Sami Javanainen

NGN-LABORATORION VERKKOLIITÄNNÄT

Tietotekniikan koulutusohjelma
Tietoliikenteen suuntautumisvaihtoehto
2009

NGN-LABORATORION VERKKOLIITÄNNÄT

Sami Javanainen
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikenteen suuntautumisvaihtoehto
Maaliskuu 2009
Työn valvoja: Aromaa Juha
UDK: 004.056.5, 004.73, 621.395
Sivumäärä: 73

Asiasanat: SIGTRAN, CESoPSN, IPSEC, etäyhteys

Työssä selvitettiin, miten Satakunnan ammattikorkeakoulun NGN-laboratorion verkosta voidaan tarjota palveluliitäntöjä kolmansille osapuolille. Mahdollisia palveluita olisivat esim. NGN-laboratorion älyverkko-liitäntä IN –ja CAMEL-pyynnöille, GSM-viestikeskus-liitäntä, kansainvälinen verkkovierailu tai etäälle sijoitettava tukiasema. Työssä oleellinen osa oli tunnistaa palvelut, sekä selvittää tapa jolla toteuttaa niiden vaatimat yhteydet, perustuen standardiratkaisuihin, kuten SIGTRAN tai CESoPSN.

NGN LABORATORY NETWORK CONNECTIONS

Sami Javanainen
Satakunta University of Applied Sciences
Degree Programme in information technology
March 2009
Supervisor: Aromaa Juha
UDC: 004.056.5, 004.73, 621.395
Number of pages: 73

Key words: SIGTRAN, CESoPSN, IPSEC, remote connection

This thesis investigated how to provide service connections to third parties from the NGN laboratory. Potential services could be for example the Intelligent Network access for IN and CAMEL requests, access to SMSC, international GSM roaming or a remote base station. It was essential to recognise these services and find out how those connections are realised based on standard solutions like SIGTRAN or CESoPSN.

LYHENTEET

NGN	New Generation Network
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
3G	Third Generation
IN	Intelligent Network
VOIP	Voice over Internet Protocol
SIP	Session Initiation Protocol
PSTN	Public Switched Telephone Network
IP	Internet Protocol
SIGTRAN	Signaling Transport
IETF	The Internet Engineering Task Force
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
MTU	Maximum Transmission Unit
PDU	Protocol Data Unit
PCM	Pulse Code Modulation
SS7	Signaling System 7
SCN	Switched Circuit Network
SG	Signaling Gateway
TUP	Telephone User Part
MGC	Media Gateway Controller
IPSP	IP Signaling Point
BSN	Backward Sequence Number
FSN	Forward Sequence Number
SCCP	Signaling Connection Control Part
IID	Interface Identifier
MAP	Mobile Application Part
CAP	Control Application Part
TCAP	Transaction Capabilities Application Part
MTP	Message Transfer Part
RANAP	Radio Access Network Application Part

ISDN	Integrated Services Digital Network
TDM	Time Division Multiplexing
LE	Local Exchange
AN	Access Network
CESoPSN	Circuit Emulation Service over Packet Switched Network
ITU-T	International Telecommunication Union Standardization Sector
IPSEC	IP Security Architecture
FTP	File Transfer Protocol
VPN	Virtual Private Network
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
SPI	Security Parameter Index
AH	Authentication Header
ESP	Encapsulation Security Payload

SISÄLLYS

1 JOHDANTO

NGN-laboratorio (New Generation Networks) Satakunnan ammattikorkeakoulun tiloissa on maailmassa ainutlaatuinen. Laboratorion ja opetuksen tasosta kertovat lukuisat yhteistyökumppanit sekä heidän halunsa kouluttaa työntekijöitään Porissa.

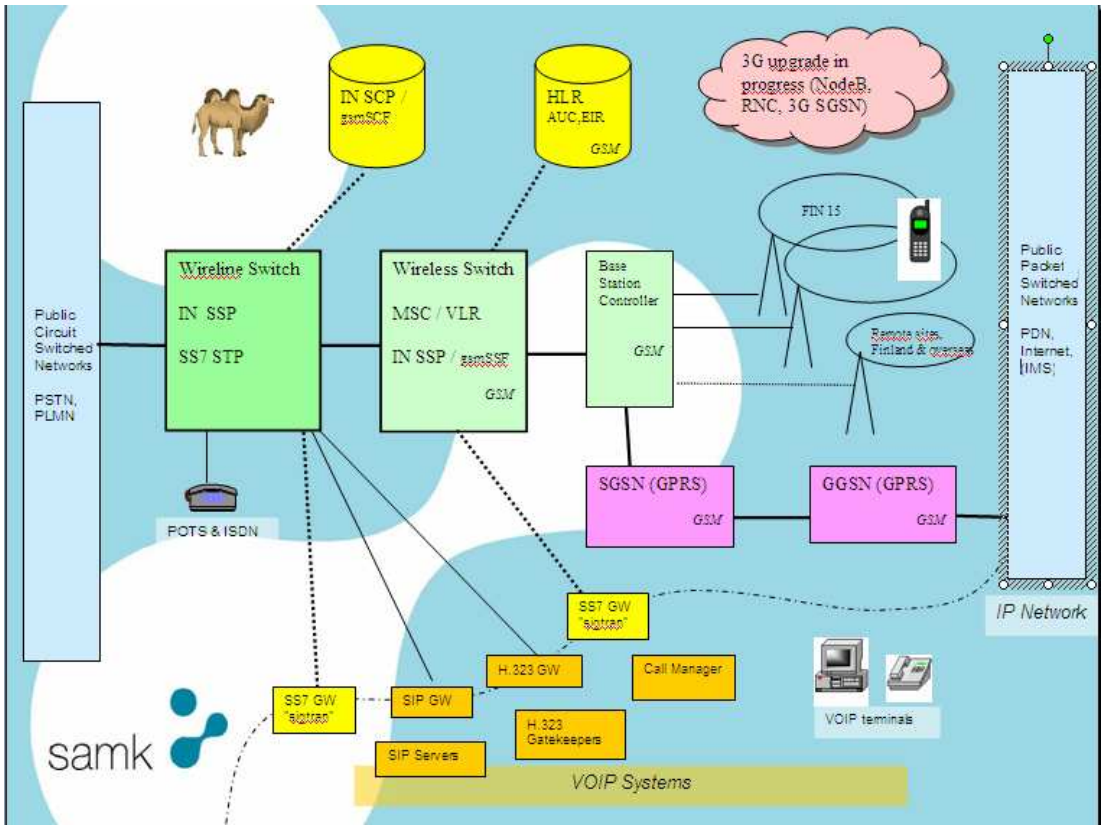
Tästä on syntynyt tarve kehittää ympäristöä lisää jossa kaikki osapuolet hyötyvät. Työssä tutkitaan eri liitäntätarpeita ja mahdollisuuksia NGN-laboratorion sekä yhteystyökumppaneiden välille. Työssä perehdytään tarkemmin tapaan jolla tarpeiden vaatimat yhteydet luodaan ja miten yhteyksistä tehdään turvallisia sekä laaditaan esimerkit miten yhteydet käytännössä määritellään.

2 NGN-YMPÄRISTÖN YHTEENLIITTÄMISTARPEET

New Generation Networks Laboratory (NGN-laboratorio) on Satakunnan ammattikorkeakoulun tietotekniikan koulutusohjelman oppimis- ja testausympäristö. Maailmassa ainutlaatuisessa laboratoriossa on lankaverkon ja matkapuhelinverkon (GSM, GPRS, 3G) laitteistot, älyverkkolaitteistoja (IN) sekä IP-puhelintekniikan (VOIP, SIP) laitteistoja. [2]

Opiskelijoiden lisäksi laboratoriota käyttävät monet yhteistyökumppanit testaukseen sekä erilaisten tuotekehitysprojektien toteuttamiseen. Yhteistyökumppaneita on jopa Yhdysvalloista ja Japanista asti. Tämä ympäristö antaa opiskelijoille erittäin hyvät lähtökohdat tulevaisuutta ajatellen. Lehtori Juha Aromaan kautta mahdollistui myös oma työharjoitteluni Yhdysvalloissa sijaitsevan yhteistyökumppanin kanssa. [2]

Laboratorio mahdollistaa aivan uuden oppimistason opiskelijoille. Enää ei ole vain totuttuja teoriatunteja vaan opettaja voi auditoriosta käsin operoida GSM-verkon laitteita, suorittaa mittauksia sekä tehdä analysointia reaaliajassa verkon tuella. Opiskelijoilla on mahdollisuus tehdä käytännön harjoituksia lukuisilla alaan liittyvillä kursseilla. [2]



NGN-laboratoriosta tekee ainutlaatuisen se, että opiskelijoiden käytössä on täydellinen matkapuhelinverkko. Laboratorio koostuu neljästä telecom-laitteistoympäristöstä: kiinteä puhelinverkko (PSTN), matkapuhelinverkko (GSM/GPRS), älyverkko (IN) ja IP-verkko (VOIP). Ympäristöt liittyvät toisiinsa sekä yleisiin tele- ja IP-verkkoihin. [2]

NGN- laboratoriossa on tunnistettu erilaisiin asiakasprojekteihin liittyen seuraavia yhteenliittämistarpeita: [2]

- yhteys etäälle sijoitettuun SM-SC:hen (MSC - SMSC), jotta voimme lähettää sekä vastaanottaa tekstiviestejä.
- IN-toiminta (SSP - SCP), gsmSSF – gsmSCF (CAMEL), missä lähinnä SCP sijoitettu etäälle.
- GSM/3G-tukiaseman tai ohjaimen sijoittaminen etäälle
- etäälle sijoitettu HLR-laitteisto
- testiympäristöjen välinen GSM-verkkovierailu esim. yhteistyökumppanimme yhdysvalloista tai mistä tahansa voisivat käyttää verkkoamme.

3 SIGTRAN

SIGTRAN (Signaling Transport) on IETF-työryhmän (The Internet Engineering Task Force) nimi, joka on tuottanut spesifikaatiot useaan protokollaan. SIGTRAN protokollapinon tarkoitus on siirtää piirikytkentäisen puhelinverkon (PSTN) paketteja IP:n yli. Sigtrania käytetään koko ajan enemmän ja enemmän. VoIP-verkossa SIGTRAN toimii ”liittimenä” PSTNään SG:n ja MGC:n kautta. SG:n tehtävänä on muuntaa ISUP/MTP ISUP/SIGTRANiksi. MGC vastaanottaa ISUP-sanomat ja luo vastaavat SIP-sanomat VoIP-verkon käyttöön. IMS:ssä SIGTRAN toimii rajapintana PSTN-verkolle, paljolti samalla tavalla kuin mitä se toimii VoIP-verkossa. SIGTRAN arkkitehtuuri muodostuu kolmesta osasta: [15]

Normaali muokkaamaton Internet Protokolla (IP)

Stream Control Transmission Protocol (SCTP) on IETF-työryhmän (Internet Engineering Task Force) määrittelemä uusi protokolla, joka toimii TCP- ja UDP–protokollien tilalla merkinannon siirrossa IP-verkossa.

Sovitusprotokollakerros, joka tukee esim. tiettyjä hallinnallisia toimintoja, joita tietyt piirikytkentäisen verkon sovellusprotokollat tarvitsevat. Tätä varten IETF on myös luonut uusia protokollia, näistä vain yksi voi olla aktiivisena kerralla:

- MTP2 User Peer-to-Peer Adaptation Layer (M2PA)
- MTP2 User Adaptation Layer (M2UA)
- MTP3 User Adaptation Layer (M3UA)
- SCCP User Adaption (SUA)
- ISDN User Adaption (IUA)
- V5 User Adaption (V5UA)

Protokollan kehitys sai alkunsa, kun VoIP-verkkoja yritettiin sulauttaa puhelinverkkoon ja tähän tarvittiin uusia keinoja. SIGTRAN:in päätarkoitus on vain siirtää protokollia, joten sanomat eivät muutu matkalla millään tavoin. Tämä tekee protokollasta läpinäkyvän. TCP on hyvin luotettava ja hyödyllinen protokolla siirrettäessä dataa pakettikytkentäisissä verkoissa, mutta piirikytkentäisen verkon sanomien siirtoon siitä ei ollut. Oli tarve kehittää uusi siirtoprotokolla, SCTP. [3][4]

3.1 SCTP (Stream Control Transmission Protocol)

Stream Control Transmission Protocol on luotettava siirtoprotokolla, joka toimii yhteydettömän ja pakettipohjaisen IP:n päällä. SCTP:n on luonut IETF ja se on standartoitu vuonna 2000 (RFC2960). Alunperin se luotiin luotettavaksi siirtoprotokollaksi välittämään viestejä SCTP:n eri käyttäjien välillä. SCTP on suunniteltu kuljettamaan PSTN merkinantosanomia IP-verkkojen yli, mutta on kykenevä laajempaankin käyttöön. SCTP on sovellustasoinen siirtoprotokolla, joka toimii UDP:n päällä. Se tarjoaa seuraavat palvelut käyttäjilleen:

- Sovellustasojen jakaminen osiin, mukautuakseen MTU:n kokoon.
- Jaksottainen datasähkeiden lähetys useissa datavirroissa sekä vaihtoehto valita tilauksen saapumis/toimitus-ilmoitus yksittäisistä datasähkeistä.
- Vaihtoehtoinen multiplexointi käyttäjän datasähkeestä SCTP:n datasähkeisiin, riippuen MTU:n kokorajoituksista. [4][11]

SCTP sisältää toiminnot jonka avulla vältetään kohtuulliset ruuhkat, vastustuskyvyn tulvimiselle sekä “valepukuisille” hyökkäyksille. SCTP datasähke koostuu tavallisesta otsikosta ja osista. Osat sisältävät joko hallintatietoa tai käyttäjädataa. [11]

SCTP:n PDU:ita (Protocol Data Unit) kutsutaan SCTP-paketeiksi. SCTP-paketeista muodostuu IP-paketin hyötykuorma. Paketti muodostuu osoitekentästä (Common Header, kuvassa bitit 0-64), joka vie ensimmäiset 12 tavua ja datakentistä (Chunk, ensimmäinen datakenttä kuvassa bitit 64-128 vihreänä), jotka vievät loput paketista. Jokaisen datakentän alussa on yhden tavun kokoinen tunniste (maksimissaan 255 eri tyyppistä datakenttää), josta se identifioidaan. Tunnisteita on tällä hetkellä määritelty 15 kappaletta. Loput kentästä vie 2 tavua ja tähän datan viemä tila päälle. [4]

Bits	Bits 0 - 7	8 - 15	16 -23	24 -31
+0	Source port		Destination port	
32	Verification tag			
64	Checksum			
96	Chunk 1 type	Chunk 1 flags	Chunk 1 length	
128	Chunk 1 data			
...	...			
...	Chuk n type	Chunk n flags	Chunk n length	
...	Chunk n data			

SCTP-paketin rakenne.

Lähdeporttinumero (Source Port)

Tämä on SCTP:n lähettäjän porttinumero. Vastaanottaja voi käyttää sitä yhdessä lähdeosoitteen kanssa tunnistaakseen kenelle tiedot kuuluvat. [11]

Kohdeporttinumero (Destination Port)

Tämä on SCTP:n porttinumero johon datasähke lähetetään. Vastaanottava pää käyttää tätä porttinumeroa muuttaakseen SCTP datasähkettä oikeaan muotoon vastaanottavaan päätepisteesen. [11]

Vahvistus (Verification Tag)

Vastaanottaja saa 32-bittisen datasähkeen, jolla varmennetaan yhteyden aitous. Lähetin asettaa Verification Tagin arvoiksi 0 jos datasähke pitää sisällään INIT-osan. Jos vastaanottaja vastaanottaa datasähkeen jotka kaikki ovat arvoltaan 0, se tarkastaa Chunk ID:n välittömästi seuraavasta otsikosta. Jos osan tyyppi ei ole INIT tai SHUTDOWN ACK, vastaanottaja pudottaa datasähkeen. [11]

Adler 32 Tarkistussumma (Adler 32 Checksum)

Tämä kenttä pitää sisällään Adler-32 tarkistussumman. [11]

Seuraavassa yksinkertaisempi kuva osista, jotka toimitetaan SCTP:n datasähkeeseen. Jokaisella osalla on Chunk ID-kenttä, tietty Flag-kenttä, Length-kenttä sekä Value-kenttä. [11]

1 byte	1 byte	2 bytes
Chunk ID	Chunk Flags	Chunk Length
Chunk Value (muuttuva)		

Chunk ID

Kenttä sisältää tiedon tyypin. Chunk ID:n arvot on määritelty seuraavasti:

ID ValueChunk Type

00000000 Payload Data (DATA)
00000001 Initiation (INIT)
00000010 Initiation Acknowledgment (INIT ACK)
00000011 Selective Acknowledgment (SACK)
00000100 Heartbeat Request (HEARTBEAT)
00000101 Heartbeat Acknowledgment (HEARTBEAT ACK)
00000110 Abort (ABORT)
00000111 Shutdown (SHUTDOWN)
00001000 Shutdown Acknowledgment (SHUTDOWN ACK)
00001001 Operation Error (ERROR)
00001010 State Cookie (COOKIE)
00001011 Cookie Acknowledgment (COOKIE ACK)
00001100 Reserved for Explicit Congestion Notification Echo (ECNE)
00001101 Reserved for Congestion Window Reduced (CWR)
00001110 to 11111101 - reserved by IETF

11111110	Vendor-specific Chunk Extensions
11111111	IETF-defined Chunk Extensions

Chunk Flags

Chunk Flagin tyyppi, kuten määritelty Chunk ID:ssä, määrittelee käytetäänkö näitä bittejä. Arvo on yleensä nolla jos toisin ei ole ennalta määrätty. [11]

Chunk Length

Pitää sisällään osan (chunk) koon oktetteina mukaan lukien muut kentät. [11]

Chunk Value

Tämä kenttä pitää sisällään varsinaisen tiedon mitä siirretään. Tämä on riippuvainen Chunk ID:stä. [11]

Initiation (INIT)

Tätä osaa käytetään aloittamaan SCTP “liitto” kahden päätepisteen välillä. INIT-osa pitää sisällään seuraavat parametrit. Jokainen parametri voidaan liittää vain kerran INIT-osaan, ellei toisin ole merkitty. [11]

Fixed Parameters	Status
Initiate Tag	Mandatory
Receiver Window Credit	Mandatory
Number of Outbound Streams	Mandatory
Number of Inbound Streams	Mandatory
Initial TSN	Mandatory

Variable Parameters	Status
IPv4 Address/Port	Optional
IPv6 Address/Port	Optional
Cookie Preservative	Optional
Reserved For ECN Capable	Optional
Host Name Address	Optional
Supported Address Types	Optional

Initiate Acknowledgement (INIT ACK)

INIT ACK-osaa käytetään myöntämään SCTP-assosiaation alkuunpano. Parametriosa INIT ACK:sta on muodostettu samalla tavalla INIT-osaan. Se käyttää kahta ylimääräistä muuttuvaa parametria: vastaajan eväste (The Responder Cookie) ja tuntematon parametri (Unrecognized Parameter). [11]

Selective Acknowledgement (SACK)

Tämä osa lähetetään etäisimpään päätepisteeseen, jotta saadaan kuittaus vastaanotetulle datalle. [11]

Heartbeat Request (HEARTBEAT)

Päätepisteen pitäisi lähettää tämä osa, jotta tiedetään onko toinen pää tavoitettavissa. Parametrikenttä pitää sisällään myös aika-arvot. [11]

Heartbeat Acknowledgement (HEARTBEAT ACK)

Päätepisteen pitäisi lähettää tämä kuittauksena Heartbeat Requestille. Parametrikenttä pitää sisällään myös aika-arvot. [11]

Abort Association (ABORT)

Tämä lähetetään silloin kun halutaan katkaista yhteys. Voi sisältää syyparametrin, jotta voidaan informoida vastapäätä minkä takia yhteys katkesi. [11]

SHUTDOWN

Käytetään kun yhteys halutaan lopettaa sulavasti. [11]

Shutdown Acknowledgement (SHUTDOWN ACK)

Lähetetään kun SHUTDOWN on vastaanotettu. Saattaa yhteyden lopettamisen päätökseen. SHUTDOWN ACK ei sisällä mitään parametreja. [11]

Operation Error (ERROR)

Lähetetään toiselle päätepisteelle, sisältää tiedon virheen tilasta. Sisältää yhden tai useamman syykoodin. [11]

State Cookie (COOKIE)

Käytetään vain ja ainoastaan yhteyden alustamisessa. Jokaista Data-osaa edeltää COOKIE-osa, mutta voidaan rinnastaa useampi Data-osa samaan datasähkeeseen yhdelle COOKIElla. [11]

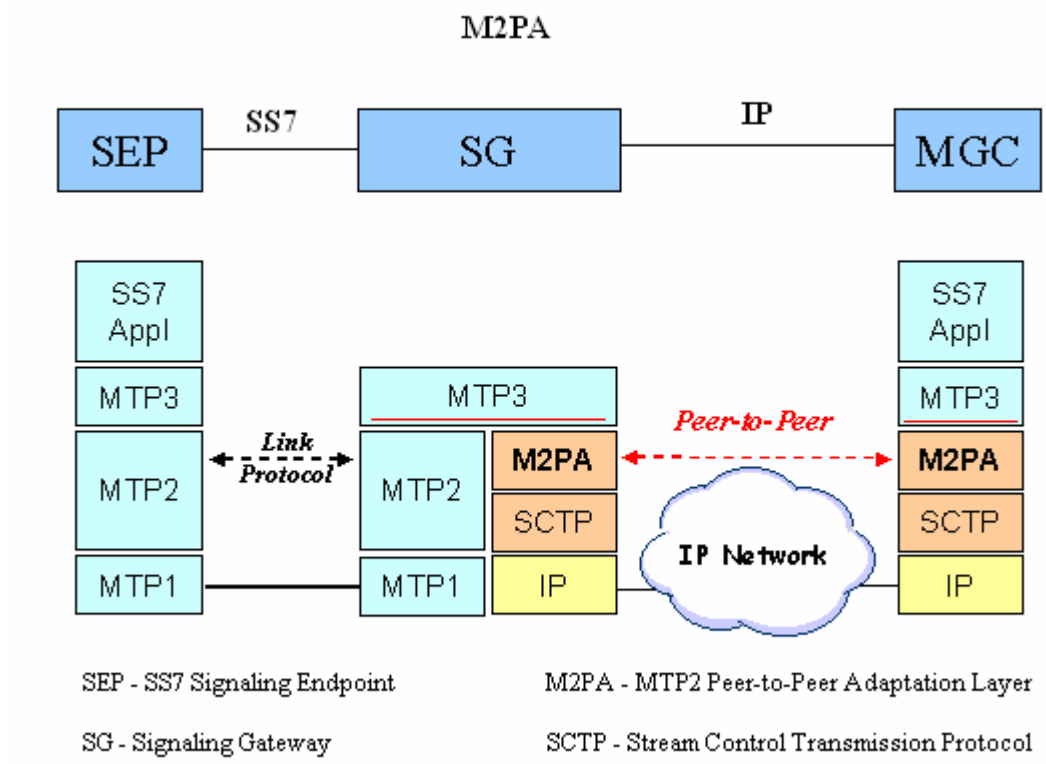
Cookie Acknowledgement (COOKIE ACK)
Käytetään yhteyden alustamisen yhteydessä. Tällä kuitataan perille tullut COOKIE. Jokaista Data-osaa edeltää COOKIE ACK. [11]

Payload Data (DATA)
Sisältää käyttäjätiedot. [11]

Suurimmat erot TCP:hen ovat multihoming ja multistreaming. TCP-virta (stream) määritellään jonoksi bittejä, joiden täytyy saapua kohteeseensa tietyssä järjestyksessä. SCTP-virta koostuu viestijonoista, eli bittien sijaan käsitellään kerralla kokonaisia sanomia. Multistreaming tarkoittaa SCTP:n kykyä lähettää rinnakkaisia viestivirtoja samaan aikaan. Esim. PCM:ssä (Pulse Code Modulation) useat samanaikaiset puhelut kulkevat eri aikaväleissä. SCTP-yhteydeltä vaaditaan myös, että usean puhelun data voidaan siirtää samanaikaisesti. Multihoming tarkoittaa ominaisuutta, joka mahdollistaa SCTP-päätepisteeseen osoittamisen eri IP-osoitteilla. Esim. jos päätepisteet ja verkko on konfiguroitu oikein, viestit matkaavat kohteeseensa eri fyysisiä siirtoteitä pitkin eri osoitteilla. Näin tiedonsiirto on paljon varmempaa mahdollisten verkkojen häiriöiden suhteen. [4][11]

Jos SCTP-päätepisteellä on useita eri IP-osoitteita, niin se ilmoittaa niistä kaikista käyttämällä INIT-datakentän (Chunk type 1) osoite –parametriä. Serveri ilmoittaa omista osoitteistaan INIT-ACK-datakentässä (Chunk type 2). Jos sanomien INIT- tai INIT-ACK-datakentissä ei ole IP-osoitteita, niin käytetään IP-paketin (joka kantaa SCTP-paketin) kohdeosoitetta. SCTP monitoroi yhteyksiä lähettämällä HEARTBEAT–datakenttiä kaikkiin käyttämättömiin siirtoteihin. Vastaanottaja vastaa HEARTBEAT-ACK–datakentällä. Näin jokaisen siirtotien tila on joko aktiivinen (active) tai toimimaton (inactive). [4]

3.2 MTP2 User Peer-to-Peer Adaptation Layer (M2PA)



M2PA protokolla tukee SS7:n MTP3:n merkinantosanomia IP:n yli käyttäen SCTP:n palveluita. M2PA:ta käytetään myös SS7:n merkinantopisteiden välissä käyttäen MTP3-protokollaa. SS7:n merkinantopisteet voivat myös käyttää standardeja SS7 linkkejä käyttäen SS7 MTP2:sta välittääkseen MTP3 merkinantosanomien kuljetuksen. [8]

SCN (Switched Circuit Network) on tarpeellinen merkinatoprotokolla merkinannon toimitukseen IP-verkon yli. Tämä pitää sisällään merkinannon siirron seuraavien välillä:

- SG (Signaling Gateway) ja MGC (Media Gateway Controller)
- SG (Signaling Gateway) ja IPSP (IP Signaling Point)
- IPSP ja IPSP

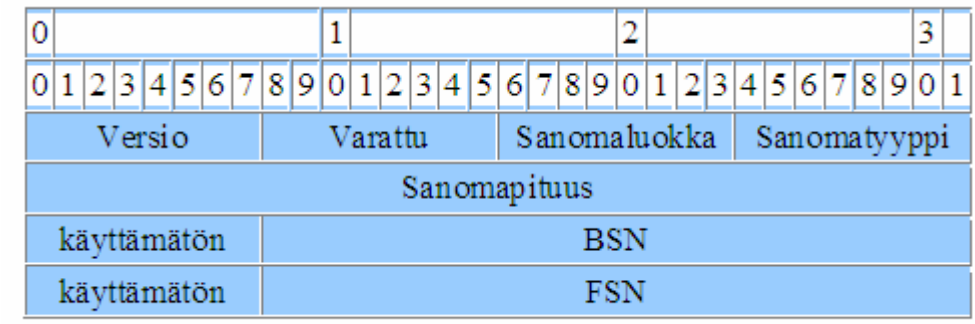
SCN merkinantosolmut voivat saada pääsyn tietokantoihin ja muihin laitteisiin IP-verkossa, alueella jossa ei käytetä SS7 merkinantolinkkejä. Samalla tavalla kuin IP-puhelimien sovellukset saavat pääsyn SS7 palveluihin. [8]

Toimitusmekanismi, jota tässä kuvataan, sallii kokonaisten MTP3 sanomien käsittelyn sekä verkonhallintakyvyt kahden minkä tahansa SS7 solmun välillä kommunikoiden IP-verkon yli. SS7 solmua varustettuna IP yhteydellä kutsutaan IP merkinantopisteeksi (IP Signaling Point, IPSP). [8]

Toimitusmekanismi tukee:

- MTP3:n protokollan saumaton toiminta IP-verkkoyhteyden yli.
- MTP2 / MTP3 rajapinnan raja.
- raportointi kaikista muutoksista.

M2PA-protokollaotsikon rakenne:



Versio

Tämä kenttä sisältää M2PA:n version. Tuettu versio on M2PA 1.0. [8]

Sanomaluokka

Ainoa sallittu arvo M2PA sanomille on 11. [8]

Sanomatyyppi

Seuraava lista pitää sisällään sanomien tyypit määritetyille sanomille:

1 Käyttäjädata

2 Yhteyden tila

Sanomapituus

Sanoman pituus määrittelee sanoman pituuden oktetteina. [8]

BSN

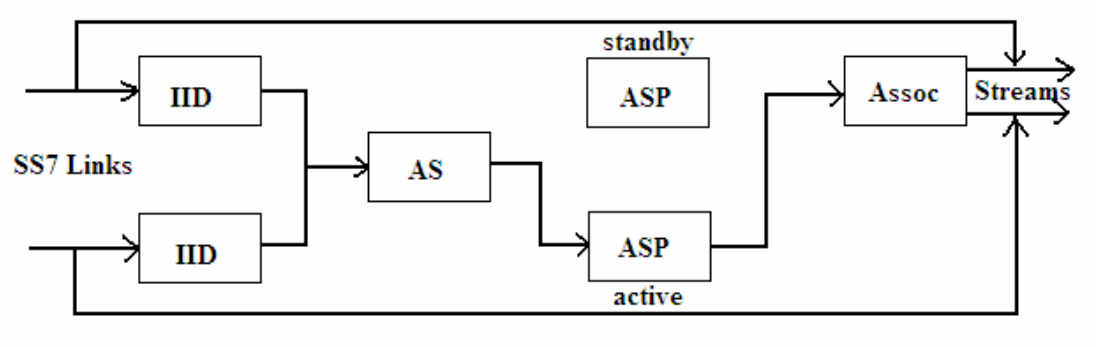
Backward Sequence Number – tämä on viimeisen vastaanotetun sanoman FSN. [8]

FSN

Forward Sequence Number - lähetetyn käyttäjädatasanoman M2PA:n sarjanumero. [8]

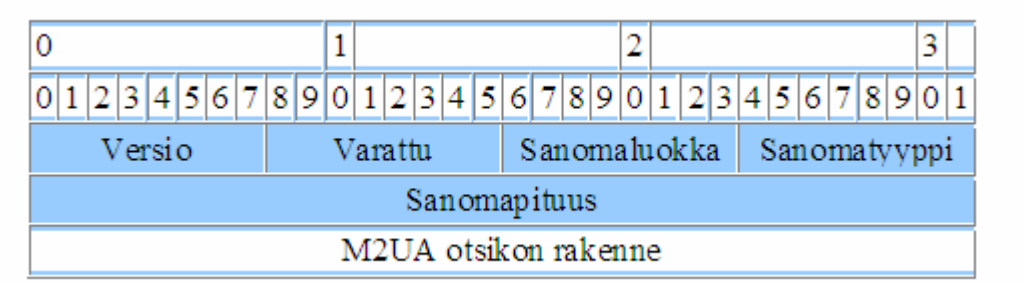
3.3 MTP2 User Adaption Layer (M2UA)

M2UA on tarkoitettu SS7 MTP2-käyttäjän merkinantosanomien takaisinkuljetukseen käyttäen SCTP:tä. Tämä protokolla on tarkoitettu SG:n ja MGC:n väliseen kommunikointiin. SG vastaanottaa SS7 merkinantoa standardin SS7 rajapinnan yli käyttäen SS7 MTP:tä välittääkseen kuljetuksen. M2UA pitää sisällään myös IID:n, (interface indentifier) jota käytetään kun ASP (application server process) lähettää UP (User Part) sanoman SG:lle, ilmoittaakseen, että on nyt aktiivinen ja voi aloittaa liikenteen käsittelyn siihen liittyvälle AS:lle (application server). M2UA toimii myös liikenteen hoitajana SS7-verkon ja MGC:n tai ASP:n välillä. Tehdäkseen tämän, M2UA:n on tiedettävä kaikkien ASPeiden ja MGCeiden tilat ja pystyttävä hoitamaan näiden kokonaisuuksien liikenteen virta. [9][15]



Esimerkiksi jos SG näyttää, että kaksi ASP:tä on vapaana, M2UA on vastuussa päätöksestä mikä ASP on aktiivinen ja mikä on valmiustilassa. Ei ole vaadittu mitään toimintoa ASP:n informointiin siitä mitkä ovat aktiivisia ja mitkä valmiustilassa M2UA yksinkertaisesti päättää mille ASP:lle reitittää liikenteen. [15]

M2UA-otsikon rakenne:



Versio

Versio-kenttä pitää sisällään M2UA version. Tuettu versio on 1.0. [9]

Varattu

Tämä kenttä pitäisi olla asetettu nollaan. [9]

Sanomaluokka

Sanomaluokan arvo voi olla mikä tahansa seuraavista:

0 Management Messages (MGMT)
3 ASP State Maintenance Messages (ASPSM)
4 ASP Traffic Maintenance Messages (ASPTM)
5 MTP2 User Adaption Messages (MAUP)

Sanomatyyppi

Hallinto:

0 Error (ERR)
1 Notify (NTFY)

ASP tilan ylläpito:

1 ASP Up (UP)
2 ASP Down (DOWN)
4 ASP Up Ack (UP ACK)
5 ASP Down Ack (DOWN ACK)

ASP liikenteen ylläpito:

1 ASP Active (ACTIVE)
2 ASP Inactive (INACTIVE)
3 ASP Active Ack (ACTIVE ACK)
4 ASP Inactive Ack (INACTIVE ACK)

MTP2 käyttäjän tila:

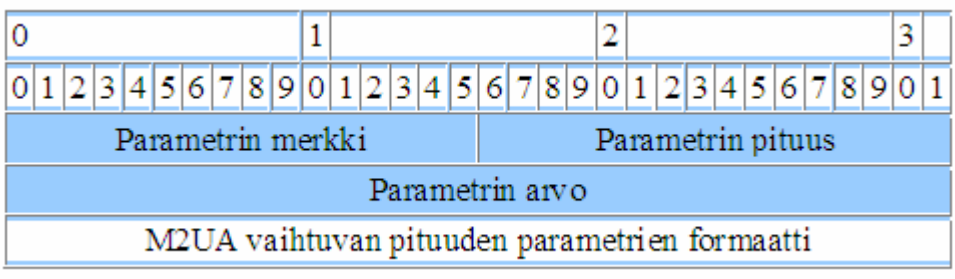
1 Data
2 Establish Request
3 Establish Confirm
4 Release Request
5 Release Confirm
6 Release Indication
7 State Request
8 State Confirm
9 State Indication
10 Data Retrieval Request
11 Data Retrieval Confirm
12 Data Retrieval Indication
13 Data Retrieval Complete Indication
14 Congestion Indication
15 TTC Data

Sanomopituus

Sanoman pituus määrittelee pituuden okteitteina, mukaan lukien otsikon. [9]

Vaihtelevien parametrien formaatti:

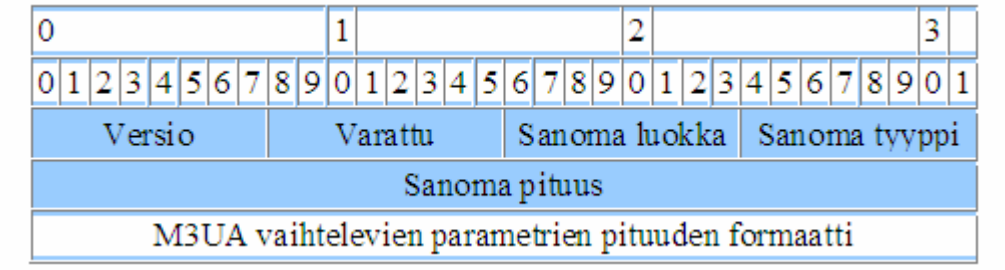
M2UA sanoma koostuu otsikosta, jota seuraa 0 tai vaihteleva määrä parametreja. [9]



3.4 MTP3 User Adaptation Layer (M3UA)

M3UA tukee ISUP, SCCP ja TUP (Telephone User Part) sanomien siirtoa IP:n yli, käyttäen SCTP:n palveluita. Protokollaa käytetään SG:n ja MGC:n väliseen kommunikointiin tai kun muodostetaan yhteyttä SG:ltä IP-pohjaiseen sovellukseen. M3UA:ta käytetään myös MTP3:n palveluiden laajentamiseen, mutta tarkoitus ei ole kuitenkaan käyttää M3UA:ta MTP3:n siirtoon. SG vastaanottaa SS7 merkinantoa standardin SS7 rajapinnan yli käyttäen MTP:tä välittääkseen siirron. Protokolla koostuu otsikkoa seuraavista parametreista. [10][15]

M3UA-otsikon rakenne:



Sanomaluokka

Sanoman luokan arvo voi olla mikä tahansa seuraavista:

0 Management (MGMT)
1 Transfer Messages
2 SS7 Signalling Network Management (SSNM)
3 ASP State Maintenance (ASPSM)
4 ASP Traffic Maintenance (ASPTM)
9 Routing Key Management (RKM)

Sanomatyyppi

Hallinto:

0 Error (ERR)
1 Notify (NTFY)

Siirto:

1 Payload Data (DATA)

SS7 SNM (Signaling Network Management):

1 Destination Unavailable (DUNA)
2 Destination Available (DAVA)
3 Destination State Audit (DAUD)
4 SS7 Network Congestion State (SCON)
5 Destination User Part Unavailable (DUPU)
6 Destination Restricted (DRST)

ASP:n tilan hallinta:

1 ASP Up (UP)
2 ASP Down (DOWN)
3 Heartbeat (BEAT)
4 ASP Up Ack (UP ACK)
5 ASP Down Ack (DOWN ACK)
6 Heartbeat Ack (BEAT ACK)

ASP:n liikenteen hallinta:

1 ASP Active (ACTIVE)
2 ASP Inactive (INACTIVE)
3 ASP Active Ack (ACTIVE ACK)
4 ASP Inactive Ack (INACTIVE ACK)

Reitityshallinto:

1 Registration Request (REG REQ)
2 Registration Response (REG RSP)
3 Deregistration Request (DEREG REQ)
4 Deregistration Response (DEREG RSP)

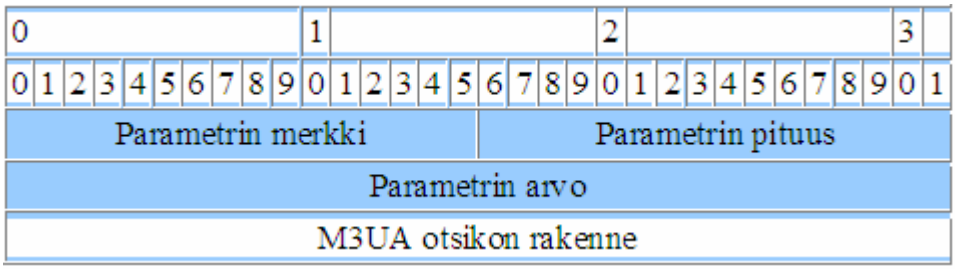
Sanomapituus

Määrittelee sanoman pituuden okteitteina mukaan lukien otsikon. [10]

Parametrien vaihteleva pituus

M3UA sanoma koostuu otsikosta, jota seuraa 0 tai useampi eri mittainen parametri, jotka on määritelty sanoman tyypissä. [10]

Parametrien formaatti seuraavasti:



Parametrin merkki

Parametrin merkki tarkoittaa parametrin tyyppiä:

0	Reserved
1	Network Appearance
2	Protocol Data 1
3	Protocol Data 2
4	Info String
5	Affected Destinations
6	Routing Context
7	Diagnostic Information
8	Heartbeat Data
9	User/Cause
10	Reason
11	Traffic Mode Type
12	Error Code
13	Status Type/ID
14	Congestion Indications
15	Concerned Destination
16	Routing Key
17	Registration Result
18	De-registration Result
19	Local_Routing Key Identifier
20	Destination Point Code
21	Service Indicators
22	Subsystem Numbers
23	Originating Point Code List
24	Circuit Range
25	Registration Results
26	De-registration Results

Parametrin pituus

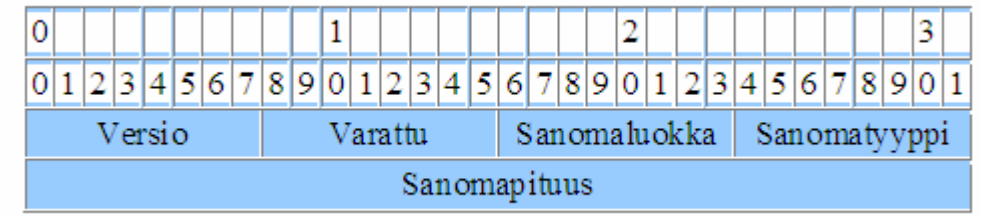
Käsittää parametrin koon bitteinä. Parametrin pituus pitää sisällään parametrin merkin, parametrin pituuden sekä parametrin arvo-kentät. [10]

3.5 SCCP User Adaptation (SUA)

Tällä hetkellä on menossa jatkuva SCN-verkkojen ja IP-verkkojen integraatio. Verkon palvelun tuottajat suunnittelevat kaikki IP arkkitehtuurit, jotka tukevat SS7:ä ja SS7:n kaltaisia merkinantoprotokollia. IP mahdollistaa tehokkaan tavan tiedon siirtoon ja operaattoreille laajentaa verkkojaan ja rakentaa uusia palveluita. [12]

Signalling Connection Control Part User Adaptation Layer (SUA) protokolla tarkentaa SCCP-käyttäjäsanomien (MAP & CAP yli TCAP, RANAP, jne) sekä uuden kolmannen sukupolven sanomien siirron IP:n yli kahden merkinantopisteen välillä. Protokollaa käytetään kuljettamaan SS7 SCCP:tä tai ISUP:a IP-verkkoon sekä kuljettamaan sanomat ASP:lle, joka hoitaa yhteydet AS:n ja muiden elementtien välillä verkossa. Tämä protokolla voi myös tukea SCCP-sanomien siirtoa kahden päätepisteen välillä, jotka ovat kokonaan IP-verkon sisällä. [12]

Otsikko näyttää seuraavalta:



Versio

Protokollan versio. [12]

Sanomaluokka

Seuraavat sanomaluokat ovat mahdollisia:

0 Management (MGMT) Message
2 SS7 Signalling Network Management (SSNM) Messages
3 ASP State Maintenance (ASPSM) Messages
4 ASP Traffic Maintenance (ASPTM) Messages
7 Connectionless Messages
8 Connection-Oriented Messages
9 Routing Key Management (RKM) Messages

Sanomatyyppi

Seuraavat sanomatyypit ovat olemassa:

SUA Management Messages

0	Error (ERR)
1	Notify (NTFY)
2 - 127	Reserved by the IETF
128- 255	Reserved for IETF-Defined Message Class Extensions

SS7 Signaling Network Management (SSNM) Messages

0	Reserved
1	Destination Unavailable (DUNA)
2	Destination Available (DAVA)
3	Destination State Audit (DAUD)
4	SS7 Network Congestion (SCON)
5	Destination User Part Unavailable (DUPU)
6	SCCP Management (SCMG)
7 – 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

Application Server Process Maintenance (ASPM) Messages

0	Reserved
1	ASP Up (UP)
2	ASP Down (DOWN)
3	Heartbeat (BEAT)
4	ASP Up Ack (UP ACK)
5	ASP Down Ack (Down ACK)
6	Heartbeat Ack (BEAT ACK)
7 - 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

ASP Traffic Maintenance (ASPTM) Messages

0	Reserved
1	ASP Active (ACTIVE)
2	ASP Inactive (INACTIVE)
3	ASP Active Ack (ACTIVE ACK)
4	ASP Inactive Ack (INACTIVE ACK)
5 - 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

Connectionless Messages

0	Reserved
1	Connectionless Data Transfer (CLDT)
2	Connectionless Data Response (CLDR)
3 - 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

Connection-Oriented Messages

0	Reserved
1	Connection Request (CORE)
2	Connection Acknowledge (COAK)
3	Connection Refused (COREF)
4	Release Request (RELRE)
5	Release Complete (RELCO)
6	Reset Confirm (RESCO)
7	Reset Request (RESRE)
8	Connection Oriented Data Transfer (CODT)
9	Connection Oriented Data Acknowledge (CODA)
10	Connection Oriented Error (COERR)
11	Inactivity Test (COIT)
12 - 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

Sanomapituus

Sanoman pituus määrittelee sanoman pituuden oktetteina, mukaan lukien otsikon. [12]

3.6 ISDN User Adaptation (IUA)

Arkkitehtuuri joka on määritelty SCN:lle merkinannon siirtämiseen IP:n yli, käyttää monia protokollia mukaan lukien IP kuljetus-protokolla, merkinannon kuljetus-protokollan sekä sovitusmoduulin tukemaan palveluita. IUA määrittelee sovitus moduulin joka on sopiva siirtämään ISDN Q.921-User Adaptation Layer-viestejä. [7]

IUA kerros toteuttaa seuraavat toiminnot:

- Liittäminen

  IUA kerros ylläpitää liitäntää rajapinnan tunnisteesta fyysiselle rajapinnalle merkinannon yhdyskäytävällä. Fyysinen rajapinta voi olla T1-linja, E1-linja jne. ja voi pitää sisällään TDM aikavälin. Lisäksi SG on kykenevä tunnistamaan merkinantokanavan. IUA kerros ylläpitää molempien SG:n ja MGC:n TEI:n ja SAP:n tilannetta. [7]
- ASP:n tila

  IUA kerros SG:llä ylläpitää ASP:n tilaa jota se tukee. ASP:n tila muuttuu vastaanotettujen viestien tai vastaanotetuista viittauksista paikalliselta SCTP:ltä. [7]

- SCTP:n virtojen hallinta

  SCTP sallii käyttäjälle määritellyn virtojen avattavan määrän. IUA:n vastuulla on huolehtia tarpeellisesta virtojen hallinnosta. Rajapinnan tunniste on IUA sanomaotsikko. [7]

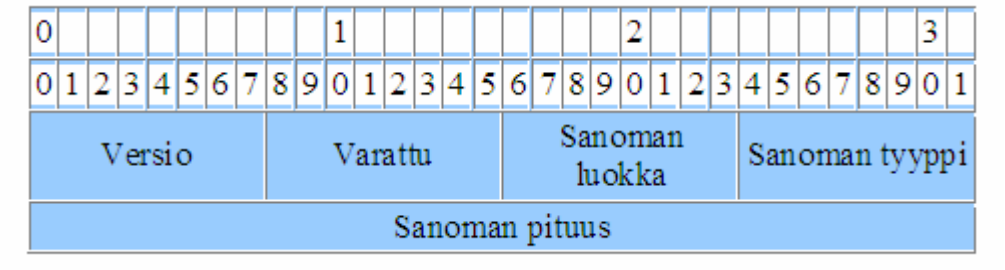
- Sisäinen verkonhallinta

  Mikäli parhaillaan aktiivinen ASP muuttuu ACTIVE tilasta pois, IUA kerros SG:llä antaa merkin paikalliselle kerroshallinnolle (Local Management) ettei IUA-käyttäjä ole saatavilla. Kerroshallinto voisi ohjeistaa Q.921:sta toimenpiteisiin jos se näyttää tarpeelliselta. [7]

- Ruuhkan hoito

  Jos IUA kerros ruuhkautuu se saattaa lopettaa yhteydenpidon SCTP:hen. [7]

Otsikko



Versio

Pitää sisällään IUA:n sovellutuskerroksen version. [7]

Sanoman luokat ja tyypit

Seuraava lista pitää sisällään voimassa olevat sanomaluokat:

0	Management (MGMT) Message
3	ASP State Maintenance (ASPSM) Messages
4	ASP Traffic Maintenance (ASPTM) Messages
5	Q.921/Q.931 Boundary Primitives Transport (QPTM) Messages
9-127	Reserved by the IETF
128-225	Reserved for IETF-Defined Message Class extensions

Seuraava lista pitää sisällään sanomien nimet määritetyille sanomille.

Q.921/Q.931 Boundary Primitives Transport (QPTM) Messages

0	Reserved
1	Data Request Message
2	Data Indication Message
3	Unit Data Request Message
4	Unit Data Indication Message
5	Establish Request
6	Establish Confirm
7	Establish Indication
8	Release Request
9	Release Confirm
10	Release Indication
11-127	Reserved by the IETF
128-225	Reserved for IETF-Defined QPTM extensions

Application Server Process State Maintenance (ASPSM) messages

0	Reserved
1	ASP Up (UP)
2	ASP Down (DOWN)
3	Heartbeat (BEAT)
4	ASP Up Ack (UP ACK)
5	ASP Down Ack (DOWN ACK)
6	Heatbeat Ack (BEAT ACK)
7-127	Reserved by the IETF
128-255	Reserved for IETF-Defined ASPSM extensions

Application Server Process Traffic Maintenance (ASPTM) messages

0	Reserved
1	ASP Active (ACTIVE)
2	ASP Inactive (INACTIVE)
3	ASP Active Ack (ACTIVE ACK)
4	ASP Inactive Ack (INACTIVE ACK)
5-127	Reserved by the IETF
128-255	Reserved for IETF-Defined ASPTM extensions

Management (MGMT) Messages

0	Error (ERR)
1	Notify (NTFY)
2	TEI Status Request
3	TEI Status Confirm
4	TEI Status Indication
5-127	Reserved by the IETF
128-255	Reserved for IETF-Defined MGMT extensions

Viestin pituus

Määrittää sanoman pituuden oktetteina mukaan lukien myös otsikon. [7]

3.7 V5 User Adaptation (V5UA)

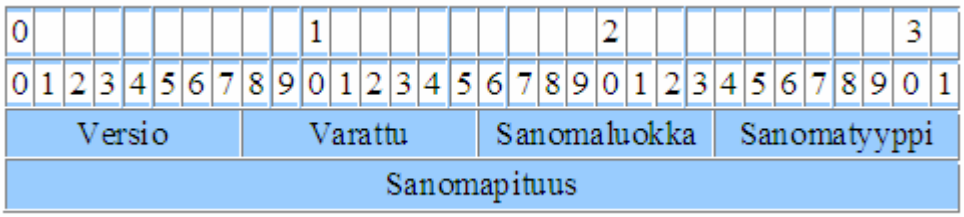
SCN:n (Switched Circuit Network) protokollan merkinannon kuljetusta tarvitaan V5.2 SG:ltä MGC:lle. Koska V5.2 kerros 2 ja erityisesti kerros 3 eroaa Q.921:n ja Q.931:n sovituskerroksesta, IUA standardin pitää olla laajennettu täyttämään V5.2:n tarpeet. [13]

V5.2 on ETSI rajapinta (lähdeviite ETS 300 347-1), määritelty LE:n (Local Exchange) ja AN:n (Access Network) välille tarjotakseen pääsyn seuraaville tyypeille:

- Analoginen puhelin
- ISDN perusnopeus
- Toinen analoginen tai digitaalinen pääsy jatkuville yhteyksille ilman merkinantoinformaatiota.

IUAP tarvitsee laajentaa V5UA:ksi, jotta se tukisi V5.2 takaisintoimitusta. V5UA kierrättää joitakin IUA primitiivejä Q.921/Q.931 rajalta: DL-DATA ja DL-UNIT DATA. DL-DATAa käytetään molempien V5 kerros 3 ja V5 ISDN kerros 3 sanomien siirtoon. DL-UNIT-DATAa käytetään ainoastaan V5 ISDN sanomiin. [13]

Otsikko



Versio

Pitää sisällään V5UA:n sovituskerroksen version. Tuettu versio on 1. [13]

Sanomaluokat ja tyypit

Seuraava lista pitää sisällään voimassa olevat sanomaluokat. [13]

Sanomaluokka:

0	Management (MGMT) Message
3	ASP State Maintenance (ASPSM) Messages
4	ASP Traffic Maintenance (ASPTM) Messages
9	V5 Boundary Primitives Transport Messages (V5PTM)

Sanomien nimet määritetyille sanomille ovat seuraavat:

Management (MGMT) Messages

0	Error (ERR)
1	Notify (NTFY)
2	TEI Status Request
3	TEI Status Confirm
4	TEI Status Indication
5-127	Reserved by the IETF
128-255	Reserved for IETF-Defined MGMT extensions

Application Server Process State Maintenance (ASPSM) messages

0	Reserved
1	ASP Up (UP)
2	ASP Down (DOWN)
3	Heartbeat (BEAT)
4	ASP Up Ack (UP ACK)
5	ASP Down Ack (DOWN ACK)
6	Heatbeat Ack (BEAT ACK)
7-127	Reserved by the IETF
128-255	Reserved for IETF-Defined ASPSM extensions

Application Server Process Traffic Maintenance (ASPTM) messages

0	Reserved
1	ASP Active (ACTIVE)
2	ASP Inactive (INACTIVE)
3	ASP Active Ack (ACTIVE ACK)
4	ASP Inactive Ack (INACTIVE ACK)
5-127	Reserved by the IETF
128-255	Reserved for IETF-Defined ASPTM extensions

V5 Boundary Primitives Transport Messages (V5PTM)

1	Data Request Message	(MGC -> SG)
2	Data Indication Message	(SG -> MGC)
3	Unit Data Request Message	(MGC -> SG)
4	Unit Data Indication Message	(SG -> MGC)
5	Establish Request	(MGC -> SG)
6	Establish Confirm	(SG -> MGC)
7	Establish Indication	(SG -> MGC)
8	Release Request	(MGC -> SG)
9	Release Confirm	(SG -> MGC)
10	Release Indication	(SG -> MGC)
11	Link Status Start Reporting	(MGC -> SG)
12	Link Status Stop Reporting	(MGC -> SG)
13	Link Status Indication	(SG -> MGC)
14	Sa-Bit Set Request	(MGC -> SG)
15	Sa-Bit Set Confirm	(SG -> MGC)
16	Sa-Bit Status Request	(MGC -> SG)
17	Sa-Bit Status Indication	(SG -> MGC)
18	Error Indication	(SG -> MGC)

4 CESOPSN

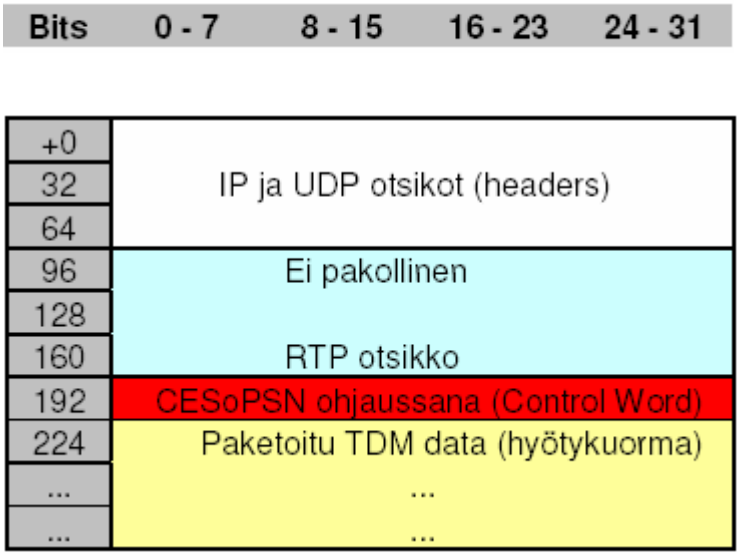
European Conference of Postal and Telecommunications Administrations (CEPT) aluperin lanseerasi E-carrier järjestelmän, jonka myöhemmin ITU-T (International Telecommunication Union Standardization Sector) otti haltuunsa. E1 on maailmanlaajuinen (pois lukien USA ja Japani) järjestelmä, jolla digitaalisen puhelinverkon yhdessä fyysisessä siirtotiessä voidaan kuljettaa samaan aikaan useita eri puheluja. [14]

E1:ssä on 32 eri aikaväliä, joista 30 on varattu puheen siirtoon. Yksi aikaväli on merkinannolle ja yksi on varattu kehyslukitukselle. Vastaanottaja tietää tämän perusteella milloin uusi kehys alkaa. Aikavälit siirtävät 8 bittiä dataa omalla vuorollaan, joita on 8000 sekunnissa. Linkki toimii yleensä kahdella erillisellä kaapelilla, joiden tiedonsiirtonopeus on 2.048Mbit/s. [4]

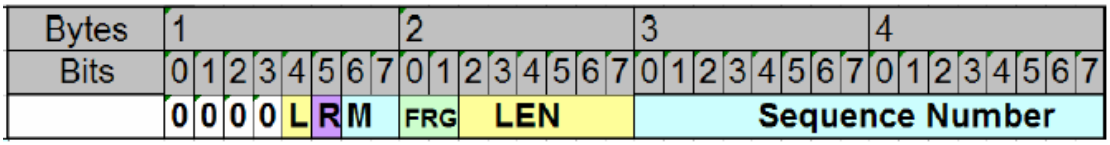
CES tai CESoPSN (Circuit Emulation Services over Packet Switching Network) mahdollistaa piirikytkentäisen verkon palveluiden siirtämisen Internetin yli. Se siirtää aikajaettua signaalia luomalla eräänlaisen virtuaalisen siirtotien pakettiverkon yli. Tätä emuloitua siirtotietä IP:n yli kutsutaan nimeltä pseudowire (PW). Tämä palvelu täyttää harvoin samat edellytykset kuin oikea E1-linja, verkkojen viiveistä yms. johtuen. [4]

CESoPSN:n kehityksessä se määriteltiin täyttämään nämä edellytykset:

Jokainen paketti sisältää saman verran "korvaavaa" TDM-dataa (Time Division Multiplexing), tämä helpottaa kadonneitten pakettien käsittelyä. Eli jokainen paketti sisältää yhtä pitkän ajan jakson aikajaettua signaalia. Aika tiedon kulkemiseen päästä päähän tulee olla kiinteä (end-to-end delay). Pakettien muodostamiseen kuuluva aika: a) Viive pakettien muodostamiseen kuuluu olla 1-5ms b) Järjestelmä joka sallii muuttaa tätä viivettä, täytyy tukea viiveen muuttamista sellaisessa skaalassa, joka on 125 mikrosekunnin monikerta. Jos siirretään esim. kanavamerkinantoa (CAS), tämä data siirretään omissa paketeissaan erillään muusta TDM-datasta. [4][14]



CESoPSN-paketti käytettäessä UDP:tä.



CESoPSN Control Word.

CESoPSN ohjaussanomat ensimmäiset 4 bittiä ovat nollia. L asetetaan, jos kytkennässä (circuit) havaitaan jotain virheitä. M–kenttä toimii L–kentän jatkeena (toimivat 3-bittisenä koodina). R–kenttä asetetaan, jos toiminto, joka suorittaa TDM-datan pakkauksen CESoPSN-paketteihin, kadottaa peräkkäisten pakettien numerojärjestyksen. FRG-kenttää käytetään todella harvoin. Sillä määritellään, esim. jos osa datasta kuuluu lähettää PW:n toisessa päässä eri porttiin. LEN– kentässä on paketin koko, jos se on alle 64 tavua, niin se asetetaan nollaksi. Viimeisessä kentässä on paketin järjestysnumero, joka helpottaa havaitsemaan kadonneita paketteja. [4] [14]

L	M	TULKINTA
0	00	Normaali tilanne, ei virheitä.
0	10	Tilanne jossa vastaanottava osapuoli havaitsee TDM-virrassa bittikuvioita, jotka kertovat katkoksista lähetyksessä (Remote Defect Indication). Tämän jälkeen se yrittää katkoksista huolimatta asettaa ulosmenevän portin (trunk) virhettä vastaavaan tilaan.
0	11	Varattu CESoPSN:n signalointi-paketeille.
1	00	TDM-data on epäkelpoa. Yrittää asettaa ulosmenevän portin AIS-tilaan (Alarm Indication Signal).

CESoPSN-ohjaussanoman L- ja M-kenttien selitykset.

Yhteyden laatu ei kokeilujen perusteella ole aina ollut kovinkaan vakaata, johtuen esim. pakettiverkkojen viiveistä jne. Viivettä on yritetty eliminoida asettamalla puskurit (jitter buffer). Vastaanottaja ottaa vastaan CESoPSN-paketin ja siirtää sen puskuriinsa, josta se tietyn ajan välein purkaa niitä TDM-dataksi. Synkronisaation pitäminen on myös hankalaa. Mahdollista on käyttää molemmissa päissä samaa ulkopuolista kelloa, mikä on usein mahdotonta pitkien välimatkojen takia. Yleisesti CESoPSN yrittää pitää kelloa yllä pakettien järjestysnumeroiden ja niiden aikaleimojen avulla. [4][14]

5 IPSEC

IPSEC on Internetin IETF-järjestön kehittämä perusstandardi. IPSEC-protokollat mahdollistavat TCP/IP-yhteyksien kryptografisen suojauksen verkkokerroksella ja suojaavat yhteydet muun muassa yleisessä Internet-verkossa. [5]

5.1 Tietoturvatavoitteet

IPSEC on joukko yleiskäytännöllisiä protokollia, joilla suojataan TCP/IP-liikennettä. Käytännössä suojaus tapahtuu niillä HOST-koneiden välillä eikä HOST-konetta käyttävien käyttäjien välillä. [1]

IPSEC-protokollien suojaustavoitteet ovat:

- Suojata liikennettä luotettujen tietokoneiden välillä väärennyksiltä tai salakuuntelulta. Luotettavilta Host-koneilta tuleva ja sinne päätyvä liikenne pitää suojata. Kahden Host-koneen välinen liikenne voi kulkea muiden Host-koneiden kautta ja hyökkääjä voi päästä käsiksi liikenteeseen. Hyökkääjä ei pysty vahingoittamaan sanomia väärentämällä tai salakuuntelemalla niitä. [1]

- Suojata käytössä olevia Internet-viestintäohjelmistoja. Verkossa on käytössä lukuisia Internet-ohjelmistoja, kuten sähköposti, Web-yhteydet, FTP, etäpääteyhteydet, jotka kaikki perustuvat TCP/IP-protokolliin. Tämä liikenne pitää suojata, kun se kulkee käyttäjien välillä. Jotta käytössä olevia TCP/IP ohjelmistoja ei tarvitsisi kustannussyistä muuttaa tai korvata, lisätään niihin IPSEC-tuki. [1]

- Epäluotettava verkko on jo rakennettu ja kustannukset ovat merkittävä tekijä. Vähemmän luotettava verkko on jo käytössä ja se siirtää liikennettä luotettujen pisteiden välillä. Useimmiten tämä verkko on yleinen Internet. Monessa tapauksessa on liian kallista rakentaa omaa verkkoa. [1]

- Suojauksen tulee olla automaattista suojaa tarvitsevien Host-koneiden välillä. Monet organisaatiot eivät halua, että yksittäinen käyttäjä tekee päätöksiä pitäisikö joku liikenne suojata ja joku ei. Järjestelmän tulisi sen sijaan olla automaattisesti turvallinen niiden pisteiden välillä, jotka suojausta tarvitsevat. [1]

5.2 IPSEC-tekniikan perusominaisuudet

Verkko- ja linkkitason kryptotekniikalla ja IPSEC-protokollilla on määrätyt erot.

- Tietoturvan pitää olla riippumatonta ja transparenttia oleviin ISP-palveluihin nähden. Tärkeimpiä syitä IPSEC-protokollien kehittämiseen on ollut, että voidaan käyttää jo olevia ISP (Internet Service Provider)-palveluja liikenteen välittämiseen tietokoneiden ja käyttäjien välillä. Internet-verkon arkkitehtuuri ei kuitenkaan anna mitään mahdollisuuksia sälyttää esimerkiksi eheysvaatimuksia ISP-operaattoreiden harteille. IPSEC-teknologialla voidaan suojautua niitä uhkia vastaan, joihin ISP:t eivät pysty. Esimerkiksi linkkitason salaus ei ole transparenttia ISP-palveluille. Linkkitason suojausta voidaan käyttää vain kiinteiden pisteiden välillä. [1][6]

- Linkkitasolla käytetty kryptotekniikka jättää paketteihin enemmän selväkielistä tekstiä. Verkkotason kryptauksessa IP-pakettiin jää enemmän selväkielitekstiä. Vain se voidaan salata, mitä ei tarvita reitittämiseen. Paketin internetosoite on selvätekstistä, jotta ISP voi reitittää paketit määränpäähän, vaikka koko sanoman sisältö onkin salattu. [1][6]

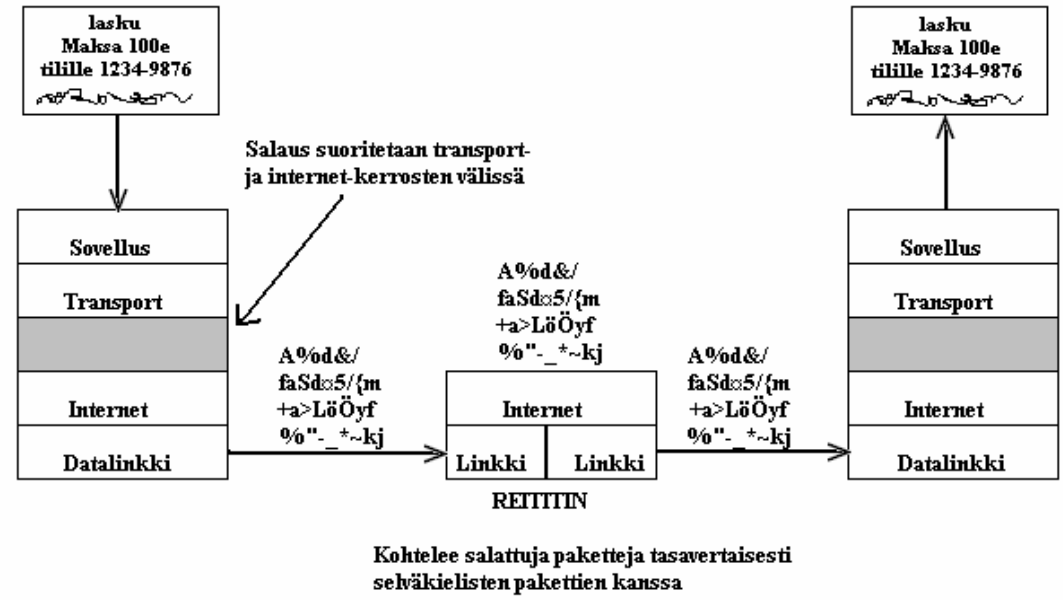
- Toimipistesalaus mahdollistaa myös toimipisteautentikoinnin. Verkkotason tietoturva voi erottaa toisistaan liikenteen sallittujen ja muiden toimipisteiden välillä, mutta se ei pysty erottamaan luotettavasti yksittäisten käyttäjien liikennettä sallitussa työpisteessä. Tämä voidaan hyväksyä monessa tapauksessa. Käyttäjätason autentikointi hoidetaan muilla menetelmillä, kuten salasanoilla, niin kauan kunnes tunnistusta tapahtuu sallitussa verkossa.

Tästä on syntynyt uusi virtuaaliverkkojen markkina (VPN, virtual private network), missä maantieteellisesti kaukanakin toisistaan olevia toimipisteitä voidaan liittää turvallisesti toisiinsa. VPN:ssä käytetään yleisen turvattoman verkon (yleensä) Internet ominaisuuksia organisaation oman suljetun verkon toteuttamiseksi. VPN:n pisteestä toiseen siirtyvä liikenne on suojattu ulkopuolisilta. VPN-sovelluksissa sisäpiiriin kuuluvien käyttäjien liikenteen erottaminen toisistaan ei yleensä ole ongelma. [1][6]

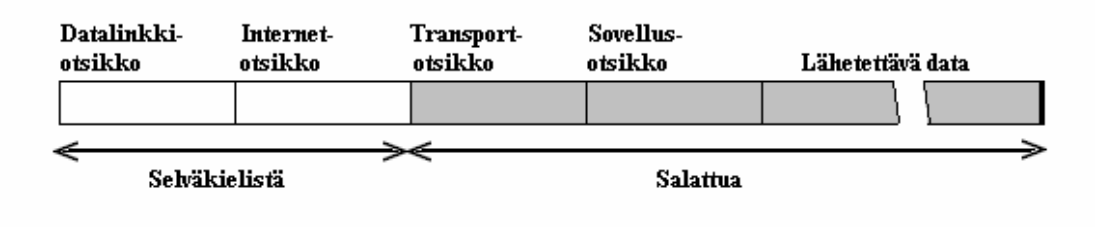
Avainten hallintaa ei ole ratkaistu yksikäsitteisesti. IPSEC-avainten hallintaan on olemassa useita ratkaisuja. Vaikka tähän on myös Internet-standardeja, laite- ja ohjelmistotoimittajilla on myös omia ratkaisuja, mikä hidastaa IPSEC-teknologian nopeaa leviämistä. [1]

5.3 IPSEC – IP tietoturvaprotokolla

IPSEC on laajassa käytössä olevien IP-verkkoprotokollien laajennus, millä estetään IP-pakettien urkkiminen ja muuntaminen. IPSEC on syntynyt osana käytössä olevan IPv6-protokollan kehitystä. IPSEC-protokolla voidaan sovittaa myös IPv4 protokolliin. Verkkotason IPSEC-suojaus ei vaikuta sovellusohjelmiin tai sovellusprotokolliin ja IPSEC-paketteja voivat käsitellä jo käytössä olevat reitittimet ja reitittävät-Host-koneet. [1]



IPSEC-suojaus on transparenttista Internet-sovelluksille ja –reitittimille IPSEC-suojaus tapahtuu IP-reititysinformaation ”yläpuolella” ja sovellusdatan ”alapuolella”. Reitittimet eivät huomioi ylimääräisiä IPSEC-otsikoita, eivätkä sovellukset näe IPSEC-kryptopalveluja. [1]



IPSEC-salauksen paketin perusformaatti

IPSEC salaa ja sinetöi kuljetus- ja sovellusdatan siirron aikana. Myös Internet otsikon eheys suojataan. Koska Internet-otsikko on selväkielistä, IP-reitittimet voivat reitittää salattuja IPSEC-sanomia vastaanottavaan Host-koneeseen saakka. [1]

IPSEC on suunniteltu IP-pakettien luottamuksellisuutta sekä väärennysten havaitsemista varten. IPSEC määrittelee kaksi optionaalista pakettiotsikkoa, kummallekin suojaustavalle (turvapalvelulle) oman. Otsikot sisältävät numeroarvon, mitä kutsutaan SPI-parametriksi (SPI, security parameter index). Host-kone käyttää SPI-parametria kryptoavainten ja niiden käytön tunnistamiseen. IP-paketti voi sisältää yhden tai molemmat otsikot riippuen tarvittavasta turvapalvelusta. Yleensä implementoidaan molemmat. [1]

IPSEC-otsikot ovat:

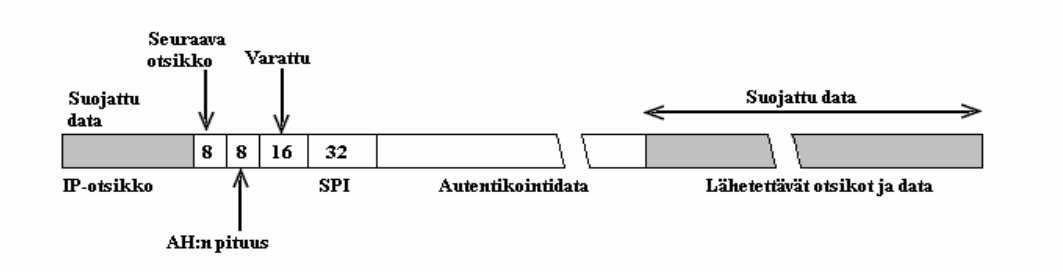
- Autentikointiotsikko (Authentication Header, AH). AH sisältää eheyden tarkistusinformaatiota, millä voidaan tarkistaa onko paketin sisältöä väärennetty tai muutettu matkalla läpi epäluotettavan verkkoyhteyden. AH-otsikko sisältää tätä varten kryptografisen tarkistussumman (checksum). Tarkistussumma tuottaa salaista avaininformaatiota, joten ulkopuolinen murtautuja ei pysty laskemaan toista tarkistussummaa, mikä osoittaisi sisällön aitouden. [6]

- Koteloitu salattu data (Encapsulating Security Payload, ESP). ESP salaa paketin loppuosan datasisällön, joten sisältöön ei päästä käsiksi matkalla. ESP-otsikon formaatti vaihtelee sen mukaan, mitä salausalgoritmia käytetään. Kaikissa tapauksissa käytettävä salausavain valitaan parametrin SPI avulla. [6]

Kummankin IPSEC-suojaukseen pyrkivän host-koneen tulee muodostaa aluksi turvayhteys (security associaton) toinen toiseensa. Turvayhteys määrittelee, mitä ja miten IPSEC-suojausta käytetään, eli mitä turvapalvelua milloinkin käytetään, miten salaus ja/tai autentikointi suoritetaan, ja mitä avaimia pitää käyttää. Turvayhteys muodostetaan kyseessä olevan IP-paketin vastaanottajan otsikon ja pakettiotsikon SPI-parametrin avulla. [6]

5.4 IPSEC-autentikointi

IPSEC-protokollan IP-paketin AH-otsikko sisältää paketin sisällöstä lasketun kryptografisen tarkistussumman. AH sijoitetaan IP-otsikon ja minkä tahansa sitä seuraavan pakettisisällön väliseen pakettiin. Pakettien datasisältöön ei tarvitse tehdä mitään muutoksia. Suojaus on kokonaan AH-otsikossa. [1]



kuva 6.18

IPSEC-protokollan AH-otsikon muoto ja sisältö

Kuvassa 6.18 on AH-otsikon muoto ja sisältö. AH:n muoto on hyvin yksinkertainen. Ensimmäinen merkki identifioi seuraavan protokollaotsikon tyypin ja paikan ja AH voidaan jopa ylittää autentikoimatta sitä. SPI kertoo vastaanottajalle, mikä turvayhteys koskee tätä otsikkoa. Otsikon loppuosa muodostuu 32 bitin merkeistä, mikä sisältää mainitun kryptografisen tarkistussumman. Tarkistussumman tai hash-funktion

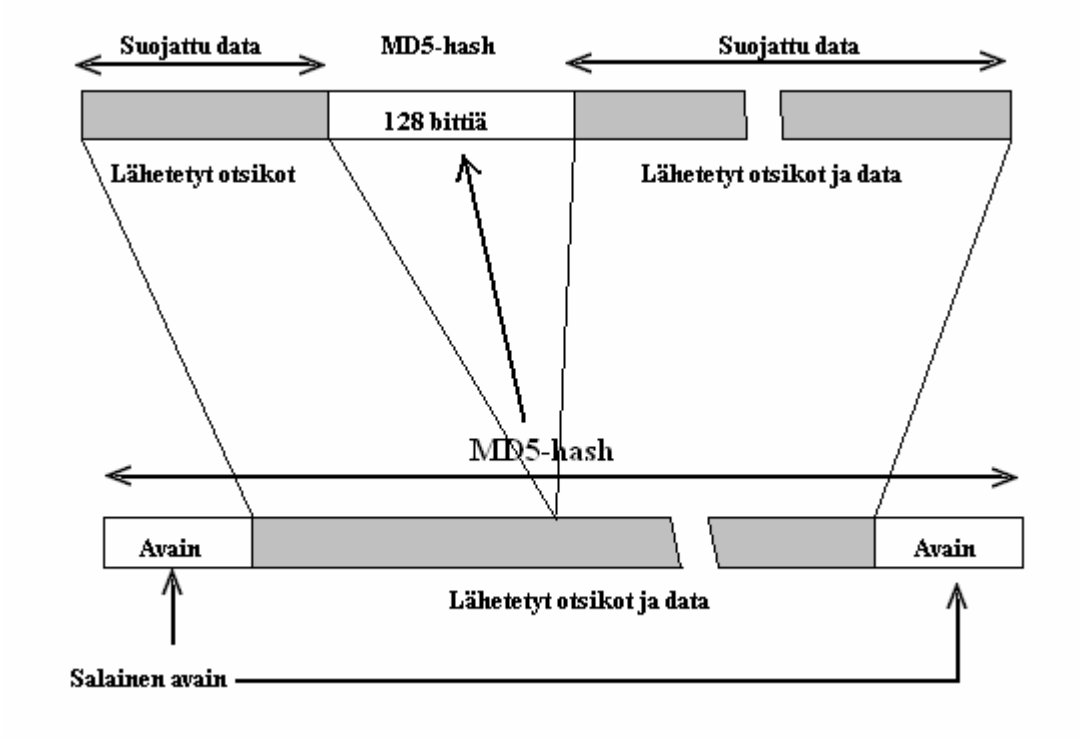
yksityiskohtainen muoto ja sisältö riippuu siitä, mitä algoritmia tällä turvayhteydellä käytetään (SHA-1, MD5, DES, CBC). [1]

Kryptografinen tarkistussumma määrätään paketin IP-otsikosta yhdistettynä AH:ta seuraavilla otsikoilla. Sisällyttämällä IP-otsikko tarkistuslaskentaan, AH voi havaita kaikki paketin osoiteinformaatioon kohdistuneet muutokset tai yritykset ohittaa itse AH. [1]

Vastaanottava host-kone suorittaa vastaavat laskennat ja todentaa tarkistussumman. Kaikkien kenttien arvot, jotka eivät vastaa summaa, asetetaan nollaksi. Tarkistussumman laskentaan käytetään SPI-parametriin yhdistettyä avainta. Jos tarkistussumman tulos ei vastaa AH-otsikossa vastaanotettua arvoa, paketti hylätään. [1]

IPSEC-autentikoinnin hash-funktion oletusarvona on avainnettu MD5 (salainen avain ja 128-bittinen tiiviste), jonka tulee sisältyä kaikkiin IPSEC implementaatioihin. Protokolla jättää salaisen avaimen pituuden avoimeksi. Kaksi host-konetta voi liikennöidä keskenään, jos ne sopivat avaimen pituudesta, sisällöstä ja bittien järjestyksestä. [1]

Autentikointiprosessi



Kuva 6.19

Avainnetulla MD5-tiivisteellä varustettu IPSEC-autentikointi

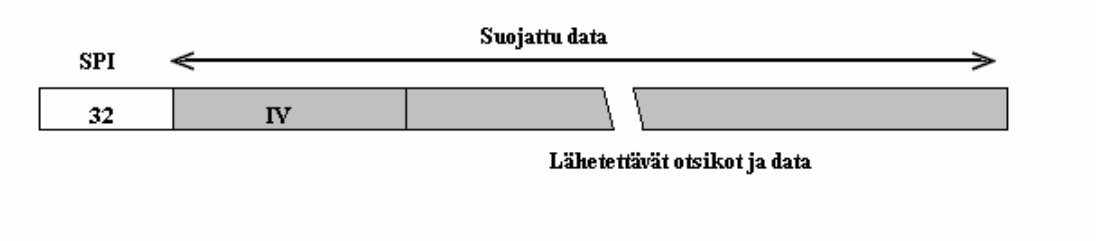
Kuvassa 6.19 on esitetty IPSEC-autentikoinnin yleinen periaate. Periaate on sama kuin muussakin normaalissa hash-funktiota käyttävässä autentikoinnissa sillä erotuksella, että hash-funktio laskee tiivisteen salatusta datasta (keyed hash). Hyökkääjä ei pysty toistamaan hash-laskentaa, koska hänen pitää ensiksi purkaa data, josta tiiviste määrätään. [1]

AH alkaa 64 bitin otsikolla, joka identifioi sitä seuraavan otsikon, määrittelee AH:n pituuden 32 bitin merkkeinä ja identifioi turvayhteyden paketin autentikointia varten. Autentikoinnin datakenttä sisältää vaihtuvan määrän 32 bitin merkkejä. Tyypillisesti se sisältää suojatusta datasta lasketun avainnetun hash-arvon. Huomattakoon, että normaalisti avoimessa Internet-ympäristössä tiivistefunktiot ovat julkisia algoritmeja, jotka sisällytetään salausalgoritmeihin sellaisenaan. Laajasti hyödynnettävissä Internetissä (sähköposti, Web, e-kauppa,…) hyökkäykset kuitenkin ovat toisen tyyppisiä kuin IP-verkkojen tapauksissa, missä yksinkertaiset selväkielisanomista lasketut hash-tiivisteet eivät riitä. [1]

SPI-parametriin liittyvä salainen avain liitetään suojattuun dataan kahdesti. Analyysit ovat osoittaneet, että tämä konsepti kestää hyökkäyksiä enemmän kuin yhden avaimen käyttö. Tämän jälkeen lasketaan MD5-tiiviste kombinoidusta datasta (kuva 6.19). Syntyvä 128 bitin tiiviste sijoitetaan paketin AH-otsikkoon. Vastaanottaja todentaa tiivisteen konstruoimalla oman hash-arvon käyttämällä samaa salaista avainta, mikä oli liitetty suojattavan datan alkuun ja loppuun. Jos vastaanotettu sanoma on aito, AH-otsikossa vastaanotettu ja perillä laskettu tiiviste ovat samat ja päinvastoin. [1]

5.5 IPSEC-salaus

Myös IPSEC ESP määrittelee uuden otsikon IP-pakettiin. ESP-prosessointi salaa siirrettävän paketin. ESP-otsikko sisältää vastaanottavan host-koneen turvayhteyden SPI-parametrin (kuva 6.20). Koteloidun datan formaatti riippuu pelkästään tällä turvayhteydellä käytettävästä kryptotekniikasta. [1]



kuva 6.20
IPSEC ESP-otsikon muoto ja sisältö

Normaaliolosuhteissa ESP sijaitsee AH-otsikon ”sisällä”. Paketin generoiva host-kone kryptaa datan käyttämällä turvayhteydellä valittua algoritmia ja avainta, ja asettaa SPI-parametrin ESP-otsikkoon. Autentikointi suoritetaan tämän jälkeen paketin salatusta sisällöstä. [1]

Vastaanotossa prosessoidaan ensiksi AH, jos sitä on. Jos salattua dataa on peukaloitu matkalla, AH-prosessointi havaitsee tämän ja paketti hylätään. Tämän jälkeen host-kone ottaa käyttöönsä ESP-otsikkoon liitetyn avaimen ja kryptoalgoritmin ja purkaa salauksen. [1]

Oletuksena DES-algoritmin CBC-moodi

Kaikkien IPSEC-toteutusten tulee sisältää oletuksena DESin CBC-moodi. Moodi käyttää 56 bitin salaista avainta. Jotta CBC-moodi toimisi oikein, DES tarvitsee 56 bitin avaimen lisäksi aloitusvektorin IV. Data salataan peräkkäin 64 bitin lohkoina. Algoritmi ei voi prosessoida vajavaisia lohkoja, joten data tulee täyttää 64 bitin lohkoiksi. [1] [6]

Vastaanottava kone käyttää ESP-otsikon SPI-parametria selvittääkseen, miten koteloitu data pitää purkaa ja miten tunnistetaan käytettävä avain. Jos ESP-otsikkoa ei ole suojattu AH-menetelmällä siirron aikana, väärennetyllä avaimella toteutetun datasisällön salaamisen tai siirron aikana tapahtuneen datasisällön muuttumisen tunnistamiseen voidaan käyttää vain kahta suhteellisen epäluotettavaa menetelmää. [1]

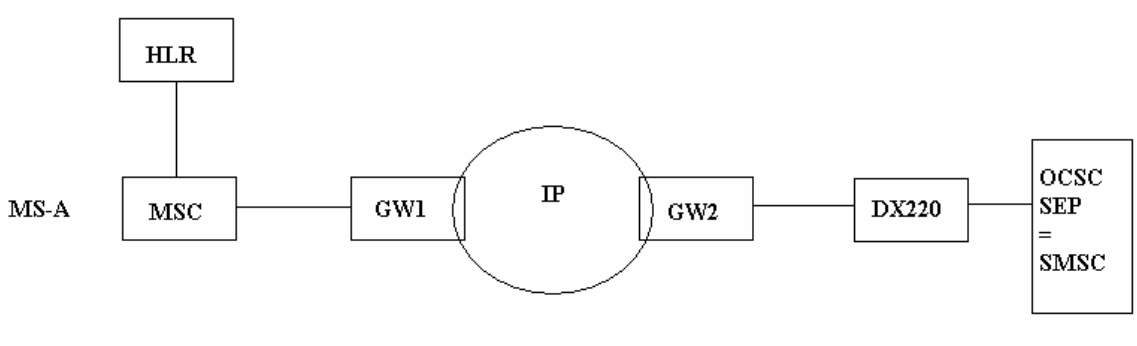
Ensiksi, DES/CBC-prosessi voi todentaa, että koteloitu data esiintyy 64 bitin lohkoina ja hylätä datan, jos näin ei ole. Toiseksi DES/CBC-prosessi voi todentaa, että hyötydatan tyypillä on laillinen arvo. Todellinen eheyden tarkistus pitää suorittaa AH-otsikon avulla, joskin joissakin tapauksissa tämä voidaan todeta myös korkeamman tason protokollilla. [1]

6 RATKAISUESIMERKKEJÄ

6.1 SIGTRAN

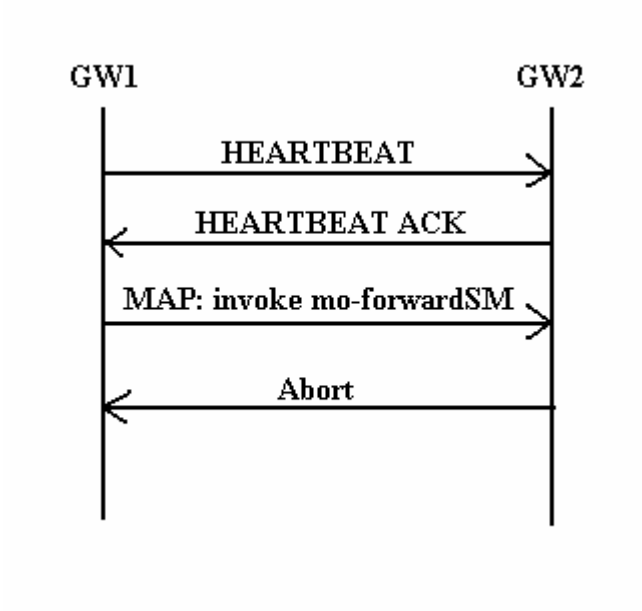
Esittelen seuraavassa kaksi esimerkkiä kappaleessa 2 kuvattujen tarpeiden toteuttamiseksi. Sigtranin viestikeskusyhteyden mahdollistajana sekä CESoPSN kuljettamaan TDM-pohjaista dataa yli IP-verkon nopeulla 2 Mbit/s.

SMS FORWARD



Tarkoituksena on lähettää tekstiviesti MS-A:sta MS-B:hen. SMSC:nä toimii OCSC:hen tehty logiikka. Ollaan lähettämässä viestiä MS-B:lle, joten tarvitsee selvittää missä tilaaja on. SMSC selvittää tilaajan sijainnin lähettämällä kyselyn HLR:lle. HLR palauttaa tiedon SMSC:lle ja jos tilaajan sijainti selvisi, lähetys on nyt mahdollinen. IP-verkon yli voidaan mennä kolmella eri tavalla tässä tilanteessa. Käyttäen SCTP-tasoa, jolloin käytetään GT-analyysia vastapään ”osoitteen” selvityksessä, MTP3-taso ja MTP2-tasoa, jolloin osoitamme vastapäätä PC:lla (Point Code). Tässä tapauksessa käytämme SCTP-tasoa eli GT-analyysia.

Seuraavassa kuvassa on kuvattu GW1:n ja GW2:n välistä liikennettä tekstiviestin lähetyksessä.



GW1 lähettää GW2:lle HEARTBEATin (heartbeat request), jolla se saa tiedon onko vastapää tavoitettavissa. GW2 kuittaa GW1:lle HEARTBEAT ACKilla (heartbeat acknowledgement). Seuraavaksi MSC lähettää MAP-sanoman INVOKE MO-FORWARDSM SMSC:lle, mutta koska logiikka ei toimi oikein se palauttaa sanoman ABORT.

Liitteessä esimerkki konfiguraatiosta Gateway 1:lle (MSC:n pää), joka vääntää yhden piirikytkentäisen 64kbps-merkinantokanavan SCTP:n päälle IP:n yli siirrettäväksi. Toisessa reitittimessä tehdään GT-analyysi ja verkkomuunnos (NA1 → NA0) kuvitetulla SMSC:n numerolle ja heitetään viesti eteenpäin toiselle reitittimelle IP:n yli. Vastaavasti toisesssa reitittimessä tehdään GT-analyysi ja verkkomuunnos (NA0 → NA1) samalle SMSC:n numerolle ja viesti laitetaan eteenpäin piirikytkentäiseen merkinantokanavaan. (Sama konfiguraatio Gateway 2:lle (lankakeskuksen pää), mutta eri IP –ja GT-osoitteilla).

6.2 CESoPSN

Liitteenä esimerkki konfiguraatiosta T-Marc-kytkimille, jossa siirrettiin Nokian InSiten Abis-rajapinta IP:n yli. Aikavälit 1-2 olivat varattuja TCH-kanaville, 30 TRX-signaloinnille ja 31 OMU-signaloinnille.

6.3 IPSEC

Esimerkki IPSEC-tunnelin luomisesta.

Vaiheet:

1. enable
2. configure terminal
3. crypto isakmp policy
4. encryption
5. hash
6. authentication
7. exit
8. crypto isakmp key
9. crypto ipsec transform-set
10. crypto map
11. set peer
12. set transform-set
13. match address
14. exit
15. interface
16. ip address
17. crypto map
18. exit
19. access-list

Vaihe 1

Router> enable

-tällä komennolla päästään reitittimeen “kiinni” kun vaadittava salasana on annettu.

Vaihe 2

Router# configure terminal

-pääsy konfiguraatiotilaan.

Vaihe 3

Router(config)# crypto isakmp policy 1

-määrittelee IKE:n (Internet Key Exchange) sekä päästään ISAKMP konfiguraatiotilaan.

Vaihe 4

Router(config-isakmp)# encryption 3des

-määritellään salausalgoritmi.

Vaihe 5

Router(config-isakmp)# hash md5

-hash tarkoittaa tiedon tiivistämistä pienempään tilaan sitä varten, että alkuperäistä tietoa voidaan vertailla vertailemalla niiden tiivisteitä ja md5 on tiivisteen algoritmi.

Vaihe 6

Router(config-isakmp)# authentication pre-share

-määritellään todennustapa.

Vaihe 7

Router(config-isakmp)# exit

-palataan takaisin yleiseen konfiguraatiotilaan.

Vaihe 8

Router(config)# crypto isakmp key cisco 123 address 10.2.1.2

-konfiguroidaan todennusavain.

Vaihe 9

Router(config)# crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac

-muunnetaan joukoksi sallittuja turvallisuusprotokollia sekä algoritmeja.

Vaihe 10

Router(config)# crypto map to_vpn 10 ipsec-isakmp

-konfiguroidaan IKE:n laajennettu todennus reitittimelle.

Vaihe 11

Router(config-crypto-map)# set peer 10.2.1.2

-määritellään IP-osoite “sisääntulolle”.

Vaihe 12

Router(config-crypto-map)# set transform-set to_vpn

-asetetaan käyttämään vpn-protokollaa.

Vaihe 13

Router(config-crypto-map)# match address 101

-tehdään lista sallituista osoitteista.

Vaihe 14

Router(config-crypto-map)# exit

-palataan takaisin yleiseen konfiguraatiotilaan.

Vaihe 15

Router(config)# interface Fastethernet 0/0

-konfiguroidaan rajapinta Fa 0/0.

Vaihe 16

Router(config-if)# ip address 10.1.3.1 255.255.255.0-annetaan rajapinnalle IP-osoite sekä aliverkon peite.

Vaihe 17

Router(config-if)# crypto map to_vpn

-asetetaan salaus rajapinnalle.

Vaihe 18

Router(config-if)# exit

-palataan takaisin yleiseen konfiguraatiotilaan.

Vaihe 19

Router(config)# access-list 101 permit ip 10.1.3.0 0.0.0.255 10.2.1.0 0.0.0.255

Router(config)# access-list 101 permit ip 10.2.1.0 0.0.0.255 10.1.3.0 0.0.0.255

-luodaan lista sallituille osoitteille.

Seuraavaksi konfiguroidaan CS7 linkki tunnelin “yläpuolelle”.

Vaiheet:

1. cs7 local-peer
2. local-ip
3. exit
4. cs7 linkset
5. link

Vaihe 1

Router(config)# cs7 local-peer 5000

-otetaan käyttöön cs7 ja määritellään sen tila.

Vaihe 2

Router(config-cs7-ip)# local-ip 10.1.3.1

-annetaan linkille IP-osoite.

Vaihe 3

Router(config-cs7-ip)# exit

-palataan takaisin yleiseen konfiguraatiotilaan.

Vaihe 4

Router(config)# cs7 linkset dasher 3.3.3

-määritellään, että linkki toimii rinnakkaisena.

Vaihe 5

Router(config-cs7-ls)# link 0 sctp 10.2.1.2 5000 5000

-konfiguroidaan SS7 linkki.

7 YHTEENVETO

Edellä mainittuja yhteyksiä tullaan luomaan tulevaisuudessa ammattikorkeakoulun tarpeisiin, mutta omaksi epäonnekseni en päässyt testaamaan konfiguraatioita käytännössä. Asia jota työssäni käsittelen, on vaikea ymmärtää ainoastaan teoriapohjalta. Työssäni tutkin kahta esimerkkiä millä yhteydet voidaan toteuttaa tarpeiden välillä sekä yhteyksien tietoturvaa. Ajatuksena miten reitittimet ja kytkimet konfiguroidaan on selvä, sekä mitä tarvitsee ottaa huomioon kun käytetään eri ”tasoja” kuten MTP2, MTP3 jne. siirrettäessä pakettaja IP-verkon yli. Myös MSC:n, lankakeskuksen sekä SMSC:n roolit pakettien siirrossa selvisivät työn aikana. Selvitin myös työssäni miten luodaan IPSEC-tunneli reitittimien välille tietoturvaa suojaamaan.

Itselleni entuudestaan melko tuntemattomat standardit kuten SIGTRAN ja CESoPSN tulivat tutuksi teorian osalta ja vieläkin tutummaksi käsittelemäni IPSEC.

Suosittelen esittämieni ratkaisujen käyttöönottoa liitettäessä asiakasverkkoja NGN-laboratorion verkkoon. Katson, että ratkaisujen pohjalta on luotavissa yhtenäinen konsepti entistä laaajemman yhteistyön ja liiketoiminnan käynnistämiseksi.

LÄHTEET

[1] Kerttula, E. Tietoverkkojen Tietoturva. 1p. Helsinki: Edita, 1998. 510 s.

[2] Keskustelut lehtori Juha Aromaan kanssa – SAMK 2009

[3] Wikipedia – SIGTRAN. [verkkodokumentti]. [viitattu 23.01.2009]. Saatavissa: http://en.wikipedia.org/wiki/SIGTRAN

[4] Antti Peurakoski – Opinnäytetyö: hajautettu testausympäristö, SAMK 2008.

[5] Wikipedia – IPSEC. [verkkodokumentti]. [viitattu 17.12.2008]. Saatavissa: http://fi.wikipedia.org/wiki/IPsec

[6] IETF – IPSEC. [verkkodokumentti]. [viitattu 18.12.2008]. Saatavissa: http://www.ietf.org/rfc/rfc2401.txt

[7] SIGTRAN – IUA. [verkkodokumentti]. [viitattu 07.01.2009]. Saatavissa: ftp://ftp.rfc-editor.org/in-notes/rfc3057.txt

[8] SIGTRAN – M2PA. [verkkodokumentti]. [viitattu 08.01.2009]. Saatavissa: http://www.protocols.com/pbook/sigtran.htm#M2PA

[9] SIGTRAN – M2UA. [verkkodokumentti]. [viitattu 08.01.2009]. Saatavissa: http://www.protocols.com/pbook/sigtran.htm#m2ua

[10] SIGTRAN – M3UA. [verkkodokumentti]. [viitattu 10.01.2009]. Saatavissa: http://www.protocols.com/pbook/sigtran.htm#m3ua

[11] SIGTRAN – SCTP. [verkkodokumentti]. [viitattu 11.01.2009]. Saatavissa: http://www.protocols.com/pbook/sigtran.htm#sctp

[12] SIGTRAN – SUA. [verkkodokumentti]. [viitattu 12.01.2009]. Saatavissa: ftp://ftp.rfc-editor.org/in-notes/rfc3868.txt

[13] SIGTRAN – V5UA. [verkkodokumentti]. [viitattu 15.01.2009]. Saatavissa: ftp://ftp.rfc-editor.org/in-notes/rfc3807.txt

[14] CESoPSN [verkkodokumentti]. [viitattu 20.01.2009]. Saatavissa: http://tools.ietf.org/html/draft-ietf-pwe3-cesopsn-07

[15] Russel, T. SIGNALING SYSTEM #7. 5p. New York: McGraw-Hill, 2006. 702 s.

LIITTEET

Liite Sigtran-konfiguraatiosta Gateway 1 reitittimelle:

```
Current configuration : 1554 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SS7oIPGW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$LWws$JrMXzMRwQscpms1.RjBLR1
!
no aaa new-model
no network-clock-participate slot 1
no network-clock-participate wic 0
!
ip cef
no ip domain lookup
cs7 multi-instance
cs7 instance 0 variant ITU
cs7 instance 0 network-name MSC
cs7 instance 0 network-indicator reserved
cs7 instance 0 point-code 0.93.6
cs7 instance 1 variant ITU
cs7 instance 1 network-name SS7oIP
cs7 instance 1 point-code 0.153.0
```

```
!
cs7 log gtt size 5000
cs7 log gtt verbose
multilink bundle-name authenticated
!
controller E1 0/0
 description CPM link between Cisco ITP and MSC on National 1 network and ET
69
!
controller E1 0/1
 channel-group 0 timeslots 1
 description MSC National1 ET69
!
interface FastEthernet0/0
 ip address 192.168.4.151 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/1:0
 no ip address
 encapsulation mtp2
!
cs7 local-peer 7000
 local-ip 192.168.4.151
!
cs7 instance 0 linkset MSC 0.112.4
 link 0 Serial0/1:0
!
```

```
cs7 instance 1 linkset SS7oIP 0.152.0
 link 0 sctp 192.168.4.152 7000 7000
!
cs7 instance 0 route-table
cs7 instance 1 route-table
!
ip http server
no ip http secure-server
!
logging history size 500
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password esimerkki
 login
!
end
```

GT-analyysi

```
!
cs7 instance 0 gtt application-group app-group0
 multiplicity share
 instance 1 pc 0.152.0 1 gt
!
cs7 instance 0 gtt selector labra tt 0 gti 4 np 1 nai 4
 gta 3582200  app-grp app-group0
!
cs7 instance 1 gtt application-group msc
 multiplicity share
 instance 0 pc 0.112.4 1 gt
!
```

```
cs7 instance 1 gtt selector ss7oip tt 0 gti 4 np 1 nai 4
 gta 3582384  app-grp msc
!
```

Seuraavasta konfiguraatiosta on selvennetty mitä Cisco ITP:hen on tällä hetkellä konfiguroitu.

```
SS7oIPGW#sh run
Building configuration...

Current configuration : 1606 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SS7oIPGW
!
boot-start-marker
boot system flash c2600-itpk9-mz.124-11.SW.bin
boot-end-marker
!
enable secret 5 $1$fbef$kZhg0sF6CUhdm8cUFtwKl0
!
no aaa new-model
no network-clock-participate slot 1
no network-clock-participate wic 0
!
ip cef
no ip domain lookup
cs7 variant ITU
cs7 network-name labraverkko
cs7 network-indicator reserved
```

```
cs7 point-code 0.93.6
!
cs7 prompt enhanced
cs7 log gtt size 5000
multilink bundle-name authenticated
!
controller E1 0/0
 clock source line primary
 channel-group 0 timeslots 1
 description PCM link between Cisco ITP and DX220 PSTN on National 1 network and ET 59
!
controller E1 0/1
!
interface Loopback0
 ip address 10.10.40.1 255.255.255.0
!
interface FastEthernet0/0
 description link to PSTN
 ip address 192.168.1.154 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0:0
 no ip address
 encapsulation mtp2
!
interface FastEthernet0/1
 ip address 193.166.148.152 255.255.255.240
 duplex auto
 speed auto
!
cs7 local-peer 7000
 local-ip 10.10.40.1
```

```
!
cs7 linkset MSC 0.112.4
 link 0 Serial0/0:0
!
cs7 route-table system
!
ip route 0.0.0.0 0.0.0.0 193.166.148.158
!
ip http server
no ip http secure-server
!
logging history size 500
!
control-plane
!
banner motd ^C Tervetuloa C2651XM ITP-reitittimeen. Toivottavasti viihdyt vierai-
lullasi ja et hajoita mitaan. ^C
!
line con 0
 password ngnlabra
 login
line aux 0
line vty 0 4
 password ngnlabra
 login
!
end
```

SS7 variant ITU

-tässä ollaan määritelty mitä SS7 muunnosta reititin käyttää, muut vaihtoehdot: ansi, china, ttc.

cs7 point-code 0.93.6

-Jokaisella Ciscon ITP:llä täytyy olla uniikki Point Code.

cs7 network-indicator reserved

-verkon osoitin, cs7 [**instance** *instance-number*] **network-indicator {international |** national | reserved | spare}

international = kansainvälinen

national = kansallinen

reserved = varattu

spare = vara-

cs7 network-name labraverkko

-tässä määritellään verkon nimi signalointipisteelle. Nimi voi olla maksimissaan 19 merkkiä pitkä.

cs7 prompt enhanced

-näyttää tämänhetkisen linkkiyhteyden. Ei ole pakollinen, mutta ehkäisee väärien linkkiyhteyksien sammuttamista.

cs7 log gtt size 5000

-komento kirjoittaa GTT-virheet paikalliseen tai etäiseen kohteeseen. Tässä muistin laajuudeksi määritelty 5000. Kun muisti tulee täyteen se korvaa edellisen ja alkaa tekemään uutta.

clock source line primary

-määritelty, että tässä portissa kello otetaan ulkoisesta läheteestä eli sieltä mihin portti on liitetty.

E1 0/0

-PCM-linkki Cisco ITP:n ja DX 220 PSTN:n välillä kansallisessa verkossa 1 ja ET:ssä 59.

Interface 0/0

-linkki PSTN:nään

encapsulation mtp2

-käytetään olestusajastimena (timer) ITP-reitittimissä.

cs7 local-peer 7000

local-ip 10.10.40.1

-SCTP-yhteyksissä tämä on paikallinen päätepiste. Tarvitsee olla ainakin yksi IP-osoite tälle, mutta on myös mahdollista, että IP-osoitteita vaaditaan neljä, yhtä käytetään ja loput kolme ovat varalla.

cs7 linkset MSC 0.112.4

-useampi linkki yhdessä on linkkiryhmä (linkset). Jokainen linkki on määriteltävä kuuluvaksi johonkin linkkiryhmään. Tässä linkkiryhmälle on annettu nimeksi MSC ja Point Codeksi 0.112.4.

link 0 Serial0/0:0

-linkki on määritelty kyseessä olevaan porttiin.

cs7 route-table system

-cs7-reititystaulun nimeksi on määriteltävä system.

Gateway 1:n ja Gateway 2:n välinen liikenteen kaappaus liittyen tekstiviestin lähetykseen:

```
No.     Time        Source                Destination      Protocol
Info       14    33.948417   192.168.1.153          192.168.1.154
SCTP HEARTBEAT

Frame 14 (94 bytes on wire, 94 bytes captured)
    Arrival Time: Apr  9, 2008 14:07:38.966546000
    [Time delta from previous packet: 0.134876000 seconds]
    [Time since reference or first frame: 33.948417000 seconds]
    Frame Number: 14
    Packet Length: 94 bytes
    Capture Length: 94 bytes

    [Frame is marked: False]
    [Protocols in frame: eth:ip:sctp]
Ethernet II, Src: Cisco_fe:37:e0 (00:1a:6d:fe:37:e0), Dst:
Cisco_a9:26:80 (00:1a:e2:a9:26:80)
    Destination: Cisco_a9:26:80 (00:1a:e2:a9:26:80)
    Source: Cisco_fe:37:e0 (00:1a:6d:fe:37:e0)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.153 (192.168.1.153), Dst:
192.168.1.154 (192.168.1.154)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
        0000 00.. = Differentiated Services Codepoint: Default
(0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 80
    Identification: 0xd1ad (53677)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: SCTP (0x84)
    Header checksum: 0x64f8 [correct]
        [Good: True]
        [Bad : False]
    Source: 192.168.1.153 (192.168.1.153)
    Destination: 192.168.1.154 (192.168.1.154)
Stream Control Transmission Protocol, Src Port: 7000 (7000), Dst
Port: 7000 (7000)
    Source port: 7000
    Destination port: 7000
    Verification tag: 0xa37032d4
    Checksum: 0x7a8258ac [correct CRC32C]
    HEARTBEAT chunk (Information: 44 bytes)
        Chunk type: HEARTBEAT (4)
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x00
        Chunk length: 48
        Heartbeat info parameter (Information: 40 bytes)
```

```
            Parameter type: Heartbeat info (0x0001)
                0... .... .... .... = Bit: Stop processing of chunk
                .0.. .... .... .... = Bit: Do not report
            Parameter length: 44
            Heartbeat information:
01040000C0A8019A00000000000000000000000000000000...

No.     Time        Source           Destination           Protocol
Info
   15 33.950337   192.168.1.154       192.168.1.153         SCTP
HEARTBEAT_ACK

Frame 15 (94 bytes on wire, 94 bytes captured)
    Arrival Time: Apr  9, 2008 14:07:38.968466000
    [Time delta from previous packet: 0.001920000 seconds]
    [Time since reference or first frame: 33.950337000 seconds]
    Frame Number: 15
    Packet Length: 94 bytes
    Capture Length: 94 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:sctp]
Ethernet II, Src: Cisco_a9:26:80 (00:1a:e2:a9:26:80), Dst:
Cisco_fe:37:e0 (00:1a:6d:fe:37:e0)
    Destination: Cisco_fe:37:e0 (00:1a:6d:fe:37:e0)
    Source: Cisco_a9:26:80 (00:1a:e2:a9:26:80)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.154 (192.168.1.154), Dst:
192.168.1.153 (192.168.1.153)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
        0000 00.. = Differentiated Services Codepoint: Default
(0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 80
    Identification: 0x9e7d (40573)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: SCTP (0x84)
    Header checksum: 0x9828 [correct]
        [Good: True]
        [Bad : False]
    Source: 192.168.1.154 (192.168.1.154)
    Destination: 192.168.1.153 (192.168.1.153)
Stream Control Transmission Protocol, Src Port: 7000 (7000), Dst
Port: 7000 (7000)
    Source port: 7000
    Destination port: 7000
    Verification tag: 0x06e3b309
    Checksum: 0xfd86d35f [correct CRC32C]
    HEARTBEAT_ACK chunk (Information: 44 bytes)
        Chunk type: HEARTBEAT_ACK (5)
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x00
```

```
        Chunk length: 48
        Heartbeat info parameter (Information: 40 bytes)
            Parameter type: Heartbeat info (0x0001)
                0... .... .... .... = Bit: Stop processing of chunk
                .0.. .... .... .... = Bit: Do not report
            Parameter length: 44
            Heartbeat information:
01040000C0A8019A0000000000000000000000000000000000...


No.     Time        Source          Destination        Protocol Info
    19 40.875305   1224                 1232           GSM SMS  in-
voke mo-forwardSM

Frame 19 (194 bytes on wire, 194 bytes captured)
    Arrival Time: Apr  9, 2008 14:07:45.893434000
    [Time delta from previous packet: 0.874621000 seconds]
    [Time since reference or first frame: 40.875305000 seconds]
    Frame Number: 19
    Packet Length: 194 bytes
    Capture Length: 194 bytes
    [Frame is marked: False]
    [Protocols in frame:
eth:ip:sctp:m2pa:mtp3:sccp:tcap:gsm_map:gsm_sms]
Ethernet II, Src: Cisco_fe:37:e0 (00:1a:6d:fe:37:e0), Dst:
Cisco_a9:26:80 (00:1a:e2:a9:26:80)
    Destination: Cisco_a9:26:80 (00:1a:e2:a9:26:80)
    Source: Cisco_fe:37:e0 (00:1a:6d:fe:37:e0)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.153 (192.168.1.153), Dst:
192.168.1.154 (192.168.1.154)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
        0000 00.. = Differentiated Services Codepoint: Default
(0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 180
    Identification: 0xd1b1 (53681)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: SCTP (0x84)
    Header checksum: 0x6490 [correct]
        [Good: True]
        [Bad : False]
    Source: 192.168.1.153 (192.168.1.153)
    Destination: 192.168.1.154 (192.168.1.154)
Stream Control Transmission Protocol, Src Port: 7000 (7000), Dst
Port: 7000 (7000)
    Source port: 7000
    Destination port: 7000
    Verification tag: 0xa37032d4
    Checksum: 0x434df2ea [correct CRC32C]
    DATA chunk(ordered, complete segment, TSN: 115589898, SID: 1,
SSN: 4090, PPID: 5, payload length: 131 bytes)
```

```
        Chunk type: DATA (0)
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x03
        Chunk length: 147
        TSN: 115589898
        Stream Identifier: 0x0001
        Stream sequence number: 4090
        Payload protocol identifier: M2PA (5)
        Chunk padding: 00
MTP2 Peer Adaptation Layer
Message Transfer Part Level 3
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT


No.     Time        Source        Destination           Protocol
Info
     21 41.022038   1232            1224                  TCAP
UDT  Abort dtid(a3411013) [Malformed Packet]

Frame 21 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Apr  9, 2008 14:07:46.040167000
    [Time delta from previous packet: 0.128290000 seconds]
    [Time since reference or first frame: 41.022038000 seconds]
    Frame Number: 21
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:sctp:m2pa:mtp3:sccp:tcap]
Ethernet II, Src: Cisco_a9:26:80 (00:1a:e2:a9:26:80), Dst:
Cisco_fe:37:e0 (00:1a:6d:fe:37:e0)
    Destination: Cisco_fe:37:e0 (00:1a:6d:fe:37:e0)
    Source: Cisco_a9:26:80 (00:1a:e2:a9:26:80)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.154 (192.168.1.154), Dst:
192.168.1.153 (192.168.1.153)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN:
0x00)
        0000 00.. = Differentiated Services Codepoint: Default
(0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x9e83 (40579)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: SCTP (0x84)
    Header checksum: 0x97d6 [correct]
        [Good: True]
        [Bad : False]
    Source: 192.168.1.154 (192.168.1.154)
    Destination: 192.168.1.153 (192.168.1.153)
```

```
Stream Control Transmission Protocol, Src Port: 7000 (7000), Dst
Port: 7000 (7000)
    Source port: 7000
    Destination port: 7000
    Verification tag: 0x06e3b309
    Checksum: 0x6ffed729 [correct CRC32C]
    DATA chunk(ordered, complete segment, TSN: 2742043329, SID: 1,
SSN: 4070, PPID: 5, payload length: 106 bytes)
        Chunk type: DATA (0)
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x03
        Chunk length: 122
        TSN: 2742043329
        Stream Identifier: 0x0001
        Stream sequence number: 4070
        Payload protocol identifier: M2PA (5)
MTP2 Peer Adaptation Layer
Message Transfer Part Level 3
Signalling Connection Control Part
Transaction Capabilities Application Part
[Malformed Packet: TCAP]
```

CESoPSN konfiguraatio T-Marc-kytkimelle (Jpn):

```
! Current Configuration:
!
! T-Marc-254  Version 6.6.3
!
hostname T-Marc-Jpn
password 5633c9b8af6d089859afcbec42fdc03f8c407aaba9668218b433bd495991146
enable password 5633c9b8af6d089859afcbec42fdc03f8c407aaba9668218b433bd495
username esimerkki password 5633c9b8af6d089859afcbec42fdc03f8c407aaba96682
ip address 192.168.21.2 255.255.255.0
! Log Configuration:
log module default server 192.168.1.115 syslog-facility clockd1 trap notifications
!
! Time-server Configuration:
!
time-server summer-time recurring last sunday March 03:00:00 last sunday October
04:00:00 60
time-server ntp add 87.104.20.61
time-server ntp add 211.255.163.63
time-server ntp add 62.236.121.72
time-server ntp start 360 3
!
! Snmp-server Configuration:
!
snmp-server system-name T-Marc-O
!
! DNS Resolver Configuration:
! DOT1X Configuration:
!
! Protocol Configuration:
!
! VLAN Configuration:
!
!CFM Configuration
```

```
!
! Super-Vlan Configuration:
!
! Monitor session Configuration:
!
! IGMP and Multicast Configuration:
!
! ACL Configuration:
!
! QOS Configuration:
!
! Port Configuration:
!
interface 1/1/1
!
interface 1/2/1
!
interface 1/3/1
!
interface 1/3/2
!
interface 1/3/3
!
interface 1/3/4
!
interface 1/4/1
!
ip route  0.0.0.0/0 192.168.21.1
!
! Switch Monitoring Configuration:
!
! LAG Configuration:
!
interface ag01
```

```
!
interface ag02
!
interface ag03
!
interface ag04
!
interface ag05
!
interface ag06
!
interface ag07
!
! Response Time Reporter Configuration:
!
! MEF OAM Configuration
!
! CES Modules Configuration:
ces 1/2
! CES 1/2 Version:CES Module R03.02.01_D017-200
ces ip address 192.168.21.5/24
ces ip gateway 192.168.21.1
clock adaptive
port 1
 framing noncas
 description BTS
exit
port 2
exit
port 3
exit
port 4
exit
channel-group 1 port 1 timeslots 1-2,30-31
```

```
circuit 1 channel-group 1
config circuit 1
 protocol cesopsn
 maximum-jitter-expected 30
 samples-aggregation 32


 destination ip 192.168.1.150
 no shutdown
exit
apply configuration
exit
```

Esimerkki T-Marc (P):

```
T-Marc-P#show running-config
Building the configuration ...

! Current Configuration:
!
! T-Marc-254  Version 6.6.3
!
hostname T-Marc-P
password 7540bfdea40902b43eff5dbb7e642adbd451b90e2461b8d2242d59b73a7079
enable password 7540bfdea40902b43eff5dbb7e642adbd451b90e2461b8d2242d59b7
username labra password 7540bfdea40902b43eff5dbb7e642adbd451b90e2461b8
ip address 192.168.1.152 255.255.255.0
! Log Configuration:
log module default server 192.168.1.113 syslog-facility syslog trap notifications
!
! Time-server Configuration:
!
time-server summer-time recurring last sunday March 03:00:00 last sunday October
04:00:00 60
```

```
time-server ntp add 87.104.20.61
time-server ntp add 211.255.163.63
time-server ntp add 62.236.121.72
time-server ntp start 360 3
!
! Snmp-server Configuration:
!
snmp-server system-name T-Marc-P
!
! DNS Resolver Configuration:
!
! DOT1X Configuration:
!
! Protocol Configuration:
!
! VLAN Configuration:
!
!CFM Configuration
!
! Super-Vlan Configuration:
!
! Monitor session Configuration:
!
 monitor session tx source interface 1/4/1
 monitor session tx destination interface 1/3/4
 monitor session rx source interface 1/4/1
 monitor session rx destination interface 1/3/4
!
! IGMP and Multicast Configuration:
!
! ACL Configuration:
!
! QOS Configuration:
!
```

```
! Port Configuration:
!
interface 1/1/1
!
interface 1/2/1
!
interface 1/3/1
!
interface 1/3/2
!
interface 1/3/3
!
interface 1/3/4
!
interface 1/4/1
!
ip route  0.0.0.0/0 192.168.1.156
!
! Switch Monitoring Configuration:
!
! LAG Configuration:
!
interface ag01
!
interface ag02
!
interface ag03
!
interface ag04
!
interface ag05
!
interface ag06
!
```

```
interface ag07
!
! Response Time Reporter Configuration:
!
! MEF OAM Configuration
!
! CES Modules Configuration:
ces 1/2
! CES 1/2 Version:CES Module R03.02.01_D017-200
ces ip address 192.168.1.161/24
ces ip gateway 192.168.1.156
port 1
 framing noncas
 description BSC
exit
port 2
exit
port 3
exit
port 4
exit
channel-group 1 port 1 timeslots 1-2,30-31
circuit 1 channel-group 1
config circuit 1
 protocol cesopsn
 maximum-jitter-expected 30
 samples-aggregation 32
 destination ip 192.168.21.5
exit
apply configuration
exit
```