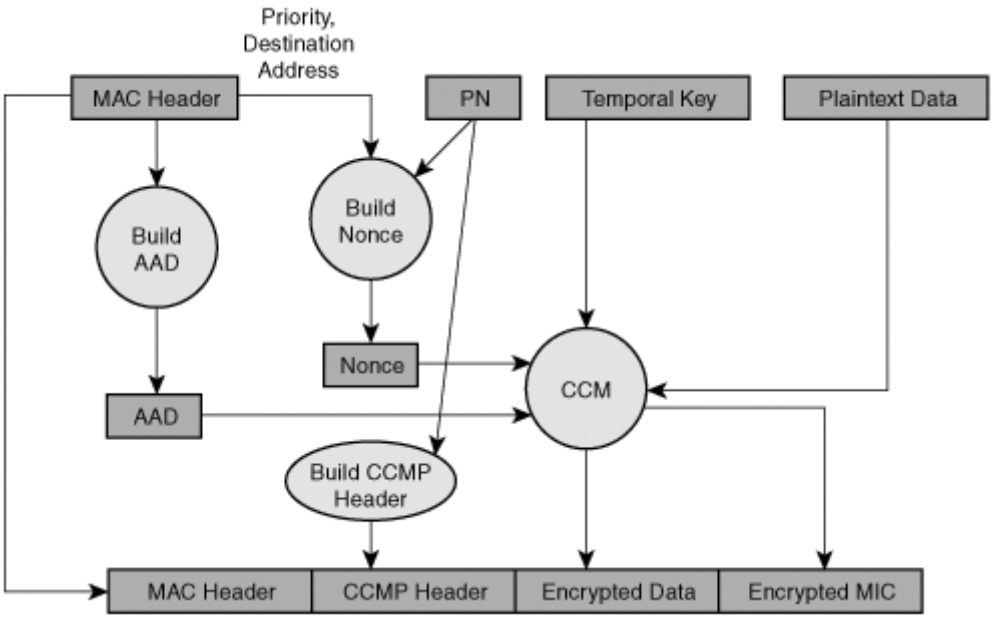
IEEE 802.11i toi mukanaan CCMP (Counter Mode/CBC-MAC Protocol) salausmenetelmän. CCMP on vahvempi salausmenetelmä, kuin TKIP. CCMP käyttää AES-algoritmia salauksen toteuttamiseen. AES on lopputulos kansainvälisestä kilpailusta, jossa etsittiin uutta, vahvaa salausalgoritmia. AES käyttää Counter mode-tilaa luottamuksellisuuden toteuttamiseen ja CBC-MAC-tilaa eheyden luomiseksi. Kuvassa (Kuva 5-8) on esillä CCMP paketin muoto. CCMP otsikko on 8 oktettia pitkä. Otsikossa on myös näkyvillä 48 bittiä pitkä PN-kenttä (Packet Number), joka on samankaltainen TKIP:ssä käytetyn TSC:n kanssa.



Kuva 5-8. CCMP paketti */1/*

CCMP:n kapselointiprosessissa data salataan sekä siihen liitetään siirtoa varten tarvittavat otsikkotiedot. CCM salaus varmistaa tiedon luottamuksellisuuden ja lohkosalain estää viestin lukemisen ilman oikeaa avainta. Eheyden tarkastuksen hoitaa MIC, joka lasketaan koko hyötydatasta sekä osasta MAC otsikkotietoja. Vaikka näitä tietoja ei salata siirron yhteydessä, näistä laskettu MIC estää kuitenkin tietojen muuttamisen. Kuvassa (Kuva 5-9.) on näkyvissä kapselointiprosessi. CCM algoritmi käyttää salaukseen AAD (Additional Authentication Data) tietueita, selväkielistä hyötydataa, tilapäisesti rakennettua pakettikohtaista tunnistetta sekä varsinaista avainta. CCM algoritmista saadaan ulos hyötykuorma sekä eheyden tarkastamiseen käytetty MIC, molemmat salattuna. Näihin lisätään CCMP otsikkotiedot ja normaali MAC-otsikko. Paketin purkaminen sujuu päinvastaisessa järjestyksessä, kuin kapselointi. Paketista erotetaan PN, josta tarkastetaan, että se on kasvanut yhdellä eikä kyseessä ole paketin uudelleenlähetys. MAC-otsikosta ja paketin numerosta lasketaan pakettikohtainen tunniste ja pelkästä MAC-otsikosta rakennetaan AAD. Salaukseen käytetty Temporal Key on vastaanottajan tiedossa. Edellä mainitut tiedot sekä salattu hyötykuorma ja MIC ajetaan CCM-algoritmin

läpi, josta saadaan ulos selväkielinen data ja MIC. Jos paketissa ollut MIC vastaa puretusta paketista laskettua MIC:tä, voidaan olla varmoja, että paketin otsikkotietoja ei ole muutettu ja paketti on saapunut perille muuttumattomana. /1/



Kuva 5-9. CCMP kapselointi /1/

AES salausalgoritmin toiminta on varsin monimutkainen, tarkempi kuvaus toiminnasta on luettavissa Wikipediasta /22/. AES on lohkosalain, joka käyttää 128 bittiä pitkiä selväkielisiä lohkoja, ja muuttaa ne 128 bittiä pitkäksi lohkoksi salattua dataa silloin, kun käytössä on 128 bittiä pitkä salausavain. CCM käyttää AES:n kahta toimintamuotoa, Counter toimintamuotoa (CTR) salaukseen sekä Cipher Block Chaining (CBC-MAC) toimintamuotoa MIC:n luomiseen. Counter toiminto paloittelee viestin 128 bittisiksi lohkoiksi. 128 bittiä pitkä laskuri antaa ulos ensimmäisen arvon, joka ajetaan AES-algoritmin läpi ja sen jälkeen salattu laskurin arvo ajetaan XOR-operaation läpi, jossa se sekoitetaan 128 bittiä pitkään viestilohkoon. Lopuksi viestilohkot yhdistetään yhtenäiseksi bittijonoksi, joka lopulta toimii salattuna viestinä. Tätä operaatiota jatketaan niin kauan, kunnes koko viesti on saatu salattua. /1/

Salauksen purkaminen on samanlainen prosessi. Tämä oli yksi avaintekijä AES:n yleistymiselle. AES:ää käyttöönotettaessa ei tarvitse asentaa muuta, kuin pelkkä

salain, ei purkutoimintoa. Salauksen purkaminen on prosessi, jossa käytettyjä laskureita salataan ja niille suoritetaan XOR-operaatio.

CBC toimintamuoto laskee selväkielisestä viestistä MIC:n. Selväkielinen viesti jaetaan 128 bittisiin lohkoihin, jotka ajetaan AES-algoritmin läpi. Salatulle viestilohkolle ja selväkieliselle viestilohkolle suoritetaan XOR-operaatio ja operaation tulos ajetaan AES-algoritmin läpi. Prosessi jatkuu niin pitkään, kuin viestiä on jäljellä. Prosessin aikana menetetään tietoa, mutta sillä ei ole merkitystä. Tarkoituksena on luoda uniikki tiiviste viestistä, joko voidaan luoda uudestaan vastaanottopäässä ja varmistaa, että viestiä ei ole muokattu.

5.3 Hyökkäyksiä verkkoja vastaan

Langattomien verkkojen luonteesta johtuen verkkoon pääsyä tai verkon näkemistä ei pystytä rajoittamaan alueellisesti tietyn tilan sisäpuolelle. Langalliseen verkkoon pääsyn estämiseksi voidaan estää fyysisesti pääsy verkon liityntäpisteisiin. Tukiasemien peittoaluetta pienentämällä voidaan rajata kantamaa pienemmäksi, mutta tämäkään ei poista mahdollisuutta ulkopuolisen käyttäjän liittymisestä verkkoon. Verkossa kulkevaa liikennettä voidaan myös kuunnella passiivisesti ilman verkkoon liittymistä.

Verkkoa vastaan tehtävät hyökkäykset voidaan yleensä lukea kahteen pääryhmään, passiivisiin ja aktiivisiin hyökkäyksiin. Näiden hyökkäysten tavoitteena on murtaa yksi tai useampi tietoturvan peruselementeistä, eli joko luottamuksellisuus, eheys tai saatavuus. /8/

Passiivisissa hyökkäyksissä voidaan joko salakuunnella verkossa liikkuvaa liikennettä viestien sisällön selville saamiseksi tai analysoida liikennettä saadakseen tietoonsa elintärkeitä tietoja verkon toiminnasta.

Aktiivisissa hyökkäyksissä hyökkääjä muokkaa verkossa liikkuvaa liikennettä. Aktiivisia hyökkäyksiä on neljää eri tyyppiä, joita voidaan yhdistellä keskenään. Tekeytymällä sallituksi käyttäjäksi hyökkääjä saa käyttöönsä palveluita ja oikeuksia, joita vain sallituilla käyttäjillä on. Toisena tapana hyökkääjä voi salakuunnella

verkossa liikkuvaa liikennettä ja vastata näihin viesteihin tekeytymällä lailliseksi käyttäjäksi. Hyökkääjä voi myös vastaanottaa paketteja, muokata tai järjestellä uudelleen niitä sekä lähettää eteenpäin muokkaamansa paketit. Palvelunestohyökkäyksillä pyritään lamauttamaan koko verkon toiminta niin, etteivät sallitut käyttäjät pääse käyttämään verkkoa hyväkseen. /8/

5.3.1 War Driving

War Driving on langattomien verkkojen tarkoituksenmukaista etsintää joko avoimien, vapaan pääsyn mahdollistavien verkkojen saalistuksessa tai kohdeverkon etsintää, kun tarkoituksena on murtautua sisälle verkkoon. Langattomien verkkojen etsintään on olemassa useita ohjelmia erilaisilla ominaisuuksilla.

Nykyisin suosituimmissa käyttöjärjestelmissä tulee esiasennettuna langattomien verkkojen etsintään tarkoitettu ohjelma, jolla voi lukea tukiaseman lähettämiä beacon-paketteja, joissa kerrotaan tarvittavia tietoja verkkoon yhdistämiseksi. Usein langattomia verkkoja saalistettaessa käytetään hyväksi ohjelmia, jotka kuuntelevat passiivisesti beacon-paketteja. Näissä ohjelmissa on usein myös mahdollista merkitä löytyneen verkon sijainti käyttäen hyväksi GPS-laitteita. Esimerkki tällaisesta ohjelmasta on Kismet /12/. Toisenlaisia ohjelmia ovat ohjelmat, jotka lähettävät aktiivisesti probe-viestejä, joihin tukiasemat vastaavat. Netstumbler /13/ on esimerkki tällaisesta ohjelmasta. /11/

Näitä keinoja vastaan ei verkkoa ylläpitävä taho voi puolustautua. SSID:n lähettämisen beacon-paketeissa voidaan kytkeä pois päältä, mutta hetken aikaa verkkoa kuunneltuaan hyökkääjä saa sen tietoonsa, kun joku sallittu käyttäjä assosoituu verkon kanssa. SSID lähetetään jokaisessa kehyksessä, kun asiakas pyytää assosiointia verkolta.

5.3.2 Luvaton päätelaite

Hyökkääjän löydettyä sopiva verkko, pitää verkkoon jotenkin päästä yhdistämään. Luvaton päätelaite on verkkoon yhteyden ottanut asiakas, jolla ei muuten ole lupaa

käyttää verkkoa hyväkseen. Verkkoon kiinnittymiseksi tarvitaan vain IEEE 802.11-standardia noudattava päätelaite, eli millä tahansa laitteella, jolla on mahdollisuus käyttää wlan-verkkoa, voidaan tämä toteuttaa.

Verkkoon assosioitumista varten tarvitaan oikeat tiedot, jotka lähetetään beacon-paketeissa sekä assosioitumisen yhteydessä lähetettävissä paketeissa. Tarvittavien tietojen hankkimiseen kuuluvia asioita käytiin läpi kappaleessa 5.1.1. Tarvittaviksi tiedoiksi luokitellaan SSID ja oikea kanava, jolla tukiaseman liikennöidään. Verkossa liikennöintiä varten tarvitaan vielä IP-osoite ja jos verkosta halutaan liikennöidä muihin verkkoihin, myös yhdyskäytävän osoite. Verkkoa passiivisesti kuuntelemalla ja paketteja kaappaamalla voidaan päätellä edellä mainitut molemmat osoitteet. Mikäli verkossa on käytössä DHCP osoitteiden jakamista varten, tarvittavat osoitteet saadaan automaattisesti verkolta. Verkkoon on saatettu myös asettaa päälle sallittujen MAC-osoitteiden suodatus, jolloin vain verkon ylläpitäjän sallimat MAC-osoitteet saavat assosioitua verkon kanssa. Verkossa sallitun MAC-osoitteen saa selville kuuntelemalla verkossa siirrettyä liikennettä, koska jokaisessa data-kehyksessä on niin lähettäjän, kuin vastaanottajankin MAC-osoitteet. Sallitun MAC-osoitteen selvittämisen jälkeen voidaan oman verkkokortin MAC-osoite ohjelmallisesti vaihtaa esiintymään verkossa sallitun kortin MAC-osoitella.

5.3.3 Salakuuntelu

Kappaleessa 5.3.1 on salakuuntelua käyty läpi verkon kanssa assosioitumisen mahdollistavien tietojen hankkimiseksi. Salakuuntelua voi harrastaa siihen sopivan ohjelmiston kanssa laitteessa, jossa on IEEE 802.11-yhteensopiva langaton verkkokortti. Verkkokortille on olemassa 2 tilaa, promiscuous- tai monitor-tila. Promiscuous-tilassa verkkokortti assosioituu normaalisti tukiaseman kanssa, ja tämän jälkeen voi aloittaa liikenteen kaappaamisen. Monitor-tilassa verkkokortti ei assosioidu tukiaseman kanssa, vaan kuuntelee passiivisesti kanavalla tapahtuvaa liikennöintiä. sniffer-ohjelmilla voidaan myös valita tapahtuvaksi kanavalta toiselle hyppimistä, jolloin voidaan kuunnella vuorollaan kaikkia kanavia. Yhdellä kertaa kortti voi lukittua vain yhdelle kanavalle. /10/

On olemassa ohjelmia, joilla voi kuunnella liikennettä ja tallentaa ne log-tiedostoon ja analysoida kaapattua liikennettä myöhemmin protokolla-analysaattorilla. Kismet /12/ on esimerkki ohjelmasta, joka kaappaa liikennettä ja tallentaa tiedot useisiin formaatteihin myöhempää analysointia varten. Toiset protokolla-analysaattorit osaavat kaapata liikennettä ja analysoida sitä samaan aikaan. Tämänkaltaisia ohjelmia ovat esimerkiksi Wireshark /15/ ja Omnipeek /14/.

WEP:llä salattuja paketteja voidaan kaapata samalla tavalla, mutta niiden lukemiseksi on ensin selvitettävä käytetty salausavain. WEP salauksen murtaminen on esitetty kappaleessa 6.3.2. Monitor-tilassa olevan liikennettä kaappaavan langattoman aseman havaitseminen on protokollatasolla mahdotonta. Asemasta vuotaa ulos pientä radiosäteilyä, mutta sen havaitsemiseksi tarvitaan herkät laitteet. /10/

5.3.4 Laiton tukiasema verkossa

Laittomia tukiasemia verkossa kutsutaan Rogue Access Pointeiksi. Nämä tukiasemat voivat olla joko verkossa sallittujen käyttäjien asentamia, omia langattomia tukiasemia tai vihamielisen hyökkääjän paikalle toimittama tukiasema Man-in-the-Middle-hyökkäysten tekemiseksi. Verkossa sallitun käyttäjän asentama tukiasema voi helposti muodostaa koko verkkoa uhkaavan tietoturva-aukon. Laittoman tukiaseman asentanut käyttäjä ei välttämättä itse edes tiedosta luomaansa uhkaa verkon turvallisuudelle.

Toisenlainen laiton tukiasema verkossa on hyökkääjän oma tukiasema, johon hyökkääjä pyrkii saamaan verkon käyttäjiä assosioitumaan. Langattomat verkkokortit valitsevat yleensä käytettäväksi tukiasemaksi sen tukiaseman, minkä signaali on kaikista vahvin. Vihamielinen tukiasema saattaa lähettää siihen assosioituneiden käyttäjien lähettämät paketit eteenpäin varsinaiseen verkkoon ja näin hyökkääjä voi saada tietoonsa huomattavan tärkeitä asioita ilman käyttäjän itsensä edes sitä huomaamatta.

5.3.5 Man in the Middle

Kappaleessa 5.3.4 kerrottiin Man-in-the-Middle-hyökkäysten toteuttamisesta laittoman tukiaseman avulla. Tämä ei kuitenkaan ole ainoa keino liikenteen ohjaamiseksi hyökkääjän omaan langattomaan asemaan.

ARP on protokollana erittäin yksinkertainen. Tiivistettynä ARP toimii näin: kun lähiverkossa sijaitsevat laitteet haluavat kommunikoida keskenään sekä asemilla on tiedossaan vain toistensa IP-osoitteet. Koska IP-osoitteiden kanssa ei kommunikoida lähiverkossa, tarvitsee tämä osoite jotenkin muuttaa Ethernetin käyttämään Layer 2-osoitteeseen, MAC-osoitteeseen. ARP-kysely lähetetään broadcast-lähetyksenä koko lähiverkolle, jossa pyydetään tietyn IP-osoitteen omaavaa asemaa vastaamaan MAC-osoitteensa ARP-kyselyn lähettäjälle. Vastauksen saatuaan, osoitetta kysyvä taho päivittää oman ARP-taulunsa, johon merkitään IP-osoitetta vastaava MAC-osoite. ARP ei mitenkään todenna vastauksen lähettäjän aitoutta ja luottaa siihen, että vastauksen lähettäjä on verkon laillinen käyttäjä. Yli 30 vuotta sitten Ethernetiä kehitettäessä ei tietoturva-asioita otettu vielä vakavasti huomioon, ja ARP on lähtöisin tältä aikakaudelta.

ARP spoofing käyttää hyväkseen sitä, ettei osapuolten välillä ole mitään todentamista. Vihamielinen hyökkääjä voi lähettää molemmille osapuolille ARP-vastauksena omien verkkokorttiensa osoitteet, jotka siis hyväksytään ja päivitetään ARP-tauluun mitään kyselemättä. Näin osapuolet luulevat kommunikoivansa suoraan keskenään, mutta todellisuudessa kaikki paketit lähetetään hyökkääjän koneen kautta vastapuolelle. Tämä taas mahdollistaa sen, että hyökkääjä voi tallentaa paketit itselleen, muokata niitä ja lähettää eteenpäin tai pelkästään seurata liikennöintiä osapuolten välissä kiinnostavien tietojen löytämiseksi. /16/

5.3.6 Palvelunestohyökkäykset

Palvelunestohyökkäyksillä pyritään lamauttamaan verkon toiminta niin, ettei verkossa sallitut käyttäjät pysty käyttämään sen palveluja hyväkseen. Palvelunestohyökkäyksiä kutsutaan yleisesti DoS-hyökkäyksiksi (Denial of Service). Käytössä on myös nimitys hajautetulle palvelunestohyökkäykselle, DDoS

(Distributed Denial of Service), jossa hyökkäykseen käytettyjä koneita sijaitsee suuri määrä ympäri Internetiä. Tyypillisiä piirteitä DoS-hyökkäyksille ovat esim. huomattavasti tavanomaista hitaampi verkon suorituskyky, tiettyjen verkkosivujen toimimattomuus ja mahdollisesti koko Internetin toimimattomuus.

Palvelunestohyökkäykset voidaan suorittaa monella eri tapaa. Hyökättävään verkkoon voidaan toimittaa liikennettä niin suurella nopeudella, ettei verkko pysty enää kuljettamaan sallittua liikennettä verkossa. Tämän tyyppiset hyökkäykset ovat usein DDoS-hyökkäyksiä, jossa liikennettä lähetetään suurelta määrältä saastuneita koneita. Tiettyä palvelua kohtaan voidaan myös lähettää niin suuri määrä kyselyitä, ettei palvelua tarjoava kone pysty enää vastaamaan niin moneen kyselyyn. Hyökkäyksiksi voidaan myös lukea tilanteet, joissa tietyltä yksilöltä estetään pääsy palveluun tai estetään palvelun toimittaminen sen tilaajalle.

Palvelunestohyökkäys voidaan kohdistaa oikeastaan mihin tahansa verkkolaitteeseen, kuten esimerkiksi reitittimiin, sähköpostipalvelimiin tai nimipalvelua pyörittäviin palvelimiin. On olemassa viisi erilaista tapaa palvelunestohyökkäyksen toteuttamiseksi. Käytettävissä olevien resurssien varaaminen on yleinen tapa hyökkäykselle, tällaisia resursseja ovat esimerkiksi siirtokaista, levytila tai CPU-aika. Reititysinformaation toimittamisen estäminen tai väärän informaation toimittaminen on yksi tapa toteuttaa hyökkäys.
SYN-floodissa lähetetään suuri määrä TCP SYN-paketteja palveluun väärennetyllä lähetysosoitteella. Palvelu vastaa näihin TCP SYN-ACK-paketeilla, jotka lähtevät tekaistuun osoitteeseen, josta kuitenkaan ei koskaan tule vastausta. Näin palvelimelle muodostuu avoimia TCP-yhteyksiä, jotka varaavat rajattuna olevan määrän TCP-yhteyksiä käyttöönsä, jolloin sallittu liikenne ei pääse avaamaan uusia yhteyksiä. Palveluita voidaan myös häiritä lähettämällä TCP RST-paketteja kohteelle väärennetyillä tiedoilla, jolloin hyökkäyksen kohteena oleva kone sulkee TCP-yhteyden, jonka tiedot olivat TCP RST-paketissa. Fyysinen verkkolaitteiden häirintä ja siirtolinjojen sulkeminen ovat myös palvelunestohyökkäyksiä. /17/

Langattomiin verkkoihin kohdistetut hyökkäykset sijoittuvat kolmelle alimmalle tasolle OSI-mallissa. Langattomiin verkkoihin toimivat kuitenkin samat hyökkäykset, kuin lankaverkkoihinkin, ja tämän lisäksi langattomalle verkolle on

omat hyökkäyksensä. ARP-hyökkäys toimii myös tässä tilanteessa, jolloin verkkoon voidaan kertoa tekaistua MAC-osoitteita.

Ohjausliikennettä vastaan on helppo hyökätä langattomissa verkoissa, koska sen eheyttä ei tarkasteta ja standardista poikkeavat menettelytavat aiheuttaisivat yhteensopivuusongelmia laitteiden välillä. Kättelyvaiheessa asema lähettää siirtotielle RTS (Request To Send)-sanoman, jolla se pyytää lupaa aloittaa lähettäminen siirtotielle. Mikäli siirtotie on vapaa tukiasema vastaa lähettämällä CTS (Clear To Send)-sanoman kaikille verkossa oleville laitteille, jolloin kanava varataan lähetystä pyytäneelle asemalle. Hyökkääjän tekeytyessä verkon tukiasemaksi, voi hyökkääjä lähettää jatkuvasti CTS-paketteja siirtotielle ja näin estää verkon käyttäjiä varaamasta siirtotietä itselleen. Yhdellä CTS-viestillä voidaan kanava varata 32 ms ajaksi. /10/

Käyttäjien tunnistukseen ja assosiointiin liittyy useita DoS-hyökkäyksiä. Todennuksen purkava deauthentication-viesti langattoman aseman on pakko hyväksyä, jolloin asema siirtyy ensimmäiseen todentamattomaan tilaan. Kuten kuvasta (Kuva 3-7) voidaan nähdä, todentamattomassa tilassa asema hylkää kaikki muut, paitsi 1. luokan kehykset, joten datan liikennöintiä varten aseman on pakko hoitaa todentaminen uudestaan. Lähettämällä toistuvasti deauthentication-viestejä asemille, voidaan estää aseman pääsy verkkoon. Tässä tarkoituksessa disassociation-viestit eivät toimi samalla tavalla, koska pelkästään assosioituminen ei vaadi enää todentamista, joten asema pääsisi heti takaisin verkkoon. /10/

5.3.7 EAP-protokollaa vastaan tehtäviä hyökkäyksiä

Käyttäjän todentamista on käyty tarkemmin läpi kappaleessa. Kappaleessa 5.1 on käyty läpi erilaisia tapoja tunnistaa asiakas. Näissä hyökkäyksissä vihamielinen hyökkääjä voi kuunnella liikennettä passiivisesti saadakseen tietoonsa käyttäjän todentamiseen käytettäviä tunnuksia ja salasanoja. Toinen vaihtoehto on hyökkääjän tekeytyminen asiakkaaksi, palvelimeksi tai molemmiksi MitM-hyökkäyksen avulla. Todentamispalvelinta jäljitelläkseen hyökkääjän on käytettävä molempia, omaa

tukiasemaa sekä palvelinta. Linuxille löytyy useita ohjelmia, joilla voidaan samaa konetta käyttää sekä tukiasemana, että todentamispalvelimena. /1/

EAP-MD5- ja EAP-TLS-toteutuksia vastaan voidaan MitM-hyökkäys suorittaa lähettämällä hyökkääjän tukiasemaan assosioituneelle asemalle EAP-Success-paketti, jolloin asema siirtyy todennettuun tilaan. Käyttäjän todentamisen jälkeen hyökkääjän tukiasemasta lähetetään asiakkaalle disassociate-viesti, jolloin käyttäjä siirtyy assosioituneesta tilasta todennettuun tilaan, eli pysyy vielä todennettuna. Tämän jälkeen hyökkääjä voi ottaa todennetun käyttäjän MAC-osoitteen omaan käyttönsä ja saada pääsyn verkkoon ja sen palveluihin. Tämän hyökkäyksen toimimiseksi edellytetään, ettei verkossa ole salausta käytössä. /10/

5.3.8 WEP-protokollaa vastaan tehtäviä hyökkäyksiä

WEP pitää sisällään useita tietoturva-aukkoja ja epäkohtia avainten käsittelyssä. Selkeimmät epäkohdat löytyvät alustusvektoreiden (IV) valinnasta sekä alustusvektoreiden lähettämisestä selväkielisenä. Heikkojen alustusvektoreiden myötä RC4:n käyttämät salausavaimet ovat heikkoja. Tarkistussumman (ICV) laskemiseen käytetty CRC32 algoritmi on tarkistussumman laskemista varten käytettävä mekanismi, eikä sitä ole tarkoitettu viestin eheyden tarkastamiseen. Alustusvektoreiden esiintyminen on ennustettavissa ja ne voidaan käyttää myös uudestaan näin heikentäen käytettävän salausavaimen tehokkuutta. Edellä mainittujen lisäksi WEP ei pidä sisällään vahvaa molemmin puolista todentamista suojatun tunnelin muodostamista varten. /1/

WEP:ssä käytettävä salausalgoritmi RC4 luottaa siihen, ettei samaa salausavainta käytetä uudestaan. WEP:n käyttämä alustusvektori IV sallii 2^{24} arvoa, eli erilaisia salausavaimia voi muodostua n. 16,7 miljoonaa kappaletta avainvirtoja yhtä WEP-avainta kohden. Avaimen murtamisen sijasta voidaan jokainen näistä avainvirroista murtaa tai vaihtoehtoisesti odottaa alustusvektorin arvojen alkamista alusta, jolloin tapahtuu törmäys, jossa saadaan tietoja datasta sekä käytetystä avainvirrasta.

RC4 salausavaimen selvittämiseen ja sanakirjojen luomiseen on monia tekniikoita, ainakin teoriassa. Kaikille seuraavaksi esitellyille tekniikoille ei löydy toteutusta pääasiassa sen toteuttamisen hankaluuden vuoksi, mutta teoriassa ne ovat mahdollisia toteuttaa.

Yksinkertaisin hyökkäys on lähettää tiedossa oleva viesti lankaverkon puolelta langatonta verkkoa käyttävälle asiakkaalle. Viestin edettyä tukiasemalle asti, tukiasema salaa paketin ja lähettää sen eteenpäin asiakkaalle. Tukiaseman ja asiakkaan välistä radiotietä kuunteleva hyökkääjä saa passiivisesti selvitettyä WEP-salatun paketin, jonka sisällön hän jo tietää. Hyökkääjä voi suorittaa XOR-operaation kaappaamansa paketin ja selväkielisen viestin kanssa, ja näin saada haltuunsa yhden käytetyistä salausavaimista. Samassa paketissa näkyy selväkielisenä myös salausavaimen muodostamiseen käytetty IV. /1/

Alustusvektoreiden törmäykseen liittyy myös ns. syntymäpäiväparadoksi, joka tuntuu järjen vastaiselta idealta. Syntymäpäiväparadoksissa on ideana se, että jos huoneessa on 23 henkilöä, yli 50 % todennäköisyydellä kaksi näistä ihmisistä viettää syntymäpäivää samana päivänä. Ihmisten lukumäärän noustessa 50:een, kasvaa todennäköisyys jo 97 % asti. Tämä samainen toimintamalli pätee aloitusvektoreiden toiston välttämiseen, kun pieni osa mahdollisista alustusvektoreista on käytetty ja lähetetty verkkoon, satunnaisesti toimivan algoritmin on hankala välttää jo aiemmin käytettyjen alustusvektoreiden uusiutumista. Alustusvektoreiden uusiutumisen yhteydessä on helppo verrata näillä tiedoissa salattujen pakettien eroavaisuuksia. Näiden pakettien salaukseen käytetyt avainvirrat voidaan tallentaa myöhempää käyttöä varten, kun rakennetaan sanakirjaa salausavaimista. /1/

Aiemmin kappaleessa 5.2.1 on mainittu alustusvektoreiden valinnasta. Useat valmistajat aloittavat alustusvektoreiden arvon nollasta ja korottavat arvoa yhdellä jokaista pakettia varten. Virrat pois kytkettäessä laskuri palaa nollaan ja uudelleen virtoja kytkettäessä aloittaa laskemisen samoilla arvoilla, kun aikaisemmassa virtojen katkaisun yhteydessä. Tätä tapahtuu kannettavia tietokoneita käytettäessä monia kertoja päivässä, joten todennäköisesti muutama tuhat alustusvektorin ensimmäistä arvoa käydään useasti läpi saman päivän aikana.

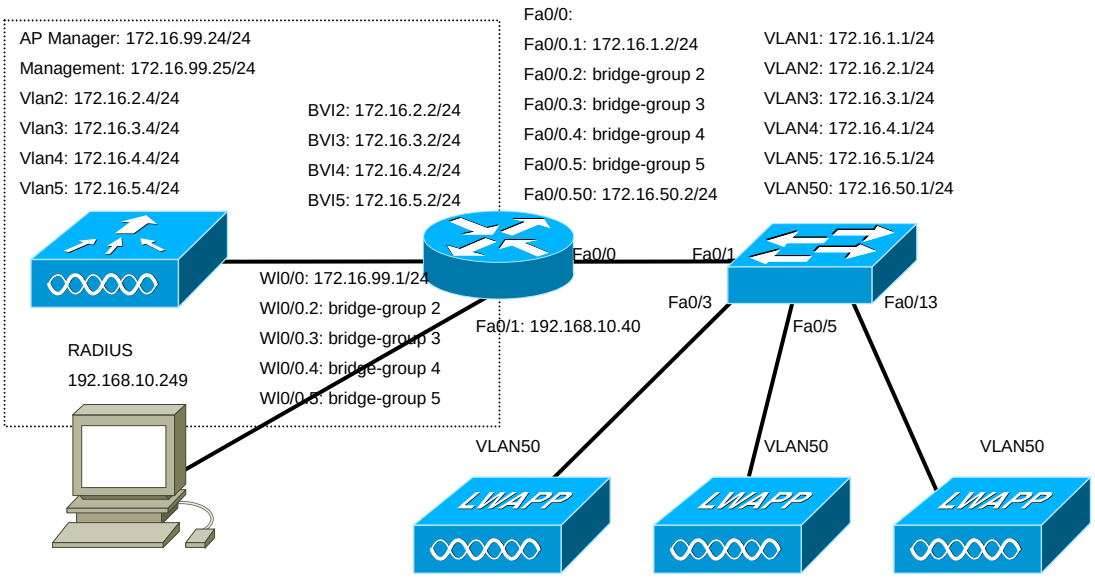
Aikaisemmat esimerkit esittelivät mahdollisia skenaarioita RC4-avainten selvittämiseksi, mutta helpompana vaihtoehtona on selvittää käytetty WEP-avain. Pienemmissä verkoissa käytetään käsin syötettäviä avaimia, mutta 26 merkkiä pitkä heksadesimaaliluku on hankala muistaa ja kirjoittaa joka kerta käsin. Valmistajat ovat kehittäneen erilaisia menetelmiä avainten säätämiseksi. Algoritmin käyttö vähentää valittavissa olevien WEP-avainten määrää ja muodostavat mahdollisuuden sanakirjahyökkäyksiä varten. WEP-avaimeen kohdistuvissa sanakirjahyökkäyksissä ajetaan sanakirjasta löytyvät avainsanat WEP-avaimen luomista varten tehdyn generaattorin läpi, jolla sanasta saadaan tehtyä WEP-avain. Sanakirjahyökkäys kohdistetaan verkosta kaapattuihin paketteihin, eli suoritetaan ns. off-line-hyökkäys. Hyökkäyksen onnistuminen voidaan tarkastaa vertaamalla ICV:n arvoja, mikäli puretun paketin tarkastussumma on oikein, hyökkäys on onnistunut ja oikea WEP-avain on löytynyt. /1/

WEP-avaimen luontiin käytetyn algoritmin luonteesta johtuen mahdollisia arvoja 40-bittistä WEP-avainta varten löytyy 2^{21} kappaletta avaimen luontiin käytetyn lauseen pituudesta riippumatta. Tästä johtuen mahdollisia avaimia syntyy noin 2 miljoonaa kappaletta, jotka voidaan murtaa brute force-hyökkäyksellä nopeasti.

Vahingollisin hyökkäys WEP-protokollaa vastaan on FMS (Fluhrer-Mantin-Shamir), joka on nimetty haavoittuvuuden löytäneiden henkilöiden mukaan. Hyökkäys kohdistuu RC4-salauksen avaimen luomisessa käytettyyn algoritmiin. Algoritmia käytettäessä osa salausavaimesta esiintyy avainvirrassa suuremmalla todennäköisyydellä. Hyökkäyksen yhteydessä kerätään suuri määrä dataa, josta etsitään heikosti muodostettuja avaimia. Paketteja, joista heikko avain löytyy, kutsutaan kiinnostaviksi paketeiksi. Kiinnostavista paketeista voi 5 % todennäköisyydellä voidaan kerätä talteen yksi tavu avaimesta. Ajan kuluessa julki vuotanut tavu esiintyy useammin, kuin muut mahdolliset arvot. Hyökkääjän on mahdollista saada avain murrettua vain noin miljoonalla kaapatulla paketilla. Runsaasti liikennöidyssä verkossa tämä paketit voidaan saada kerättyä jopa muutamassa minuutissa. /1/

6 DEMONSTRAATIO

6.1 Testiympäristö



Kuva 6-1. Testiympäristö

Laboratorioon rakennettiin kuvan (Kuva 6-1) mukainen testiympäristö langattoman verkon tietoturvan demonstroimiseksi ja tutkimiseksi. Verkko rakennettiin Cisco Systemsin laitteiden päälle.

Reitittimenä toimi 2811 ISR (Integrated Services Router) ohjelmistoversiolla C2800NM-ADVIPSERVICESK9-M ja IOS versio oli 12.4(11)T. Reitittimessä oli 2 100Mbps Ethernet-porttia sisäänrakennettuna.

Reitittimeen oli liitetty moduulina Ciscon NM-AIR-WLC6-K9 WLC (Wireless Lan Controller Module), jolla voi hallita kuutta tukiasemaa kerrallaan. Ennen verkon rakentamista, WLC:n ohjelmisto päivitettiin ensin versioon 3.2, koska esiasennettuna ollut ohjelmistoversio ei tukenut yli 32 Mt kokoisten ohjelmistojen siirtoa TFTP:n yli. Versiosta 3.2 voitiin ohjelmisto päivittää versioon 4.1.

Kytkimeksi valittiin Cisco Catalyst 3560 sen sisältämän PoE (Power over Ethernet)-ominaisuuden vuoksi. PoE:llä voidaan syöttää tukiasemien vaatima käyttösähkö suoraan verkkokaapelin kautta käyttämättömissä pareissa, ja näin vältytään erillisten virtalähteiden käyttämiseltä tukiasemien yhteydessä. Reitittimessä on 24 kappaletta 100 Mbps Ethernet-porttia. Kytkimessä käytetty ohjelmistoversio oli C3560-IPSERVICES-M ja IOS versio oli 12.2(25)SEE2.
Kytkimeen oli kytketty 3 kappaletta Cisco Aironet 1240AG tukiasemia, jotka toimivat lightweight toimintatilassa. Tukiasemien tarkka malli oli AIR-LAP1242AG-E-K9. Tukiasemat tukivat 802.11, 802.11a, 802.11b ja 802.11g standardeja.
RADIUS-palvelinta ajettiin VMWare virtuaalikoneessa, johon oli asennettu Windows Server 2003. RADIUS-palvelimena käytettiin Ciscon Secure ACS (Access Control Server) versiota 4.1.

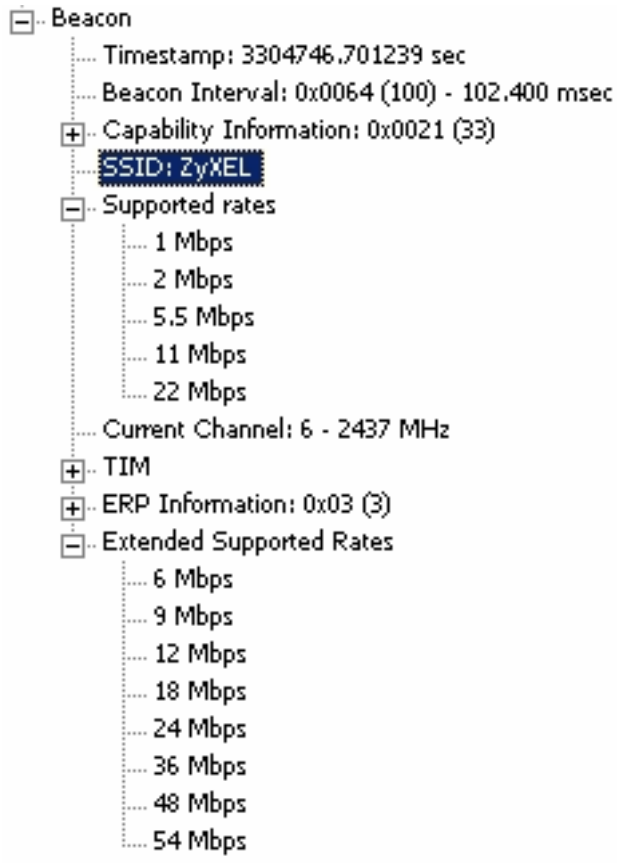
Kuvassa (Kuva 6-1) näkyy myös kaikki VLAN:t (Virtual Local Area Network), jotka luotiin verkkoon.
VLAN 1 oli vain hallintakäytössä.
VLAN 2:een liitettiin suojaamaton WLAN, joka oli kaikille avoin verkko.
VLAN 3:een liitettiin WLAN, jossa oli käytössä WEP salaus 104 bittisellä salausavaimella ja avainindeksi 1:llä. Käytetty salausavain oli a%g7F5T8VaRr&.
VLAN 4:ään ohjattiin liikenne, joka kuului WLAN:lle, jossa oli WPA-PSK suojaus.
VLAN 5 sidottiin WLAN:iin, jossa oli WPA2-suojaus 802.1x todentamisella.
VLAN 50 oli varattu tukiasemien käyttöön.

6.2 Tiedon hankkiminen

Langattoman verkon liikennettä voidaan seurata sujuvasti ulkopuolisena, passiivisena kuuntelijana. Kappaleessa 5.3 on kerrottu erilaisia hyökkäyksiä tiedon hankkimiseksi, jotta verkkoon päästäisiin kiinni.

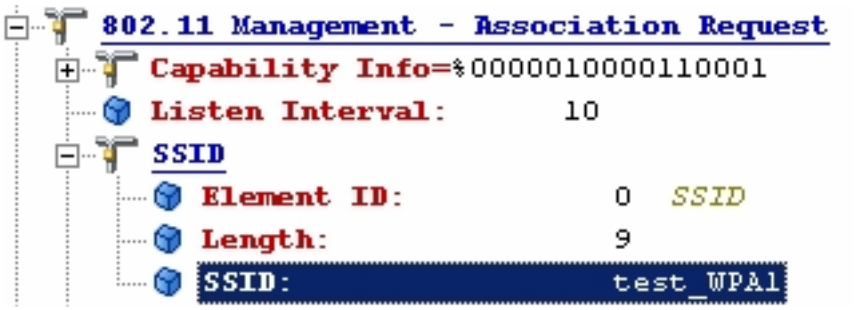
Tukiasemat lähettävät beacon sanomia usein liikennöimänsä kanavan radiotielle. Kuvassa (Kuva 6-2) on näkyvillä satunnaisen, avoimen verkon beacon-paketti. Paketti otettiin talteen ohjelmalla, jonka nimi on CommView for WiFi /24/. Paketista on piilotettu osa tiedoista, mutta avoimeen verkkoon pääsemisen kannalta kiinnostava osa, eli SSID on näkyvillä. Tämä verkko näyttää julistavan itseään

nimellä "ZyXEL", joka on oletusarvona ZyXELin langattomien tukiasemien SSID:nä. Todennäköisesti langattomalle tukiasemalle pääsisi kirjautumaan sisään oletusarvona olevalla salasanalla "1234".



Kuva 6-2. Beacon-paketti

Yllä olevassa esimerkissä beacon-paketista ei ollut piilotettu SSID:n lähettämistä. Vaikka verkon nimen lähettäminen estetään, verkon nimi löytyy myös association request-paketista, jolla pyydetään pääsyä verkkoon. Kuvassa (Kuva 6-3) on näkyvillä assosiointipyyntö testiverkkoon. Testiverkossa oli WPA-suojaus jaetulla avaimella käytössä, joten sinne ei tässä tapauksessa päästy suoraan yhdistämään. Tarkoituksena oli demonstroida SSID:n löytyminen ja selväkielisenä siirtäminen, vaikka verkossa olisikin salaus käytössä.



Kuva 6-3. Association Request

Näillä hankkimillamme tiedoilla pääsemme yhdistämään suojaamattomaan verkkoon vaivatta. DHCP:n puute kohdeverkossa ei kovinkaan paljon hidasta hyökkääjää, koska verkkoa lisää kuuntelemalla nähdään myös paketeissa oleva lähettäjän ja vastaanottajan IP ja tätä myöden saadaan selville verkossa käytössä oleva IP-avaruus.

6.3 WEP:n tarkastelu

Aikaisemmin tässä työssä on käyty läpi useita WEP suojaukseen liittyviä ongelmia. Liikenteen seuraaminen suoritettiin WildPacketsin OmniPeek Personal 4.1:llä /14/.

6.3.1 Alustusvektorit

Alustusvektoreiden valintaan liittyvistä ongelmista on kerrottu kappaleessa 5.2.1. Käytössä olleilla Cisco Aironet langattomilla verkkokorteilla muodostettiin telnet-yhteys langattoman verkon puolelta käytössä olleelle reitittimelle. Kaappauksen alkaessa alustusvektoreiden muodostaminen aloitettiin arvosta 0xAA0000 (Kuva 6-4) seuraavan arvon ollessa 0xAB0000 (Kuva 6-6). Kaapatusta liikenteestä huomattiin, että tukiasema lähetti vastauspaketit satunnaisella alustusvektorilla. Ensimmäinen tukiaseman lähettämä vastaus käytti alustusvektorin arvoa 0x25638E (Kuva 6-5) ja seuraava vastaus käytti alustusvektoria 0x38505E (Kuva 6-7). Paketeista on myös nähtävillä käytetty avainindeksi, joka on tässä tapauksessa ensimmäinen avainindeksi. Paketit on lähetetty samassa järjestyksessä, kuin ne on esitetty alla.

Kuva 6-4. 1. WEP paketti

Kuva 6-5. 2. WEP paketti

Kuva 6-6. 3. WEP paketti

Kuva 6-7. 4. WEP paketti

Langattoman verkkokortin lähettämistä paketeista voidaan päätellä, mikä tulee olemaan seuraava alustusvektorin arvo. Tässä tapauksessa se olisi 0xAC0000. Tukiaseman käyttämät alustusvektorit arvotaan satunnaisesti, jolloin seuraavaa arvoa ei voida päätellä.

6.3.2 WEP salausavaimen selvittäminen

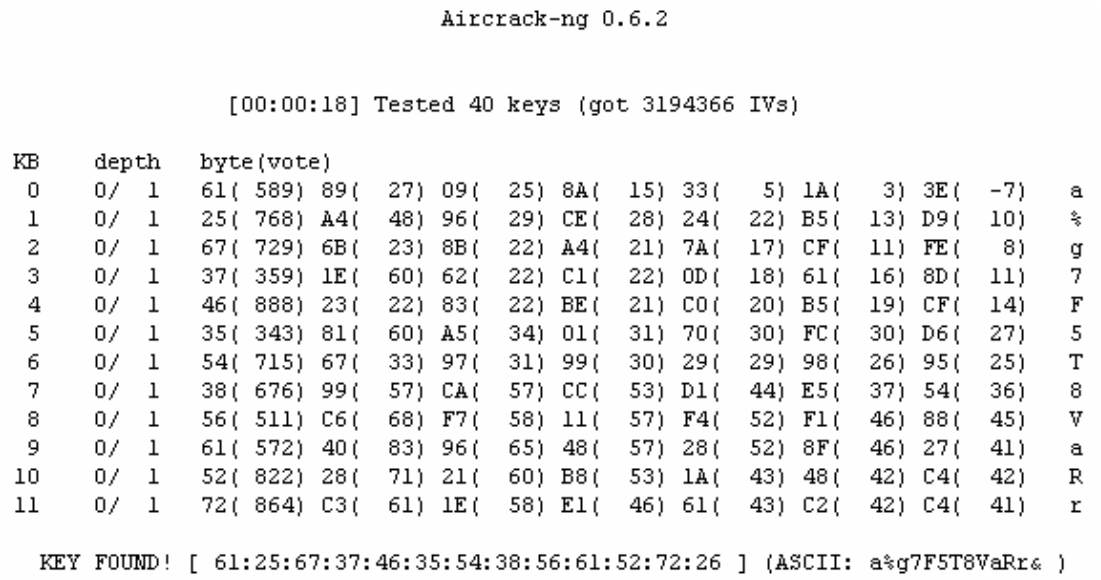
WEP:n salausavaimen murtamista varten kaapattiin suuri määrä alustusvektoreita. Kaapattujen alustusvektoreiden määrä oli 3 194 366. Avaimen selvittämiseksi ei

tarvitsisi kaapata näin suurta määrää alustusvektoreita. Yksi langaton työasema jätettiin kuuntelemaan passiivisesti liikennettä, kun kahden muun työaseman välillä siirrettiin satunnaisesti luotua liikennettä yön yli.

Alustusvektoreiden kaappaamiseen käytettiin Aircrack-ng-ohjelman /23/ mukana tullutta airodump-ng-ohjelmaa. Liikenteen kaappaaminen suoritettiin Windows XP-koneella. Airodump-ng tallensi kaappaamansa alustusvektorit erilliseen tiedostoon, josta ne luettiin avaimen selvittämistä varten Aircrack-ng-ohjelmalla. Aircrack-ng käyttää FMS-hyökkäystä avaimen selvittämiseksi. FMS-hyökkäyksestä on kerrottu kappaleessa 5.3.8.

Airodumpilla kaapatut alustusvektorit siirrettiin GNU/Linux-koneelle, ja laskeminen suoritettiin Debian 4.0 päällä. Kaapatuilla alustusvektoreilla 104-bittinen WEP-avain saatiin laskettua auki vain 18 sekunnissa. Huomattavasti pienemmillä alustusvektoreiden määrällä on myös mahdollista selvittää WEP-avain, jolloin alustusvektoreiden keräämiseen ei tarvita niin pitkää aikaa. Laskenta on koko prosessissa nopea toimitus. Jotta verkko olisi edes pienen aikaa turvassa, WEP-avainta pitäisi vaihtaa todella usein uuteen avaimeen, mikäli verkossa on runsaasti liikennettä.

Kuvassa (Kuva 6-8) on näkyvissä WEP-avaimen laskemiseen käytetyn ohjelman, Aircrackin, laskentaprosessi. Laskemiseen meni aikaa 18 sekuntia koneella, jonka suoritin on AMD Athlon XP 2600+ (1,91 GHz), joten laskentaan ei tarvita edes kallista laitteistoa, jopa vanha kannettava suoriutuu urakasta järkevässä ajassa.



Kuva 6-8. WEP-avaimen laskeminen

Avaimeksi paljastui "a&g7F5T8VaRr&", joka on tarpeeksi kryptinen siihen, että sanakirjahyökkäykset eivät pystyisi tätä selvittämään.

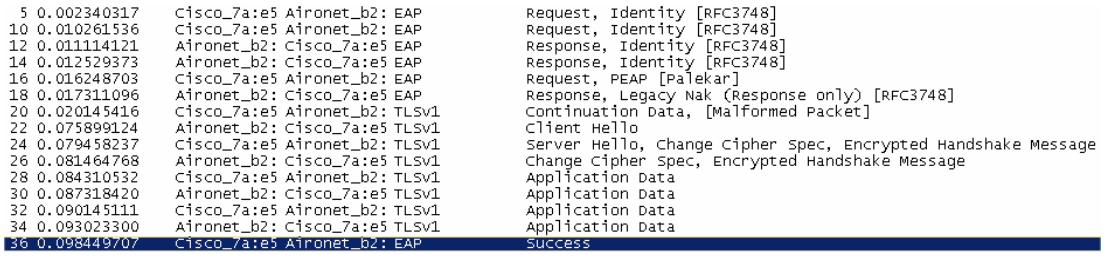
6.4 EAP-todentaminen

Käyttäjän todentamista ja EAP-protokollaa on tarkasteltu aiemmin kappaleessa 5.1. Käyttäjän todentamista tutkailtiin EAP-FAST protokollalla, jonka sisäisenä metodina toimi MS-CHAPv2. Asioiden tutkimista haittasi se pieni asia, että kaikki liikenne oli salattua niin radiotiellä, kuin langattoman verkon ohjaimelta RADIUS-palvelimelle.

Tässä esimerkissä on kuvattuna EAP-protokollan viestien vaihto lyhyesti. Liitteessä (Liite 1) on kuvassa (Kuva 6-9) esiintyvä viestien vaihto nähtävissä yksityiskohtaisemmin.

Liitteen (Liite 1) viesteissä 5, 10, 12 ja 14 on nähtävissä identiteetin vaihto-operaatio, jota seuraa viestissä 16 näkyvä RADIUS-palvelimen tarjoama sisäinen metodi, PEAP. Todennettava asiakas ei tätä hyväksy, vaan ehdottaa käytettäväksi metodiksi EAP-FAST:ia paketissa 18. RADIUS-palvelin aloittaa todentamisen paketissa 20 lähettämällä EAP-FAST Start-viestin. Paketti 22 pitää sisällään Client Hello-viestin, joka aloittaa suojatun tunnelin rakentamisen. Client Hello-viesti tarjoaa erilaisia salausmenetelmiä käytettäväksi tunnelin aikana, josta palvelin valitsee sopivimman.

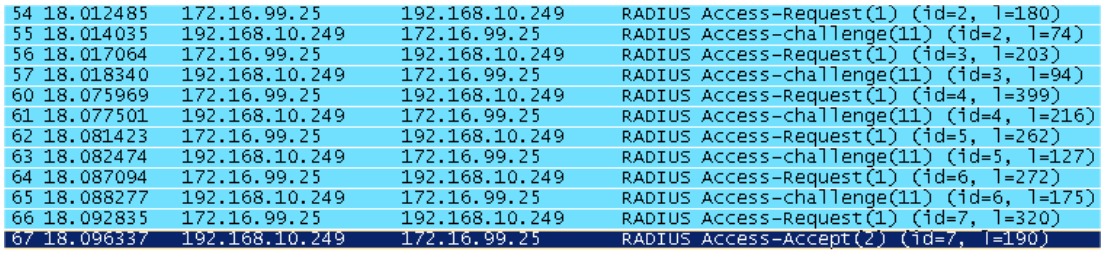
Palvelin ilmoittaa paketissa 24 omalla Server Hello-viestillä valinneensa käyttöön TLS_RSA_WITH_AES_128_CBC_SHA-menetelmän. Paketeissa 28, 30, 32 ja 34 nähdään vain TLSv1-tunnelin sisällä kulkeva salattu liikenne. Tunnelin sisällä suoritetaan varsinainen käyttäjän todentaminen metodilla MS-CHAPv2. TSLv1 on alun perin määritelty RFC 2246:ssa /26/. Prosessi päättyy paketissa 26 viestiin EAP-Success, joka kertoo todennettavalle asiakkaalle onnistumisesta. Mikäli todentaminen olisi epäonnistunut esim. salasanan ollessa väärä, viimeisenä viestinä olisi siirretty EAP-Failure.



5	0.002340317	Cisco_7a:e5	Aironet_b2: EAP	Request, Identity [RFC3748]
10	0.010261536	Cisco_7a:e5	Aironet_b2: EAP	Request, Identity [RFC3748]
12	0.011114121	Aironet_b2:	Cisco_7a:e5 EAP	Response, Identity [RFC3748]
14	0.012529373	Aironet_b2:	Cisco_7a:e5 EAP	Response, Identity [RFC3748]
16	0.016248703	Cisco_7a:e5	Aironet_b2: EAP	Request, PEAP [Palekar]
18	0.017311096	Aironet_b2:	Cisco_7a:e5 EAP	Response, Legacy Nak (Response only) [RFC3748]
20	0.020145416	Cisco_7a:e5	Aironet_b2: TLSv1	Continuation Data, [Malformed Packet]
22	0.075899124	Aironet_b2:	Cisco_7a:e5 TLSv1	Client Hello
24	0.079458237	Cisco_7a:e5	Aironet_b2: TLSv1	Server Hello, Change Cipher Spec, Encrypted Handshake Message
26	0.081464768	Aironet_b2:	Cisco_7a:e5 TLSv1	Change Cipher Spec, Encrypted Handshake Message
28	0.084310532	Cisco_7a:e5	Aironet_b2: TLSv1	Application Data
30	0.087318420	Aironet_b2:	Cisco_7a:e5 TLSv1	Application Data
32	0.090145111	Cisco_7a:e5	Aironet_b2: TLSv1	Application Data
34	0.093023300	Aironet_b2:	Cisco_7a:e5 TLSv1	Application Data
36	0.098449707	Cisco_7a:e5	Aironet_b2: EAP	Success

Kuva 6-9. EAP-viestien vaihto

Kuvassa (Kuva 6-10) näkyvien RADIUS-viestien sisällä kulkee EAP-viestit RADIUS-viestien sisään kapseloituna. Viesteissä suoritetaan onnistunut käyttäjän todentaminen.



54	18.012485	172.16.99.25	192.168.10.249	RADIUS Access-Request(1) (id=2, l=180)
55	18.014035	192.168.10.249	172.16.99.25	RADIUS Access-challenge(11) (id=2, l=74)
56	18.017064	172.16.99.25	192.168.10.249	RADIUS Access-Request(1) (id=3, l=203)
57	18.018340	192.168.10.249	172.16.99.25	RADIUS Access-challenge(11) (id=3, l=94)
60	18.075969	172.16.99.25	192.168.10.249	RADIUS Access-Request(1) (id=4, l=399)
61	18.077501	192.168.10.249	172.16.99.25	RADIUS Access-challenge(11) (id=4, l=216)
62	18.081423	172.16.99.25	192.168.10.249	RADIUS Access-Request(1) (id=5, l=262)
63	18.082474	192.168.10.249	172.16.99.25	RADIUS Access-challenge(11) (id=5, l=127)
64	18.087094	172.16.99.25	192.168.10.249	RADIUS Access-Request(1) (id=6, l=272)
65	18.088277	192.168.10.249	172.16.99.25	RADIUS Access-challenge(11) (id=6, l=175)
66	18.092835	172.16.99.25	192.168.10.249	RADIUS Access-Request(1) (id=7, l=320)
67	18.096337	192.168.10.249	172.16.99.25	RADIUS Access-Accept(2) (id=7, l=190)

Kuva 6-10. RADIUS-viestien vaihto

Kuvassa (Kuva 6-9) tapahtuva EAP-viestien vaihto tapahtuu langattoman asiakkaan ja langattoman tukiaseman välissä olevalla radiotiellä. Kuvassa (Kuva 6-10) näkyvä RADIUS-viestien vaihto tapahtuu langattoman verkon ohjaimen (WLC) sekä RADIUS todentamispalvelimen välillä lankaverkossa.

7 YHTEENVETO

Tämän työn tarkoituksena oli tutustua IEEE 802.11-standardin mukaisiin langattomiin lähiverkkojen tietoturvaan. Ennen tietoturvaan siirtymistä, työssä käytiin läpi yleistä asiaa langattomien verkkojen toiminnasta ja laitteista. Tietoturvan käsitteistöä käytiin läpi yleiskuvan luomiseksi langattoman lähiverkon tietoturvaan siirtymistä varten

Salausmenetelmät ja käyttäjän tunnistamiseen käytettävät protokollat olivat tarkemman tutkinnan kohteena. WEP-salausmenetelmän tietoturva-aukkoihin perehdyttiin niin teoriassa, kuin käytännössäkin. TKIP:n ja CCMP:n toimintaa käytiin läpi teoriassa. Avainten neuvottelemista ja käyttäjän todentamista tutkittiin kuuntelemalla liikennettä passiivisesti.

Testiympäristössä oli käytössä viisi pöytäkonetta, joista kahta konetta käytettiin liikenteen muodostamiseksi langattomaan verkkoon. Yhdellä koneella seurattiin passiivisesti verkossa tapahtuvaa liikennöintiä. Yksi kone oli verkon hallintaa varten sekä yhdellä koneella pyöritettiin todentamispalvelinta.

Työn ohessa tuli huomattua, että Cisco Systemsin tarjoamat ratkaisut ovat erittäin tehokkaita suurienkin verkkojen suojaamiseksi. Käytössä olleilla laitteilla voitiin toteuttaa verkko, joka kattaa vain erittäin pienen maantieteellisen alueen. Käytännössä näillä laitteilla saatiin toteutettua samat asiat, kuin suuryrityksille suunnatuilla laitteilla.

Testiympäristöä rakentaessa törmättiin ongelmiin, koska saatavilla ei ollut valmista ohjetta WLC moduulin käyttöönottoa varten. Näiden ongelmien ratkettua itse tietoturvamenetelmien käyttöönotto oli helppoa, eikä siinä esiintynyt suurempia ongelmia.

Tietoturvayritys Infosecurity Europen teettämässä kyselyssä /27/ vuonna 2008 yritettiin vaihtaa salasanoja suklaapatukoihin. 45 % kyselyyn osallistuneista naisista antoi salasanansa täysin tuntemattomalle ihmiselle suklaapatukkaa vastaan, miehistä 10 % paljasti salasanansa herkkuja vastaan. Vuonna 2007 samassa tutkimuksessa 64 % ihmisistä olisi paljastanut salasanansa suklaapatukan saadakseen. Tutkimus paljasti myös, että samoja salasanoja käytetään niin useissa sähköposteissa, kuin pankkitunnuksissa. Millään tietoturvamenetelmillä ei voida suojautua sosiaalista hakkerointia vastaan, jossa ihmiset ovat valmiita kertomaan salasanansa aivan tuntemattomille ihmisille niiden sitä pyytäessä. Hakkerit voivat myös esiintyä esim. ATK-ylläpitäjänä ja jonkin ongelmatilanteen varjolla he yrittävät onkia salasanaa selville. Parhaimmatkaan salausmenetelmät tai tietoturvaa parantavat ratkaisut eivät suojaa siinä tapauksessa, kun käyttäjä antaa käyttäjätunnuksensa ja salasanansa ulkopuolisen tahon tietoon.

8 LÄHDELUETTELO

/1/ Krishna Sankar, Sri Sundaralingam, Andrew Balinsky, Darrin Miller. Cisco Wireless LAN Security. 4th ed. Cisco Press, 2005. 500 s.

/2/ Mike Loukides, Colleen Gorman, Ellie Volckhausen, David Futato. 802.11 Wireless Networks: The Definitive Guide. 2nd ed. O'Reilly Media, Inc., 2005. 504 s.

/3/ Kaj Granlund. Langaton tiedonsiirto. 1. painos. Docendo Finland Oy, 2001. 399 s.

/4/ IEEE 802.11 Official Timelines
http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm
[Viitattu 9.3.2008]

/5/ Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications
http://standards.ieee.org/board/nes/projects/802-11n.pdf [Viitattu 9.3.2008]

/6/ ANSI/IEEE Std 802.11, Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. R2003. IEEE-SA Standars Board, 1999. 528 s.

/7/ Diffie-Hellman key exchange
http://en.wikipedia.org/wiki/Diffie-Hellman [Viitattu 15.3.2008]

/8/ Wireless Network Security 802.11, Bluetooth and Handheld Devices http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf [Viitattu 16.3.2008]

/9/ IEEE Std 802.11g-2003, Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amandment 4: Further Higher Data Rate Extension in the 2,4 GHz Band. IEEE-SA Standards Board, 2003. 77s

/10/ Ahvenainen, M., 2003. LANGATTOMIEN LÄHIVERKKOJEN TURVALLISUUS [Diplomityö] http://keskus.hut.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf [Viitattu 18.3.2008]

/11/ Wardriving http://en.wikipedia.org/wiki/Wardriving [Viitattu 18.3.2008]

/12/ Kismet 802.11 Layer 2 network detector. http://www.kismetwireless.net/ [Viitattu 18.3.2008]

/13/ Netstumbler http://netstumbler.com/ [Viitattu 18.3.2008]

/14/ Omnipeek http://www.wildpackets.com [Viitattu 18.3.2008]

/15/ Wireshark http://www.wireshark.org [Viitattu 18.3.2008]

/16/ ARP Cache Poisoning http://www.grc.com/nat/arp.htm [Viitattu 19.3.2008]

/17/ Denial-of-service attack

http://en.wikipedia.org/wiki/Denial-of-service_attack [Viitattu 19.3.2008]

/18/ Extensible Authentication Protocol (EAP)
http://tools.ietf.org/html/rfc3748 [Viitattu 24.3.2008]

/19/ Extensible Authentication Protocol
http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol [Viitattu 24.3.2008]

/20/ Transport Layer Security
http://en.wikipedia.org/wiki/Transport_Layer_Security [Viitattu 24.3.2008]

/21/ RADIUS
http://en.wikipedia.org/wiki/RADIUS [Viitattu 28.3.2008]

/22/ Advanced Encryption Standard
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard [Viitattu 16.4.2008]

/23/ Aircrack-ng
http://www.aircrack-ng.org/doku.php [Viitattu 23.4.2008]

/24/ Wireless Network Analyzer and Monitor – CommView for WiFi
http://www.tamos.com/products/commwifi/ [Viitattu 25.4.2008]

/25/ The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)
http://tools.ietf.org/html/rfc4851 [Viitattu 26.4.2008]

/26/ The TLS Protocol Version 1.0
http://tools.ietf.org/html/rfc2246 [Viitattu 26.4.2008]

/27/ Women 4 times more likely than men to give passwords for chocolate http://www.infosec.co.uk/page.cfm/Action=Press/PressID=1071 [Viitattu 26.4.2008]

LIITE 1

EAP-FAST-TODENTAMISEN AIKANA VAIHDETUT VIESTIT

```
No.     Time           Source                Destination           Protocol Info
      5 0.002340317    Cisco_7a:e5:d3        Aironet_b2:5d:2c      EAP      Request,
Identity [RFC3748]

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 55
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 1
        Length: 55
        Type: Identity [RFC3748] (1)
        Identity (50 bytes): \000networkid=test_WPA2,nasid=Cisco_b0:5d:80,portid=1

No.     Time           Source                Destination           Protocol Info
     10 0.010261536    Cisco_7a:e5:d3        Aironet_b2:5d:2c      EAP      Request,
Identity [RFC3748]

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 55
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 2
        Length: 55
        Type: Identity [RFC3748] (1)
        Identity (50 bytes): \000networkid=test_WPA2,nasid=Cisco_b0:5d:80,portid=1

No.     Time           Source                Destination           Protocol Info
     12 0.011114121    Aironet_b2:5d:2c      Cisco_7a:e5:d3        EAP      Response,
Identity [RFC3748]

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 11
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 1
        Length: 11
        Type: Identity [RFC3748] (1)
        Identity (6 bytes): luojus

No.     Time           Source                Destination           Protocol Info
     14 0.012529373    Aironet_b2:5d:2c      Cisco_7a:e5:d3        EAP      Response,
Identity [RFC3748]

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
```

```
    Length: 11
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 2
        Length: 11
        Type: Identity [RFC3748] (1)
        Identity (6 bytes): luojus

No.     Time           Source                Destination           Protocol Info
     16 0.016248703    Cisco_7a:e5:d3        Aironet_b2:5d:2c      EAP      Request,
PEAP [Palekar]

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 58
        Length: 6
        Type: PEAP [Palekar] (25)
        Flags(0x21): Start
        PEAP version 1

No.     Time           Source                Destination           Protocol Info
     18 0.017311096    Aironet_b2:5d:2c      Cisco_7a:e5:d3        EAP      Response,
Legacy Nak (Response only) [RFC3748]

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 6
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 58
        Length: 6
        Type: Legacy Nak (Response only) [RFC3748] (3)
        Desired Auth Type: EAP-FAST [Cam-Winget] (43)

No.     Time           Source                Destination           Protocol Info
        20 0.020145416      Cisco_7a:e5:d3            Aironet_b2:5d:2c         TLSv1
Continuation Data, [Malformed Packet]

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 26
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 59
        Length: 26
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x21): Start
        FAST version 1
        Secure Socket Layer
[Malformed Packet: SSL]

No.     Time           Source                Destination           Protocol Info
```

```
     22 0.075899124    Aironet_b2:5d:2c       Cisco_7a:e5:d3         TLSv1    Client
Hello

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 202
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 59
        Length: 202
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x1):
        FAST version 1
        Secure Socket Layer
            TLSv1 Record Layer: Handshake Protocol: Client Hello
                Content Type: Handshake (22)
                Version: TLS 1.0 (0x0301)
                Length: 191
                Handshake Protocol: Client Hello
                    Handshake Type: Client Hello (1)
                    Length: 187
                    Version: TLS 1.0 (0x0301)
                    Random
                        gmt_unix_time: Jun 12, 2007 09:55:50.000000000
                                                                    random_bytes:
3AA8D7013723862B7EB68068698E31B324812A498C64249D...
                    Session ID Length: 0
                    Cipher Suites Length: 8
                    Cipher Suites (4 suites)
                        Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
                        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
                        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
                        Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA (0x0034)
                    Compression Methods Length: 1
                    Compression Methods (1 method)
                        Compression Method: null (0)
                    Extensions Length: 138
                    Extension: EAP-FAST PAC-Opaque
                        Type: EAP-FAST PAC-Opaque (0x0023)
                        Length: 134
                        Data (134 bytes)

No.     Time           Source                Destination           Protocol Info
     24 0.079458237    Cisco_7a:e5:d3         Aironet_b2:5d:2c       TLSv1    Server
Hello, Change Cipher Spec, Encrypted Handshake Message

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 148
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 60
        Length: 148
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x81): Length
        FAST version 1
```

```
        Length: 138
        Secure Socket Layer
            TLSv1 Record Layer: Handshake Protocol: Server Hello
                Content Type: Handshake (22)
                Version: TLS 1.0 (0x0301)
                Length: 74
                Handshake Protocol: Server Hello
                    Handshake Type: Server Hello (2)
                    Length: 70
                    Version: TLS 1.0 (0x0301)
                    Random
                        gmt_unix_time: Apr 15, 2007 13:07:44.000000000
                                                                    random_bytes:
EB033D5756F1EF7159BD10EE3AEFC4BF3E3C3DDECF456EDE...
                    Session ID Length: 32
                    Session ID: F955E3C51AC5B3B97C226EE8D307932A7456119D56F66ECE...
                    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
                    Compression Method: null (0)
            TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
                Content Type: Change Cipher Spec (20)
                Version: TLS 1.0 (0x0301)
                Length: 1
                Change Cipher Spec Message
            TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
                Content Type: Handshake (22)
                Version: TLS 1.0 (0x0301)
                Length: 48
                Handshake Protocol: Encrypted Handshake Message

No.     Time           Source                Destination           Protocol Info
     26 0.081464768    Aironet_b2:5d:2c      Cisco_7a:e5:d3        TLSv1     Change
Cipher Spec, Encrypted Handshake Message

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 65
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 60
        Length: 65
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x1):
        FAST version 1
        Secure Socket Layer
            TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
                Content Type: Change Cipher Spec (20)
                Version: TLS 1.0 (0x0301)
                Length: 1
                Change Cipher Spec Message
            TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
                Content Type: Handshake (22)
                Version: TLS 1.0 (0x0301)
                Length: 48
                Handshake Protocol: Encrypted Handshake Message

No.     Time           Source                Destination           Protocol Info
```

```
        28  0.084310532      Cisco_7a:e5:d3            Aironet_b2:5d:2c         TLSv1
Application Data

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 59
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 62
        Length: 59
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x1):
        FAST version 1
        Secure Socket Layer
            TLSv1 Record Layer: Application Data Protocol: Application Data
                Content Type: Application Data (23)
                Version: TLS 1.0 (0x0301)
                Length: 48
                                                        Encrypted   Application   Data:
E9436FCAF1B2E6DC2892915DBFF717AE4F8A4A1137F66F62...

No.     Time           Source                Destination           Protocol Info
        30  0.087318420      Aironet_b2:5d:2c         Cisco_7a:e5:d3            TLSv1
Application Data

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 75
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 62
        Length: 75
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x1):
        FAST version 1
        Secure Socket Layer
            TLSv1 Record Layer: Application Data Protocol: Application Data
                Content Type: Application Data (23)
                Version: TLS 1.0 (0x0301)
                Length: 64
                                                        Encrypted   Application   Data:
DCE3B2210206F90E27FEDFD4147A2F4648C4F32A8E8A8C0A...

No.     Time           Source                Destination           Protocol Info
        32  0.090145111      Cisco_7a:e5:d3            Aironet_b2:5d:2c         TLSv1
Application Data

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 107
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 63
        Length: 107
        Type: EAP-FAST [Cam-Winget] (43)
```

```
        Flags(0x1):
        FAST version 1
        Secure Socket Layer
            TLSv1 Record Layer: Application Data Protocol: Application Data
                Content Type: Application Data (23)
                Version: TLS 1.0 (0x0301)
                Length: 96
                                                    Encrypted   Application   Data:
B0720FDEC8F59DAAA6CCECDAD6CDF99A3E98363521AA10D9...

No.     Time           Source                Destination           Protocol Info
        34  0.093023300      Aironet_b2:5d:2c         Cisco_7a:e5:d3             TLSv1
Application Data

802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 123
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 63
        Length: 123
        Type: EAP-FAST [Cam-Winget] (43)
        Flags(0x1):
        FAST version 1
        Secure Socket Layer
            TLSv1 Record Layer: Application Data Protocol: Application Data
                Content Type: Application Data (23)
                Version: TLS 1.0 (0x0301)
                Length: 112
                                                    Encrypted   Application   Data:
F99D7B88592A80AA85C664BC1FD2203B43C2C554748C4792...

No.     Time           Source                Destination           Protocol Info
     36 0.098449707    Cisco_7a:e5:d3        Aironet_b2:5d:2c      EAP      Success

802.1X Authentication
    Version: 2
    Type: EAP Packet (0)
    Length: 4
    Extensible Authentication Protocol
        Code: Success (3)
        Id: 63
        Length: 4
```

TESTIVERKON REITITTIMEN KONFIGURAATIO

```
Current configuration : 2898 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RTR
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9Vwc$Py0eg2C34moiJIXWYYXrT0
!
no aaa new-model
!
ip cef
!
ip host DLS 172.16.1.1
!
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
bridge irb
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.2 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 bridge-group 2
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 bridge-group 3
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 bridge-group 4
!
interface FastEthernet0/0.5
 encapsulation dot1Q 5
 bridge-group 5
!
interface FastEthernet0/0.50
```

```
 encapsulation dot1Q 50
 ip address 172.16.50.2 255.255.255.0
 ip helper-address 172.16.99.24
!
interface FastEthernet0/1
 ip address 192.168.10.40 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface wlan-controller1/0
 ip address 172.16.99.1 255.255.255.0
!
interface wlan-controller1/0.2
 encapsulation dot1Q 2
 bridge-group 2
!
interface wlan-controller1/0.3
 encapsulation dot1Q 3
 bridge-group 3
!
interface wlan-controller1/0.4
 encapsulation dot1Q 4
 bridge-group 4
!
interface wlan-controller1/0.5
 encapsulation dot1Q 5
 bridge-group 5
!
interface BVI2
 ip address 172.16.2.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface BVI3
 ip address 172.16.3.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface BVI4
 ip address 172.16.4.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface BVI5
 ip address 172.16.5.2 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly
!
ip default-gateway 192.168.10.254
ip forward-protocol udp 12223
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 192.168.10.254
!
ip http server
no ip http secure-server
ip nat pool public 192.168.10.42 192.168.10.48 netmask 255.255.255.0
ip nat inside source list 1 pool public overload
!
access-list 1 permit 172.16.2.0 0.0.0.255
access-list 1 permit 172.16.3.0 0.0.0.255
access-list 1 permit 172.16.4.0 0.0.0.255
access-list 1 permit 172.16.5.0 0.0.0.255
!
control-plane
!
bridge 2 protocol ieee
bridge 2 route ip
bridge 3 protocol ieee
bridge 3 route ip
bridge 4 protocol ieee
bridge 4 route ip
bridge 5 protocol ieee
bridge 5 route ip
!
line con 0
 password cisco
 login
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
!
end
```

TESTIVERKON KYTKIMEN KONFIGURAATIO

```
Current configuration : 3000 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname DLS
!
enable secret 5 $1$iwh4$pbeR6x1UsmR.QAD/e7E0q1
!
no aaa new-model
ip subnet-zero
ip routing
ip host RTR 172.16.1.2
ip dhcp excluded-address 172.16.4.1 172.16.4.9
ip dhcp excluded-address 172.16.1.1 172.16.1.9
ip dhcp excluded-address 172.16.2.1 172.16.2.9
ip dhcp excluded-address 172.16.3.1 172.16.3.9
ip dhcp excluded-address 172.16.50.1 172.16.50.9
ip dhcp excluded-address 172.16.5.1 172.16.5.9
!
ip dhcp pool pool1
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.2
!
ip dhcp pool pool2
   network 172.16.2.0 255.255.255.0
   default-router 172.16.2.2
   dns-server 192.168.0.1
!
ip dhcp pool pool3
   network 172.16.3.0 255.255.255.0
   default-router 172.16.3.2
   dns-server 192.168.0.1
!
ip dhcp pool pool50
   network 172.16.50.0 255.255.255.0
   default-router 172.16.50.2
   option 43 ascii "172.16.99.24"
!
ip dhcp pool pool4
   network 172.16.4.0 255.255.255.0
   default-router 172.16.4.2
   dns-server 192.168.0.1
!
ip dhcp pool pool5
   network 172.16.5.0 255.255.255.0
   dns-server 192.168.0.1
   default-router 172.16.5.2
!
```

```
no file verify auto
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/14
!
interface FastEthernet0/15
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
```

```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan2
 ip address 172.16.2.1 255.255.255.0
!
interface Vlan3
 ip address 172.16.3.1 255.255.255.0
!
interface Vlan4
 ip address 172.16.4.1 255.255.255.0
!
interface Vlan5
 ip address 172.16.5.1 255.255.255.0
!
interface Vlan50
 ip address 172.16.50.1 255.255.255.0
!
ip default-gateway 172.16.1.2
ip classless
ip forward-protocol udp 12223
ip route 172.16.99.0 255.255.255.0 172.16.1.2
ip http server
!
control-plane
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 no login
!
end
```

TESTIVERKON WLC-MODUULIN KONFIGURAATIO

```
802.11a cac voice tspec-inactivity-timeout ignore
 802.11a cac voice stream-size 84000 max-streams 2
 802.11b cac voice tspec-inactivity-timeout ignore
 802.11b cac voice stream-size 84000 max-streams 2
 advanced location expiry tags 1200
 advanced location expiry client 150
 advanced location expiry calibrating-client 30
 advanced location expiry rogue-aps 1200
Cisco Public Safety is not allowed to set in this domain
 cdp disable
 country FI

interface create vlan2 2
interface create vlan3 3
interface create vlan4 4
interface create vlan5 5
interface address ap-manager 172.16.99.24 255.255.255.0 172.16.99.1
interface address management 172.16.99.25 255.255.255.0 172.16.99.1
interface address virtual 1.1.1.1
interface address dynamic-interface vlan2 172.16.2.4 255.255.255.0 172.16.2.1
interface address dynamic-interface vlan3 172.16.3.4 255.255.255.0 172.16.3.1
interface address dynamic-interface vlan4 172.16.4.4 255.255.255.0 172.16.4.1
interface address dynamic-interface vlan5 172.16.5.4 255.255.255.0 172.16.5.1
interface dhcp ap-manager primary 172.16.99.1
interface dhcp management primary 172.16.99.1
interface dhcp dynamic-interface vlan2 primary 172.16.2.1
interface dhcp dynamic-interface vlan3 primary 172.16.3.1
```

```
interface dhcp dynamic-interface vlan4 primary 172.16.4.1

interface dhcp dynamic-interface vlan5 primary 172.16.5.1

interface vlan vlan2 2

interface vlan vlan3 3

interface vlan vlan4 4

interface vlan vlan5 5

interface port ap-manager 1

interface port management 1

interface port vlan2 1

interface port vlan3 1

interface port vlan4 1

interface port vlan5 1

 logging buffered 1

 mesh security eap

 mgmtuser add cisco **** read-write

 mobility group domain testijuttu

 msglog level critical

 network rf-network-name testijuttu

 radius auth add 1 192.168.10.249 1645 ascii cisco

 snmp version v2c enable

 snmp version v3 enable

 sysname Cisco_e8:ec:a0

 wlan create 1 test_open test_open

 wlan create 2 test_WEP test_WEP

 wlan create 3 test_WPA1 test_WPA1

 wlan create 4 test_WPA2 test_WPA2

 wlan interface 1 vlan2

 wlan interface 2 vlan3

 wlan interface 3 vlan4
```

```
wlan interface 4 vlan5

wlan radius_server auth add wlan-id:4 global server index:1

wlan security static-wep-key enable 2

wlan security static-wep-key encryption 2 104 ascii a%g7F5T8VaRr& 1

wlan security static-wep-key encryption 3 104 ascii **** 1

wlan security static-wep-key encryption 4 104 ascii **** 1

wlan security wpa akm  802.1x disable 3

wlan security wpa akm  psk enable 3

wlan security wpa disable 1

wlan security wpa disable 2

wlan security wpa wpa1 enable 3

wlan security wpa wpa1 ciphers tkip enable 3

wlan security wpa wpa2 disable 3

wlan enable 1

wlan enable 2

wlan enable 3

wlan enable 4
```