STUDI TENTANG VIRTUAL PRIVATE NETWORK SEBAGAI APLIKASI JARINGAN PINTAR DAN PENERAPANNYA DI INDONESIA

TUGAS AKHIR

Disusun oleh :

BOEDI PRATOTO

NRP. 2902201474

JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
S U R A B A Y A

1996

STUDI TENTANG VIRTUAL PRIVATE NETWORK SEBAGAI APLIKASI JARINGAN PINTAR DAN PENERAPANNYA DI INDONESIA

TUGAS AKHIR

Diajukan Guna Memenuhi Sebagian Persyaratan
Untuk Memperoleh Gelar Sarjana Teknik Elektro
Pada
Bidang Studi Teknik Telekomunikasi
Jurusan Teknik Elektro
Fakultas Teknologi Industri
Institut Teknologi Sepuluh Nopember
S u r a b a y a

Mengetahui / Menyetujui
Dosen Pembimbing

DR. Ir. MOCH. SALEHUDIN, M.Eng.Sc.
NIP. 130 532 026

S U R A B A Y A
AGUSTUS, 1996

ABSTRAK

Untuk memenuhi kebutuhan komunikasi yang meningkat, telah dikembangkan Virtual Private Network yang merupakan aplikasi dari Intelligent Network dengan pelayanan yang berdasarkan software yang menyerupai jaringan pribadi yang menggunakan fasilitas switching dan transmisi jaringan publik. Dengan VPN pelanggan melakukan hubungan baik nasional maupun internasional melalui jaringan PSTN biasa, namun seakan-akan menggunakan jaringan pribadi.

Pelanggan jasa ini dapat mendefinisikan format penomoran, mengatur profile grupnya, mengubah feature, melihat statistik trafik, sehingga pelanggan seakan memiliki kontrol penuh atas fasilitas komunikasinya dengan manipulasi routing dan database pada sistem IN.

Akses ke VPN dilakukan melalui jaringan PSTN dengan kode akses khusus. Kode akses internasional dilakukan melalui on-net switched dan off-net switched. Bila pelanggan internasional akan berhubungan dengan mitranya disediakan fasilitas on-net, off-net dan sub-net, dengan penomoran yang didesain oleh pelanggan. Tersedia juga berbagai feature untuk pelanggan grup VPN. Untuk menunjang suksesnya panggilan VPN, dua elemen penting adalah circuit dan format routing internasional, baik inbound maupun outbound.

Implementasi jaringan pribadi melalui VPN memerlukan biaya investasi yang sangat murah dibandingkan dengan jaringan pribadi yang menggunakan leased circuit.

KATA PENGANTAR

Dengan memanjatkan puji syukur ke hadirat ALLAH SWT, atas rahmat, kasih dan ijin-NYA sehingga kami dapat menyelesaikan Tugas Akhir ini, dengan judul :

STUDI TENTANG VIRTUAL PRIVATE NETWORK SEBAGAI APLIKASI JARINGAN PINTAR DAN PENERAPANNYA DI INDONESIA

Tugas Akhir ini disusun guna memenuhi persyaratan untuk menyelesaikan program sarjana pada Jurusan Teknik Elektro, Fakultas Teknologi Industri, Institut Teknologi Sepuluh Nopember, Surabaya.

Akhirnya semoga apa yang tersurat dan tersirat dalam Tugas Akhir ini bermanfaat dan dapat diterima sebagai sumbangan pikiran bagi masyarakat Indonesia dalam partisipasi turut memikul tanggung jawab pembangunan Bangsa dan Negara.

Surabaya, Juli 1996

Penulis

UCAPAN TERIMA KASIH

Tiada terkira besarnya bantuan yang telah penulis terima, sehingga penulisan Tugas Akhir ini bisa terselesaikan.

Dengan segala ketulusan dan keikhlasan hati, penulis mengucapkan terima kasih atas segala bimbingan, bantuan, dorongan dan dukungan, baik moril maupun materiil, kepada :

1. Bapak DR. Ir. M. Salehudin, M.Eng.Sc, selaku dosen pembimbing yang telah membimbing dan mengarahkan dalam menyelesaikan Tugas Akhir ini.

2. Bapak Ir. M. Aries Purnomo, selaku Koordinator Bidang Studi Teknik Telekomunikasi Jurusan Teknik Elektro.

3. Bapak DR. Ir. M. Salehudin, M.Eng.Sc, selaku Ketua Jurusan Teknik Elektro, Bapak Ir. Achmad Ansori, Bapak Ir. Suwadi, selaku dosen wali penulis, serta Bapak dan Ibu dosen di Jurusan Teknik Elektro.

4. Bapak Ir. Made Harta Wijaya, selaku pembimbing dari PT. Indosat yang telah banyak sekali membantu penulis dalam memperoleh data yang diperlukan.

5. Bapak Ir. Ekky Suwarso dan Ibu Ir. Nusi Indriani yang telah banyak menolong selama penulis memerlukan bantuan di PT. Indosat.

6. Papa dan Mama yang dengan curahan kasih sayangnya telah mengasuh dan membimbingku.

7. Bapak dan Ibu serta Mas Dick dan Mas Ciek yang telah dengan sabar membantu dan menerima kehadiranku yang sangat merepotkan sehingga semuanya berjalan dengan lancar.

8. Kasihku, Mada "Ayang" yang telah memberikan perhatian dan dorongan semangatnya sehingga Tugas Akhir ini terselesaikan.

9. Sahabat-sahabatku yang telah lebih dulu meninggalkan kampus, Leksmana "Leksi Tajir" Wardana, Geigy "Om Tam" Soehadi, Andri Wibawanto, M. Choirul "Acil" Anwar, Budi Susilo, A. Rizky "Pak Thol" Maulana, Ario "Swamp" Damarjati, Ery "Pipi" Prasetyawan, Aju "Atun" W., akhirnya kita senasib, sambutlah kehadiranku.

10. Rekan-rekan Cak San, Agung "Puyi" Wibisono, Nanang "Tuek" Juniarto, Prabowo "Moly" A.S., Ali "Jemblung" Sadikin, Ibnu "Irung" A.S., Iwan "Kates" D., yang telah banyak mengotori hari-hariku di ITS dengan pengalaman-pengalaman dan hura-huranya. *Nek iso ngumpul-ngumpul maneh koyok mbiyen.*

11. Teman-teman kelompok DD 19 yang selama ini telah membantu saya menghilangkan rasa sakit dengan canda dan acara-acara yang "gile bener". Thanks to Pim Pim, Bogie, Dony, Sony, Ifie, Jijie, Yanti, Firlie, Migiya dan masih banyak lagi yang lainnya.

12. Mbak Dhita dan Aries yang dengan sabar dan perhatiannya pada saya serta sudi meminjami printernya sewaktu saya sangat membutuhkannya. *Matur Nuwun Mbak, Gusti Allah sing mbales.*

13. Rekan-rekan Lab 301, Inten, Lembeng, Agung Peh, Arief, Yudhi, *pokoke konco-konco sing sak perjuangan, suwun sing akeh yo rek.*

14. Karyawan di Bidang Studi Telekomunikasi, Mas Hendry, Panut yang telah banyak memberi bantuan dan banyak mengisi kehadiranku di Laboratorium.

15. Dan semua pihak yang aku kenal dan pernah terlibat denganku, yang lupa kusebutkan, *sing akeh sepurane yo rek.*

Semoga ALLAH SWT memberikan rahmat dan ridlo-Nya atas segala amalan dan bantuan yang telah dilakukan dengan ketulusan hati. Amin ya Robbi.

DAFTAR ISI

HALAMAN

HALAMAN

HALAMAN

HALAMAN

HALAMAN

HALAMAN

DAFTAR GAMBAR

GAMBAR HALAMAN

DAFTAR TABEL

BAB I

PENDAHULUAN

I.1. LATAR BELAKANG

Dalam waktu yang tidak lama lagi, beberapa kota besar di Indonesia yang pada umumnya pertumbuhan ekonomi dan sosialnya berkembang pesat, akan membutuhkan suatu komunikasi yang mempunyai bentuk berbeda dengan apa yang kita nikmati saat ini. Hal ini disebabkan oleh berkembangnya sektor perdagangan, bisnis, industri dan sebagainya yang semakin meningkat dan memiliki bentuk yang beragam pula.

Seperti halnya mata rantai yang saling berkaitan dengan mata rantai yang lain, maka dengan meningkatnya pertumbuhan ekonomi dan sosial tersebut, mengakibatkan kebutuhan terhadap pelayanan dan jasa di bidang telekomunikasi juga turut meningkat. Apalagi ditambah dengan pertumbuhan populasi penduduk dan tuntutan bagi kemajuan yang menuju ke arah globalisasi. Hal tersebut akan mendorong semakin tingginya permintaan akan jaringan satuan sambungan yang perlu disediakan. Merupakan suatu pekerjaan besar bagi perusahaan telekomunikasi untuk dapat menambah kapasitas pelayanan jaringan, di samping merupakan kewajiban untuk mendukung unjuk kerja dari jaringan existing agar dapat beroperasi secara optimal. Meningkatnya jumlah pelanggan menyebabkan jaringan telekomunikasi semakin kompleks dan rumit.

Evolusi dari stored program control switching dan common channel signaling mempermudah pengembangan pada beberapa pelayanan yang berdasarkan jaringan publik (umum) baru seperti misalnya 800 Service, Automatic Calling Card Service dan lain-lain. Sebagai penerapan dari kemampuan-kemampuan ini terhadap pelayanan jaringan pribadi, Virtual Private Network (VPN) muncul sebagai alternatif baru untuk memenuhi kebutuhan akan jaringan pelanggan pribadi.

Pelayanan Virtual Private Network (VPN) yaitu pelayanan jaringan virtual yang berdasarkan software yang menyerupai jaringan pribadi yang menggunakan fasilitas-fasilitas switching dan transmisi jaringan publik (umum).

Penerapan teknologi Virtual Private Network (VPN) yang merupakan salah satu aplikasi dari Intelligent Network (IN) atau jaringan pintar akan memberikan pelayanan yang dapat memenuhi kebutuhan komunikasi yang meningkat tersebut dengan tingkat keamanan jaringan telekomunikasi yang tinggi.

I.2. PERMASALAHAN

Dalam tugas akhir ini akan dibahas permasalahan mengenai Virtual Private Network (VPN) sebagai suatu alternatif terbaru untuk memenuhi kebutuhan akan jaringan pelanggan pribadi dan kemungkinan penerapannya dalam jaringan publik (umum) di Indonesia serta aspek-aspek yang mempengaruhinya.

I.3. PEMBATASAN MASALAH

Dalam pembahasan tugas akhir ini akan menguraikan motivasi dan evolusi dari Virtual Private Network (VPN) dan juga sifat-sifat khasnya dan kemampuan-kemampuannya. Karena sentral-sentral jaringan publik (umum) memiliki karakteristik yang berbeda-beda, maka pembahasan mengenai kemungkinan penerapan VPN pada sentral-sentral tersebut akan dibatasi hanya pada konfigurasi sistem, fungsi dan kegunaannya.

I.4. METODOLOGI

Dengan pertimbangan bahwa pokok bahasan dalam tugas akhir ini belum diterapkan untuk telekomunikasi wilayah nasional tetapi telah diterapkan untuk ke arah wilayah internasional, maka metode yang dipakai dalam membahas permasalahan adalah melakukan studi literatur dari beberapa draft rekomendasi CCITT tentang VPN, buku-buku beserta jurnal-jurnal dan makalah-makalah yang membahas tentang VPN dan data-data yang berkaitan dengan jaringan existing di beberapa kota besar di dunia. Dari keseluruhan bahan-bahan yang terkumpul, akan dilakukan analisa dan pembahasan untuk mendapatkan kesimpulan yang diperlukan.

I.5. SISTEMATIKA PEMBAHASAN

Tugas akhir ini disusun dalam empat bab guna memudahkan pembahasan permasalahan yaitu :

⇒ Bab Satu, berisi mengenai pendahuluan yang mengetengahkan latar belakang, permasalahan, pembatasan masalah, metodologi dan sistematika pembahasan serta relevansi dari tugas akhir ini;

⇒ Bab Dua, berisi mengenai pembahasan tentang konsep Intelligent Network (IN) secara garis besar dan akan membahas sedikit mengenai VPN yang diterapkan untuk telekomunikasi ke arah wilayah internasional;

⇒ Bab Tiga, merupakan bab yang mengulas tentang Virtual Private Network (VPN) termasuk keuntungan-keuntungan VPN baik bagi pelanggan maupun penyelenggara VPN;

⇒ Bab Empat, adalah berisi tentang kesimpulan dan saran-saran dari pembahasan masalah VPN.

I.6. TUJUAN

Tujuan dari Tugas Akhir ini yaitu untuk mengkaji kelayakan penerapan layanan Virtual Private Network sebagai salah satu aplikasi dari Intelligent Network pada jaringan publik di Indonesia, yang ditinjau dari segi ekonomisnya.

I.7. RELEVANSI

Dengan hasil studi tentang penerapan Virtual Private Network (VPN) dalam jaringan publik (umum) yang existing di Indonesia untuk menunjang telekomunikasi ke arah wilayah internasional, diharapkan adanya suatu pemahaman yang mendalam tentang sasaran keseluruhan dari konsep VPN dalam mengoptimalkan operasi jaringan telekomunikasi khususnya jaringan telekomunikasi digital dalam memenuhi kebutuhan trafik yang padat dengan berbagai pelayanan jaringan yang dibutuhkan baik pada saat sekarang maupun pada masa yang akan datang terutama dalam transfer informasi antar komponen IN serta pengembangan lebih jauh dari VPN sebagai salah satu bentuk aplikasi pelayanan dari Intelligent Network (IN) atau dikenal dengan istilah Jaringan Pintar. Disamping itu, tugas akhir ini diharapkan juga dapat digunakan sebagai acuan untuk penerapan VPN lebih lanjut yang dikaitkan dengan pengembangan teknologi telekomunikasi di Indonesia.

BAB II

JARINGAN PINTAR

(INTELLIGENT NETWORK)

II. 1. KONSEP INTELLIGENT NETWORK (IN)

Konsep Jaringan Pintar atau Intelligent Network, disingkat IN, berawal dari diperkenalkannnya teknologi komputer di dalam sentral telepon dengan sistem **Stored Program Control (SPC)** yang dilengkapi beberapa fasilitas, disamping tugas utama untuk melaksanakan penyambungan juga misalnya dalam bentuk respon permintaan pelayanan yang diinginkan pelanggan. Dengan demikian sifat intelijen sudah dapat diberikan oleh sistem **SPC**. Tetapi sistem **SPC** belum dapat disebut sebagai suatu jaringan intelijen karena sistem ini baru merupakan blok yang berdiri sendiri-sendiri. Pelayanannya sudah dapat mendukung prototipe dari konsep layanan IN seperti call waiting pada *residential market* dan *centrex* pada daerah bisnis (layanan yang dibuat berdasarkan *switch based*).

Pada pertengahan tahun 1970 teknologi **SPC** sudah mendukung jaringan manajemen dan maintenance yang dapat dikenal sebagai **Operation Support System (OSS).** Di samping itu pada jaringan juga mulai diperkenalkan **Common Channel Signaling (CCS).** Dengan **CCS** sinyal informasi tidak lagi

ditransmisikan melalui kanal bicara tetapi menggunakan kanal yang terpisah. Berdasarkan prasyarat-prasyarat teknis di atas dan permintaan dari pelanggan (*end user*) maupun permintaan dari perusahaan pengoperasi jaringan menimbulkan kebutuhan evolusi dari jaringan yang solusinya adalah konsep jaringan baru yang didefinisikan sebagai **Intelligent Network (IN).** Antara tahun 1986 dan 1990 di Amerika Utara berkembang konsep IN/1 (IN generasi pertama) dan IN/1+, kemudian oleh Bellcore's diperkenalkan lagi IN/2 (IN generasi kedua). Perkembangan evolusi IN oleh **Multi-Vendor Interaction (MVI)** suatu forum industri di Amerika didefinisikan ke **Advanced Intelligent Network (AIN).**

II.2. DEFINISI INTELLIGENT NETWORK (IN)

Jaringan Pintar atau Intelligent Network (IN) didefinisikan sebagai "*suatu arsitektur jaringan yang mampu menyediakan bermacam-macam pelayanan telekomunikasi, sekaligus menyediakan kontrol atau kendali dan manajemen dari penyediaan pelayanan-pelayanan tersebut*"[1]. Pada dasarnya konsep Jaringan Pintar (IN) merupakan penambahan sistem intelijen terpusat (*centralised intelligence*) pada jaringan telepon publik sedemikian rupa hingga pelayanan yang spesifik dapat ditawarkan secara ekonomis. Dengan demikian IN bertindak sebagai arsitektur pengendali pelayanan dari suatu jaringan

---

[1] Sutanto, Agung, A. S., *Standard Intelligent Network (IN); Pentingnya Bagi Penyelenggara Telekomunikasi*, Gematel, PT Telkom, Desember 1994, hal 5

telekomunikasi. ITU-T sendiri telah mendefinisikan model konsep IN kedalam **Physical Entities (PEs)** dan **Functional Entities (FEs).**

Arsitektur Jaringan Pintar (IN) yang tidak tergantung pada tipe jaringan telekomunikasi dan perangkat fisik (Physical Entities) dalam jaringan memungkinkan pemisahan kemampuan switch dan routing dari kemampuan penyediaan pelayanan dalam jaringan. Informasi pemrosesan panggilan tidak lagi harus dalam switch tetapi dapat juga ada pada komponen lain dalam jaringan. Dengan adanya himpunan modul software service, ITU-T menyebutnya **Service Independent Building Blocks (SIB),** yang bisa disusun dengan berbagai cara menjadi pelayanan tertentu, menjadikan IN mampu :

- merekayasa pelayanan baru secara cepat
- menyebarluaskan pelayanan baru dalam jaringan secara cepat
- menyediakan pelayanan kebutuhan pelanggan dengan cepat dan mudah

Dari banyak pemegang peran dalam bidang telekomunikasi dan komputer, keduanya menginginkan integrasi diantara mereka, sehingga tercipta struktur terpadu untuk kendali/kontrol dan manajemen informasi secara global. IN adalah jembatan untuk mencapai penyatuan kedua pihak tersebut. IN menginginkan penyatuan kreasi pelayanan (*deployment*), pemeliharaan (*maintenance*), dan manajemen sistemnya.

II.3. TUJUAN INTELLIGENT NETWORK (IN)

Intelligent Network (IN) secara umum mempunyai tujuan adalah sebagai berikut :

a. Menyediakan arsitektur jaringan yang fleksibel

Dengan arsitektur jaringan yang bersifat fleksibel tersebut maka dimungkinkan :

- proses adaptasi terhadap perubahan teknis, sistem pengaturan dan kebutuhan pemasaran
- adanya sistem yang tidak tergantung pada kapabilitas dan jasa pelayanan khusus
- pengontrolan fungsi dan jasa pelayanan untuk jumlah pelanggan yang lebih besar
- administrasi dan kontrol sistem jaringan secara efisien
- dukungan terhadap kebutuhan infrastruktur jaringan komunikasi nasional

b. Menyediakan antarmuka jaringan yang standar

Dengan tersedianya antarmuka jaringan yang standar diharapkan adanya :

- suasana persaingan promosi yang kompetitif

- sistem pengaturan yang konsisten
- rangsangan penggunaan jaringan secara maksimal
- penggunaan standar yang baku, seperti CCS#7 dan TCAP untuk signaling network dan ISDN untuk prosedur dan kapabilitas

c. Kemudahan dan kecepatan dalam pengenalan jasa pelayanan

Tujuan ini meliputi :

- kemampuan dalam mengantisipasi kebutuhan pasar
- pengembangan dan perluasan jangkauan jasa pelayanan
- kemampuan melayani pelanggan di daerah khusus dan yang bersifat individu

Adapun yang menjadi faktor pendorong digelarnya Jaringan Pintar (IN) antara lain adalah[2] :

a) Arsitektur Jaringan Terbuka

ITU-T yang menstandarkan antarmuka arsitektur IN yang bersifat terbuka menyebabkan dimungkinkannya muncul banyak penyedia jasa (*subscriber service* atau *service provider*). Pengelola jaringan

---

[2] _____, *Intelligent Network; Sebagai Solusi Jaringan Jasa Telekomunikasi*, Makalah Presentasi Teknologi Komunikasi, PT Telkom, Desember 1994, hal. 4

(*Network Operator*) dapat menciptakan kompetisi diantara penyedia jasa karena untuk menciptakan advanced service dibutuhkan kompetisi.

b) Ketidaktergantungan pada Vendor

Sasaran pokok IN adalah terbebasnya dari ketergantungan terhadap satu pembuat peralatan tertentu karena telah terdapatnya antarmuka yang standar berdasarkan ITU-T, misalnya CCS#7 beserta **Transaction Capability Application Part (TCAP).** Perusahaan yang mengoperasikannya (*Network Operator*) dapat memilih Network Elemen dari beberapa vendor tanpa banyak masalah dalam kompabilitas. Lingkungan yang distandarkan terbuka untuk banyak vendor misalnya terdapat pada network elemen dan OSS.

c) Distributed Architecture

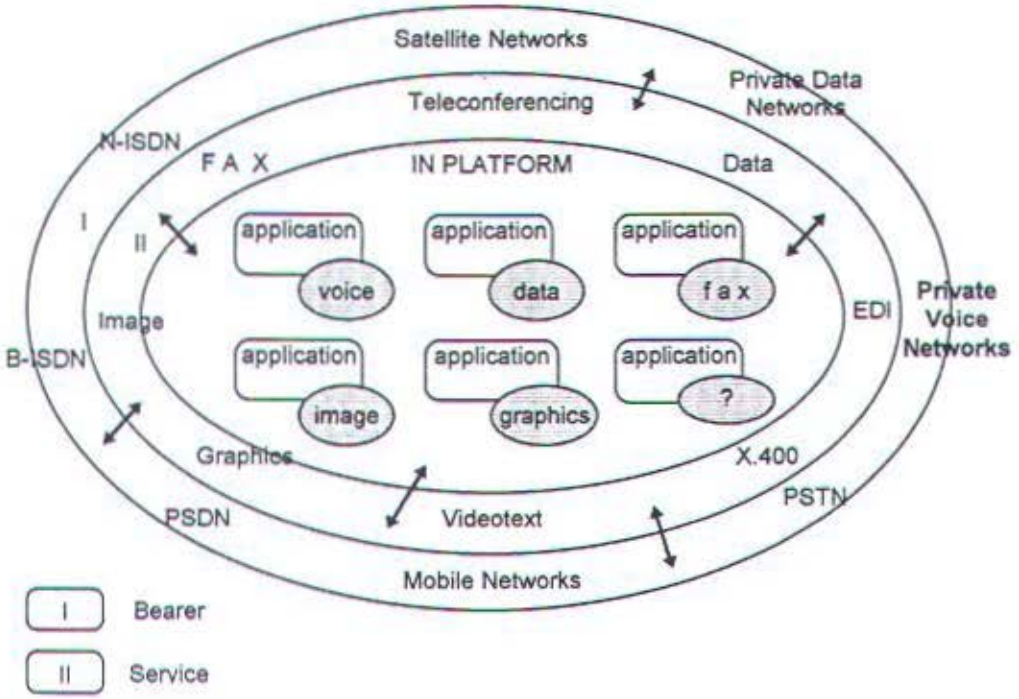
Industri processing data/computer melihat perubahan arsitektur mainframe dari terpusat ke distribusi, saling terkoneksi dengan Work Station. Sehingga pada jaringan telekomunikasi kemampuan processing dan intelijen dapat dipindahkan dari switching office ke bagian eksternal misalnya pada platform IN. Oleh Bellcore visi jaringan yang terdistribusi penuh telah diproyeksikan dengan dimulainya **Information Networkng Architecture (INA).**

d) Network Evolution (Evolusi Jaringan)

Aspek pokok dari perkembangan arsitektur IN adalah mendukung perkembangan Network Evolution. Hal ini dimungkinkan dengan terpisahnya fungsi penyelenggara pelayanan jaringan (*service segment*) dengan fungsi transport (*transport segment*). Pengembangan fungsi transport pada bit-bit secara cepat dan handal pada masa-masa yang akan datang seperti pada multimedia dan terjadinya perkembangan pada akses lain yang bersifat mobilitas misalnya PCN maka hal ini akan tetap dapat terintegrasi dengan platform IN. Dengan kata lain IN platform akan menjadikan terintegrasinya service jaringan yang berasal dari akses POTS, mobile, ISDN, seperti dijelaskan pada gambar 2.1.

e) Computer and Communications Technology

Secara teknis pengaruh kuat dunia komputer merupakan kekuatan yang mendorong teknologi IN. Dengan platform IN maka perkawinan dari kedua teknologi tersebut yaitu teknologi informatika dan telekomunikasi akan lebih mendekatkan hubungan komputer dan komunikasi dan mewujudkan era ke arah yang dikenal dengan **Computer and Communications**.



GAMBAR 2.1[3]

INTEGRASI MULTIMEDIA

II.4. ELEMEN-ELEMEN INTELLIGENT NETWORK

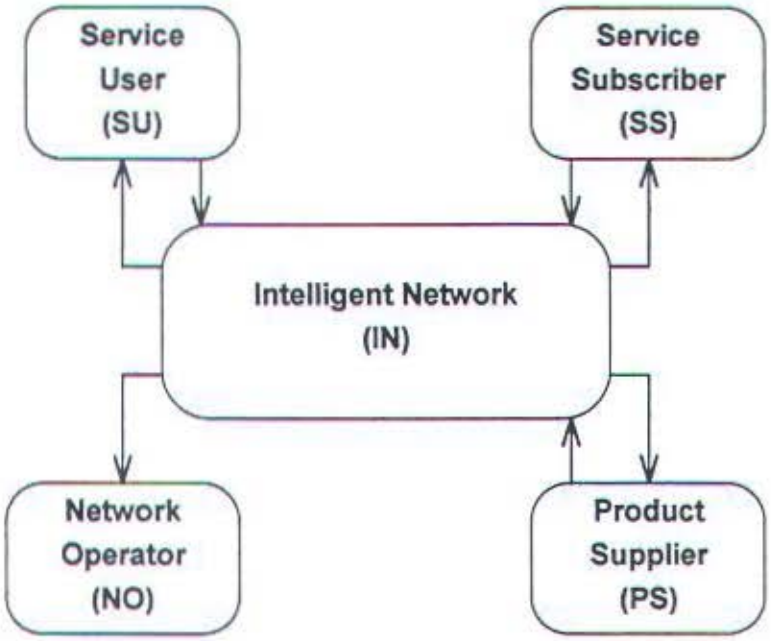
II.4.1 Antarmuka Pengguna IN

Teknologi Jaringan Pintar (IN) merupakan kebutuhan yang cukup penting bagi dunia telekomunikasi, dan penggunaannya diperkirakan akan makin

---

[3] Ibid, hal 5

meluas ke berbagai pihak yang berkepentingan. Secara skematis pengguna teknologi Jaringan Pintar (IN) digambarkan sebagai berikut :



GAMBAR 2.2[4]

ANTARMUKA PENGGUNA IN

[4] Ambrosch, W.D., Maher, A., Sasscer, B., *The Intelligent Network; A Joint Study by Bell Atlantic, IBM and Siemens*, Springer-Verlag, Berlin, 1989, hal 69

Keterangan gambar :

SU - IN : kode akses (*service*) dan **virtual number** (*sevice subscriber*). Jika service meliputi seluruh mode kecepatan aliran antara service dan user, maka **Plain Old Telephone Service (POTS)** tidak dapat digunakan tanpa **Multi Frequency Signaling (MF).**

IN - SU : pembangunan panggilan dan **audible ringing**. Untuk sevice yang lebih maju pemakai dapat meningkatkan kecepatan aksesnya dengan memasukkan digit-digit tambahan.

SS - IN : permintaan pelayanan termasuk yang berhubungan dengan data seperti parameter **routing** dan **screening** serta **Alternate Billing Number.**

IN - SS : konfirmasi permintaan panggilan, konfirmasi data yang telah diperbarui, petunjuk dialog, informasi dan statistik pelayanan.

NO - IN : suplai, dukungan operasi, administrasi dan pemeliharaan service data dan logic.

IN - NO : data operasi jaringan, pengukuran trafik dan informasi pembayaran.

PS - IN : sumber ketentuan-ketentuan dalam IN, dan penunjang NO dalam area administrasi dan pemeliharaan.

IN - PS : keperluan terhadap produk IN.

Jadi dari sudut pandang user, IN tampak sebagai kotak hitam (*black box*) tanpa memperhatikan komponen jaringan yang spesifik, dimana ia terhubung.

II.4.2 Service User

Service User adalah pihak-pihak yang memanfaatkan jasa pelayanan dari IN, contohnya pihak yang melakukan dial pada nomor panggilan tertentu. Peralatan service user umumnya berupa pesawat telepon, namun dapat juga peralatan dengan standar ISDN. Oleh sebab itu fungsi-fungsi pelayanan juga didasarkan kemampuan akses pada kedua tipe peralatan tersebut. Pada umumnya service user tidak mempunyai hubungan kontrak dengan Operator Jaringan IN (Network Operator).

Kemampuan akses dari pelayanan tersebut tidak mencakup peralatan POTS yang tidak menggunakan fungsi dialing multifrekuensi (MF), karena interaksinya sulit bila menggunakan dial pensinyalan pulsa.

II.4.3 Service Subscriber

Service Subscriber dengan akses service dari *Network Operator*, menghubungkan pelayanan yang tersedia ke pemakai (*end user*). Service Subscriber terikat kontrak dengan Opera Jaringan IN. Hal lain yang dapat dilakukan oleh Service Subscriber adalah melakukan perubahan parameter pelayanan. Cara yang dapat dilakukan, yaitu :

- dengan pengajuan permintaan service kepada *Network Operator* yang bertanggung jawab dalam memperbarui data-data yang diperlukan.
- dengan melalui terminal data, Subscriber harus dapat melakukan dial dan akses ke dalam sistem manajemen pelayanan.

Untuk keperluan akses ke dalam sistem manajemen tersebut disediakan dua jalan, yaitu :

1) Direct Access, berupa hubungan langsung melalui terminal synchronous 3270 dengan circuit 9.6 KB. Setiap sisi terminal menggunakan dua buah rangkaian, dimana rangkaian kedua dapat digunakan sebagai backup atau untuk mengoperasikan printer.

2) Dial - In Access, menggunakan komponen hardware yang mendukung terminal diantaranya sistem 24 line dengan 80 karakter per line, standar karakter EBCDIC dan *audible alarm*.

Subscriber dapat pula meminta informasi trafik dalam bentuk daftar/tabel. Misalnya untuk jasa pelayanan **Freecall** (*Freephone*), data pemanggil (nomor dan waktu pemanggilan) dan frekuensi panggilan merupakan informasi yang penting. *Service Suscriber* mendefinisikan feature pelayanan disertai dengan struktur pendukungnya (dapat berupa *routing tree*).

II.4.4 Network Operator

Network Operator merupakan pihak yang menyediakan, mengatur dan juga mengelola jaringan agar dapat dimanfaatkan oleh *Service User* dan *Service Subscriber*. Network Operator sering juga disebut sebagai **Service Administrator** dan merupakan penyelenggara jaringan telekomunikasi dengan pelayanan IN. Aktifitas Network Operator terdiri dari :

- menetapkan schedule dari sistem manajemen, seperti mentransmisikan perubahan-perubahan parameter, mem-backup database dan menyusun laporan
- memodifkasi database karena adanya perubahan data pemakai (*user*)
- menambahkan data *service subscriber* baru ke dalam database
- mendefinisikan parameter untuk pengukuran trafik dan pembebanan biaya

- mendefinisikan parameter laporan pelayanan
- menyediakan laporan khusus bagi *service subscriber*

II.4.5 Network Product Supplier

Jaringan **Product Supplier (PS)** menyediakan produk-produk yang digunakan oleh *Network Operator* untuk melakukan aktifitasnya. Sebagai penyedia peralatan yang diperlukan oleh *Network Operator*, maka *Network Product Supplier* juga merupakan pihak pendukung khususnya dalam hal administrasi dan pemeliharaan produk. PS menerbitkan spesifikasi dan ketentuan-ketentuan operasional produk-produk yang digunakan dalam jaringan.

II.5. UNSUR-UNSUR INTELLIGENT NETWORK

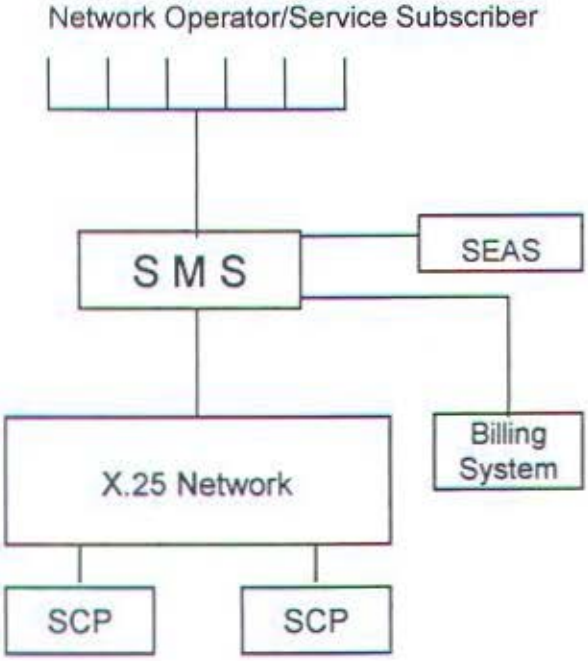
II.5.1. Service Management System (SMS)

Service Management System (SMS) dimiliki oleh operator jaringan. SMS melengkapi Service Control Point (SCP) dengan data atau program baru dan mengumpulkan statistik dari SCP. SMS juga memungkinkan pelanggan untuk mengendalikan parameter-parameter layanannya sendiri melalui terminal yang dihubungkan dengan SMS. Modifikasi ini difilter atau diperbaiki oleh operator jaringan. SMS biasanya adalah suatu komputer komersial seperti IBM/370 atau

Siemens 7.5xx. SMS juga dapat memberikan suasana untuk mengembangkan layanan baru.

III.5.1.1. Arsitektur SMS

SMS dihubungkan ke SCP melalui jaringan X.25. Banyaknya saluran dari SMS ke jaringan X.25 bergantung pada jumlah trafik yang didukungnya. SMS dapat pula dihubungkan ke Signaling, Engineering and Administration System (SEAS) atau ke suatu operator untuk kepentingan charging.



GAMBAR 2.3[5]
ANTARMUKA SMS

[5] Ibid, hal. 58

SMS dan SCP saling menukarkan informasi dan mengontrol operasi message diantara kedua komponen. Message-message yang dikirimkan diantara kedua komponen tersebut dikelompokkan dalam :

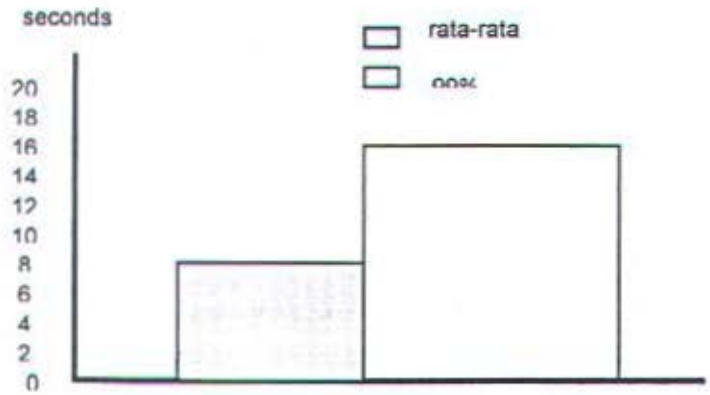
Measurement Data

SMS mengumpulkan data dari SCP tentang trafik dan unjuk kerjanya. SCP menyediakan hasil pengukuran yang diperlukan SMS. Message ini mencatat operasi hardware dan software serta trafik yang keluar dan masuk ke SCP. Secara periodik catatan itu diminta oleh SMS yang kemudian akan menyimpannya.

Status Data

SMS juga menangani penurunan unjuk kerja SCP dan mengurangi banyaknya data yang hilang akibat trafik yang berlebihan.

Waktu respons maksimal SCP terhadap suatu message SMS adalah 8 detik. Sedangkan untuk 99% message SMS responsnya tidak melebihi 16 detik.



GAMBAR 2.4[6]

WAKTU RESPON SCP TERHADAP MESSAGE SMS

[6] Ibid, hal. 41

III.5.1.2. Fungsional SMS

Fungsi-fungsi yang dijalankan oleh SMS adalah :

- User Access Control

  SMS mengontrol akses-akses dari service subscriber dan operator untuk seluruh service yang ditawarkan. Setiap user diidentifikasi dengan sebuah ID dan password yang dapat diubah-ubah, dan diatur fungsi dan data mana saja yang dapat diaksesnya.

- Database Control

  SMS mensupport satu atau lebih database dari suatu service. Database ini dapat diakses dari aplikasi pelayanan lewat suatu sistem manajemen database yang bersangkutan. Setiap operator pelayanan mempunyai akses penuh ke database pelayanan dan dapat meng-update datanya untuk menyesuaikan perkembangan data terakhir.

- Manajemen Trafik dan Unjuk Kerja SCP

  Secara otomatis, SMS juga menerima trafik dan data dari SCP yang dikelolanya. Beberapa proses yang dilakukan SMS dalam mengelola trafik dan data tersebut diantaranya menganalisa dan mendeteksi bila terjadi overload, merespons permintaan interogasi dari jaringan dan service operator.

- Support Node dan Service SCP

SMS mengatur konfigurasi data yang dihubungkan ke SCP. Data tersebut dapat dikelompokkan dalam :

a. Informasi hubungan SCP dengan jaringan CCS#7.

b. Data implementasi SCP (seperti alokasi disk dan *buffer).*

c. Data pengontrolan suatu service (seperti proses query dan respons time).

Fungsi support ini umumnya digunakan pada saat penginstallan SCP atau service baru serta saat perubahan database.

- Billing

Ada dua level fungsi billing/charging yang disediakan SMS, yaitu billing bagi service subscriber untuk penggunaan fungsi tertentu dari SMS dan billing bagi penyedia service untuk seluruh aktifitas SMS yang berhubungan dengan service yang disediakannya. Besarnya charging dipengaruhi beberapa faktor seperti lama waktu akses kedalam SMS dan banyaknya data dalam database yang diakses.

- Report Generation

SMS menyediakan program report mengenai aktifitas dalam SMS dan node SCP yang dikelolanya. Isi report meliputi analisa trafik dan unjuk kerja, informasi billing dan aktifitas terminal user.

II.5.2. Service Control Point (SCP)

Service Control Point (SCP) dipakai apabila layanan baru diperkenalkan pada jaringan dan difungsikan. Apabila layanan didasarkan atas unsur-unsur fungsional (IN/1 dan IN/2), maka komponen-komponen fungsional dilaksanakan dengan bantuan Service Logic Interpreter. Beberapa layanan SCP memerlukan banyak data, yang dikumpulkan ditempat penyimpanan yang dapat dicapai segera, misalnya disket. Program layanan dan data diperbaiki melalui SMS. SCP adalah komputer komersial atau suatu switch yang diubah. Faktor kritis adalah bahwa unit dapat mencapai data secara efisien dan dapat dipercaya dan menyediakan lahan untuk menciptakan layanan cepat (melalui pembuatan program sendiri dan program portabel).

II.5.2.1. Definisi

Service Control Point (SCP) adalah sistem komputer yang memiliki perangkat keras dan lunak untuk berkomunikasi dengan SSP. SCP memiliki database dan service logic program untuk melengkapi panggilan IN dan terutama berperan pada saat pengenalan pelayanan IN.

SCP bersifat real time dan memiliki sistem availability yang tinggi sebagai penyimpan database untuk penyediaan pelayanan IN. SCP merupakan suatu kesatuan node yang dapat dicapai melalui jaringan Common Channel Signaling (CCS) dan atau dengan Packet Switched Public Data Network (PSPDN). Komponen ini menyediakan interface jaringan untuk pembangunan

pelayanan IN termasuk dalam mengakses pesan dan respons dari komponen lain dalam jaringan.

SCP menyediakan semua fungsi untuk mendukung satu atau lebih aplikasi pelayanan IN. Node SCP berisi perangkat keras dan lunak yang berguna dalam pembangunan aplikasi tersebut. Fungsi - fungsi tersebut dapat bersifat indipenden maupun digunakan bersama untuk beberapa aplikasi.

II.5.2.2. Fungsi-fungsi Pemrosesan dalam SCP

Tugas utama SCP adalah menyediakan kemampuan akses yang tinggi serta pemrosesan aplikasi-aplikasi database. SCP mampu membentuk fungsi-fungsi berikut :

a. Pemrosesan Message

Kemampuan ini meliputi fungsi-fungsi untuk mengalirkan message melalui SCP menuju node-node tujuan, seperti :

- Eksekusi protokol interface jaringan (CCS#7, X.25, BX.25)
- Penanganan protocol error
- Diskriminasi message
- Distribusi dan routing message
- Manajemen dan testing jaringan

- Pemrosesan aplikasi
- Administrasi node

b. Operasi, Administrasi dan Maintenance Node

Fungsi-fungsi ini diperlukan dalam mengoperasikan dan mengontrol SCP, meliputi :

- Pengukuran unjuk kerja
- Keamanan
- Deteksi dan perbaikan error
- Deteksi overload dan flow control
- Kontrol konfigurasi

c. Pemrosesan query

SCP melakukan pemrosesan parameter yang terdapat dalam message TCAP "Query" dan memformulasikan jawabannya di dalam message TCAP "Response" yang akan dikembalikan ke SSP.

d. Directing connection control

SCP memiliki tanggung jawab untuk memberitahu SSP bagaimana cara me-route panggilan berdasarkan nomor direktori yang tersimpan di dalamnya. Pada jaringan multi operator, SCP juga harus memberi informasi kepada SSP

apakah panggilan tersebut akan melalui operator telekomunikasi lain.

e. Meminta interaksi dengan pemanggil

Pada kondisi panggilan yang memerlukan informasi tambahan dari pemanggil (seperti PIN), SCP akan meminta SSP untuk mengumpulkan informasi tersebut dan mengirimkannya ke SCP dengan menggunakan message TCAP.

f. Meminta notifikasi terminasi

Respons dari SCP bisa berisi permintaan ke SSP untuk melaporkan setelah panggilan berakhir. SSP akan menjawab permintaan ini dengan message TCAP "Undirectional".

g. Meminta aktivasi/deaktivasi trigger

SCP bisa meminta SSP untuk mengaktivasi atau mendeaktivasi trigger pelanggan yang akan dijawab oleh SSP dengan message "Response" yang berisi informasi keberhasilan aktivasi atau deaktivasi.

h. Automatic call gapping (ACG)

Untuk menghindari overload pada komponen SCP, SCP akan meminta *Automatic Call Gapping (ACG)* pada SSP yang akan bereaksi dengan cara memberikan terminasi ke setiap panggilan IN saat kontrol ACG berlaku.

II.5.2.3. Interface Eksternal SCP

Model IN mendefinisikan dua set interface untuk SCP yang keduanya digunakan untuk menyediakan pelayanan aplikasi database, yaitu :

a. Service network interface

Interface SCP ini menggunakan jaringan CCS dan/atau PSPDN dalam pemrosesan message. Seperti juga jaringan CCS yang memerlukan availability yang tinggi pada tiap pensinyalan end-point, maka interface ini perlu hal yang serupa pula. Interface SCP dengan jaringan CCS memakai protokol CCS#7. Fungsi komunikasi front-end SCP menyediakan terminasi saluran yang menghubungkan secara fisik SCP dengan jaringan CCS. Ujung saluran jaringan CCS tersebut terhubung pada komponen STP. Jumlah saluran dipengaruhi oleh besarnya volume trafik yang ada. SCP dapat berkomunikasi dengan PSPDN menggunakan protokol X.25. Saluran transmisi menghubungkan front-end SCP dengan packet switch ke PSPDN.

b. Support system interface

Sebagai pelengkap interface jaringan, arsitektur IN menyediakan support system interface, yang meliputi :

- Service Management System (SMS)
- Signaling, Engineering and Administration System (SEAS)

- Remote maintenance operations centers
- Local maintenance operations centers

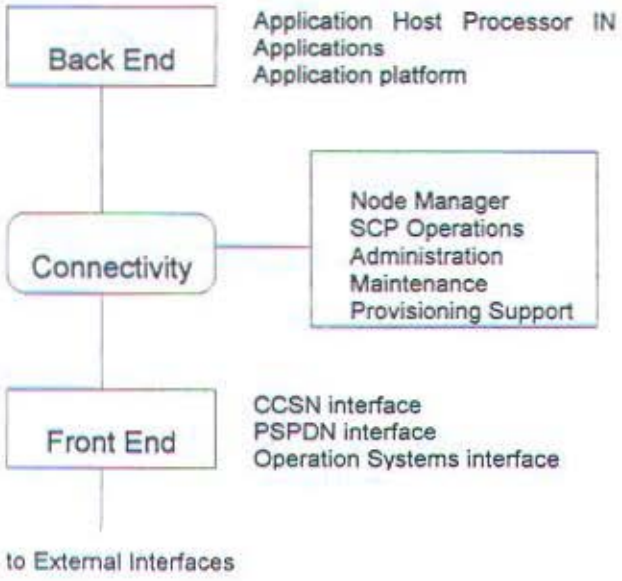
Transport diantara beberapa sistem pendukung di atas dengan SCP menggunakan **Operation System Network (OSN)**, dengan akses melalui interface generik OSN. SCP memakai protokol X.25 untuk mengirim dan menerima message ke dan dari SMS. SMS akan menyediakan sistem administrasi pendukung aplikasi-aplikasi yang ada pada SCP. Dengan adanya sistem tersebut, SMS mengumpulkan trafik dan melakukan pengukuran unjuk kerja SCP. Untuk mengalokasikan tiap aplikasi SCP pada channel yang virtual ke SMS dibutuhkan kapabilitas transmisi yang memadai antara SCP dan SMS.

Protokol X.25 digunakan pula oleh SCP untuk berkomunikasi dengan maintenance operations centers. Sistem ini menerima alarm dan status informasi dari SCP. Selain itu maintenance operations centers mengontrol operasi SCP termasuk konfigurasi sistem dan inisialisasi agar diperoleh availabilitas dan unjuk kerja SCP seperti yang diharapkan.

II.5.2.4. Arsitektur SCP

Service Control Point (SCP) menyediakan volume database yang cukup besar dengan transaksi yang realtime, multi-tasking dan availabilitas yang tinggi. Untuk fleksibilitas yang tinggi, maka SCP memiliki komponen-komponen utama sebagai berikut :

- Connectivity



GAMBAR 2.5[7]

KOMPONEN UTAMA SCP

- Front end
- Back end
- Node manager

II.5.2.4.1. Connectivity

Connectivity menghubungkan tiga komponen yang lain menggunakan sepasang token ring untuk memperoleh fleksibilitas, kapasitas dan kecepatan

---

[7] Ibid, hal. 77

transmisi yang lebih besar. Masing-masing komponen memiliki processor token ring dan direplika di komponen yang lain dengan konfigurasi hardware dan software yang uniform. Replika tersebut umumnya dioperasikan pada beberapa alternatif pembebanan untuk mencapai unjuk kerja maksimum.

Kapasitas Connectivity SCP didasarkan pada jumlah jaringan pelayanan, saluran pendukung dan beban trafik maksimum. Permasalahan beban trafik dapat diatasi dengan penggunaan processor Signaling Point Interface (SPI). Sedangkan jumlah SCP bergantung macam pelayanan yang ada dan demografi trafik.

II.5.2.4.2. Front End

Front End adalah komponen yang menyediakan interface untuk komunikasi eksternal ke jaringan pendukung. Tiap interface eksternal beroperasi secara independen, karena itu untuk tiap SCP terdapat satu set front end. Interface eksternal tersebut meliputi :

- Interface Common Channel Signaling Network (seperti SCCP)

  Signal Point Interface (SPI) menyediakan interface CCS#7 antara SCP dan CCSN untuk pemrosesan message pelayanan. SPI menerima message pelayanan dan Signaling Network Management (SNM) dari CCSN dan mendistribusikannya ke aplikasi lain dalam Applications Host Processor (AHP) atau pada Node Manager. SPI menerima pula message dari aplikasi pada AHP dan Node Manager

kemudian me-route message tersebut ke saluran CCS#7. Node Manager akan mengontrol distribusi message node internal. Selain itu SPI berperan dalam manajemen jaringan pensinyalan CCS#7 dan prosedur administrasi dengan mengatur interface dan mengkomunikasikannya ke Node Manager. Jumlah processor SPI bergantung kebutuhan kapasitas pada SCP berupa kebutuhan jumlah saluran dan trafik.

- Interface PSPDN (seperti X.25)

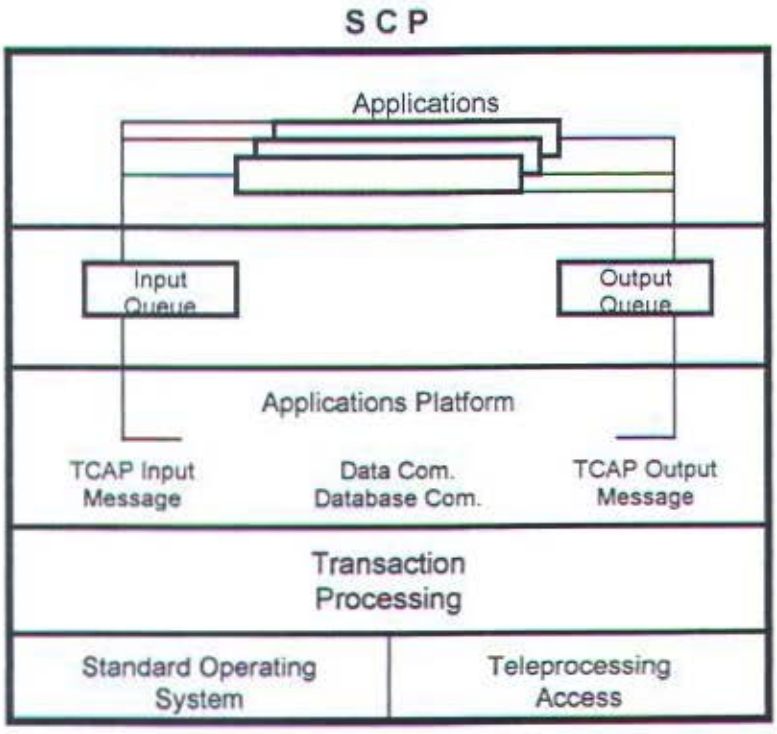
  Melalui interface X.25 yang terpisah, SCP mampu menyediakan pelayanan database secara langsung ke Packet Switched Public Data Network.

- Operator Systems Network Interface (OSNI).

  Operations Support Systems (OSS) mendistribusikan akses OSN melalui X.25. OSNI akan menggandakan kecepatan saluran transmisi data dan menyediakan jaringan packet-sitching data. OSNI menangani User Application Layer (UAL) dan pemrosesan X.25 untuk node SCP. Selain itu OSNI menangani interface ke panel alarm SCP yang menunjukkan status SCP dan komponennya. Interface CCSN dan PSPDN merupakan interface jaringan pelayanan, sedangkan interface OSN adalah interface pendukungnya.

II.5.2.4.3. Back End

Komponen Back End adalah dasar pelayanan database dan berisi processor System/370 yang menyimpan aplikasi database. Tiap *Host* processor ini memiliki platform perangkat lunak node serta **Application Program Interface (API)**. Aplikasi yang tersedia residen pada dua atau lebih *host*. Setiap aplikasi diatur secara independen oleh suatu host processor. Bila ada update database maka disinkronisasikan pada seluruh host SCP.



GAMBAR 2.6[8]

KOMPONEN SOFTWARE SCP

[8] Ibid, hal. 80

Back End berisi AHP sistem/370 yang memiliki komponen-komponen perangkat lunak seperti pada gambar 2.6.

Sistem software terdiri sistem yang mendukung operasi saluran utama. **Virtual Teleprocessing Access Methode (VTAM)** telah dievaluasi untuk kepentingan ini. Sistem operasi dioptimasikan agar dapat bekerja maksimal memenuhi semua kebutuhan operasi SCP.

Platform aplikasi terdiri beberapa fungsi yang digunakan bersama oleh seluruh aplikasi IN, termasuk penanganan dan kontrol data, fungsi komunikasi dan fungsi pemrograman aplikasi. Elemen utama pembentuk platform adalah :

- Komunikasi Data, yang mengatur input dan output aplikasi
- Manajemen Database, yang memproses data dan melakukan update bila diperlukan serta menangani perbaikan data.
- Interface Node Manager, yang meproses seluruh interaksi dengan Node Manager. Elemen ini juga bertindak sebagai pengontrol operasi platform dan aplikasinya.
- Application Program Interface (API), yang memungkinkan personel operator perusahaan telekomunikasi untuk membuat aplikasi baru.

II.5.2.4.4. Node Manager

Node Manager adalah titik koordinasi sentral node SCP. Manajemen node yang lengkap, termasuk semua fungsi kontrol dan koordinasi, dibutuhkan

untuk kontinuitas operasi, administrasi dan pemeliharaan komponen. Hal ini meliputi pula komponen Node Manager dan fungsi interfacenya yang residen pada tiap sub sistem processor *Front End dan Back End*. Tujuan utama Node Manager adalah menjamin agar SCP tampak sebagai suatu kesatuan bagi interface eksternalnya. Fungsi-fungsi yang didukung oleh Node Manager ialah :

- Manajemen jaringan pelayanan
- Manajemen jaringan pendukung
- Interface operasi lokal dan sistem remote
- Spesifikasi data dan administrasi keamanan
- Proses pengukuran
- Konfigurasi manual dan kontrol status hardware/software
- Penanganan kesalahan/error
- Diagnostik

Node Manager mengontrol SCP dan membentuk kesatuan image SCP bagi node-node yang lain seperti STP, SMS dan SEAS. Fungsi-fungsi Node Manager tersebut secara terperinci dikelompokkan dalam 5 golongan :

- Manajemen Unjuk Kerja
- Sistem Pemeliharaan
- Pengontrolan Konfigurasi

- Sistem Administrasi
- Pengontrolan Operasi

a. Manajemen Unjuk Kerja

Manajemen unjuk kerja meliputi fungsi-fungsi sebagai berikut :

- Monitoring status sistem

Monitoring status Node Manager menunjukkan status operasional SCP tentang data yang diperoleh tiap komponen. Setiap komponen SCP mengelola data internal yang menggambarkan proses yang sedang berlangsung dan sub-komponen yang sedang aktif. Status internal dikirimkan ke Node Manager. Secara periodik komponen-komponen tersebut mengirim message status ke Node Manager untuk menunjukkan keaktifannya. Periode itu bergantung tingkat prioritas tiap komponen. Tingkatan-tingkatan tersebut adalah *critical, major dan minor,* yang dihubungkan ke tiga tingkat alarm. Periode tiap level didasarkan pada timing tiap level alarm yang dihubungkan. Sebagai contoh, komponen SCP pada level major periodenya 15 detik, sedang alarm pada tingkat ini dicapai dalam 30 detik. Tiap komponen SCP pada awalnya menempati level yang normal dan dapat diubah sesuai kondisi. Misalnya suatu level yang normal bagi SPI adalah major, namun bila satu SPI saja yang beroperasi maka

level bisa diubah menjadi critical. Jika Node Manager tidak menerima message status pada saat yang tepat, maka dikirimkan permintaan respons pada komponen tersebut. Bila permintaan ini tidak memperoleh tanggapan yang berarti komponen SCP tersebut tidak dapat beroperasi, maka komponen lain diminta untuk melakukan *bypass* dan alarm diaktifkan. Node Manager kemudian melakukan test pada komponen tersebut untuk mengetahui ada tidaknya problem. Jika problem tidak ditemukan, alarm dibatalkan dan komponen tersebut dioperasikan kembali.

- Pengukuran Data

Setiap komponen SCP mengakumulasikan hasil pengukuran yang dilakukannya dalam suatu interval waktu tertentu (normalnya antara 15-30 menit) dan meneruskannya ke Node Manager. Frekuensi pengukuran ini dikendalikan oleh Node Manager. Tiap komponen SCP juga menyimpan data pengukuran terakhir untuk menjaga apabila suatu Node Manager mengalami switch over ,maka Node Manager lain yang menggantikannya akan meminta data tersebut. Node Manager mengkombinasikan hasil pengukuran yang diterima dari seluruh komponen SCP kemudian mengirimkannya ke SMS.

b. Pemeliharaan

Pemeliharaan meliputi fungsi-fungsi sebagai berikut :

- Pemulihan service

  Node Manager mendefinisi ulang konfigurasi SCP untuk *bypass* komponen yang mengalami gangguan dan menotifikasi komponen lain yang terkait. Saat komponen tersebut telah siap, maka Node Manager kembali mendefinisi konfigurasi SCP dan komponen *online* kembali.

- Notifikasi problem

  Setiap komponen SCP akan menginformasikan terjadinya problem pada Node Manager. Message yang menunjukkan adanya problem dibutuhkan oleh Node Manager untuk membangkitkan sinyal indikasi bagi peralatan alarm.

- Manajemen alarm

  Ada tiga tingkat alarm, critical, majo dan minor. Critical alarm memiliki prioritas penanganan paling tinggi, diikuti dengan alarm major. Message output yang dihasilkan dari notifikasi problem mengikuti urutan prioritas yang sama termasuk waktu dan urutan terjadinya problem. Bila jumlah message output tersebut melampaui kapasitas maka prioritas yang lebih tinggi yang akan diutamakan. Node Manager menangani informasi tentang adanya kesalahan dan seberapa tingkat kesalahan tersebut.

- Verifikasi

  Setiap komponen SCP secara otomatis melakukan verifikasi bila timbul problem dengan mengulang operasi yang gagal atau melakukan test rutin. Hasilnya akan diteruskan ke Node Manager. Bila dideteksi adanya problem, Node Manager meminta suatu test dari komponen (subkomponen) untuk meyakinkan terjadinya problem tersebut.

- Isolasi

  Pada saat problem terdeteksi, maka dilakukan isolasi *online* oleh Node Manager terhadap komponen SCP dan oleh komponen SCP terhadap subkomponennya. Isolasi ini diikuti dengan proses perbaikan atau penggantian bagian yang terganggu serta proses konfigurasi ulang. Program diagnostik dan prosedur *offline* juga merupakan suatu sistem isolasi.

- Perbaikan

  Komponen SCP dirancang untuk proses yang berkelanjutan dan dapat diperbaiki tanpa peralatan yang sangat khusus bila mengalami kerusakan. Beberapa komponen seperti SPI, OSNI, dapat diganti secara mudah.

- Error logging

  Message yang salah yang terkirim ke Node Manager tidak langsung

diproses melainkan dikumpulkan dalam suatu selang waktu tertentu yang dapat diubah dengan fasilitas pengontrolan perubahan parameter yang ada pada Node Manager.

c. Pengontrolan konfigurasi

Pengontrolan konfigurasi meliputi fungsi-fungsi :

- Inisialisasi

Langkah pertama dalam inisialisasi adalah mengaktifkan seluruh komponen SCP, lalu memasukkan setiap komponen tersebut dalam **Initial Program Loaded (IPL)** pada keadaan *idle*. Node Manager berkomunikasi dengan OSNI dan memintanya berkomunikasi dengan terminal *craft* untuk meminta hubungan. Terminal tersebut menghubungi Node Manager yang dimaksud dengan prosedur dan password yang ada serta menset parameter operasi untuk SCP, sekaligus membawanya ke SCP yang lain. Terminal ini kemudian bertindak sebagai terminal pengontrolan. Node Manager utama berkomunikasi dengan komponen SCP yang lain untuk semua kegiatan manajemen node. Node Manager mendistribusikan parameter operasi ke seluruh komponen dan juga melakukan koordinasi dengan Node Manager yang menjadi *backup*. Sedangkan SPI berkomunikasi dengan host aplikasi guna pertukaran message menggunakan fasilitas saluran CCS#7. OSNI

melakukan hal yang serupa untuk input *update* database dari SMS. Sedangkan dengan SMS sendiri OSNI berkomunikasi untuk menerima parameter SCP dan pemrosesan permintaan pengukuran SCP dari SMS.

- Pemulihan

Pada saat komponen SCP yang rusak berhasil diperbaiki maka *craft* terminal menotifikasi Node Manager bahwa komponen tersebut telah siap kembali. Node Manager akan mengupdate konfigurasinya dan menotifikasi komponen SCP lain serta STP dan SMS bila diperlukan. Dengan demikian komponen tersebut dapat aktif kembali dalam pemrosesan di SCP.

- Switch-over Node Manager

Node Manager tersusun dari satu processor utama dan satu atau lebih processor lain sebagai backup. Processor yang menjadi backup akan diaktifkan bila processor utama tidak bekerja. Node Manager utama berlaku sebagai titik focus bagi seluruh aktifitas pengendalian, alarm, status dan pengukuran. Processor backup mempunyai fungsi yang sama kecuali tidak adanya interface ke komponen SCP lain. Backup disinkronisasi dengan processor utama agar dapat dilakukan switch-over. Backup Node Manager memonitor Node Manager utama melalui pertukaran message secara periodik.

Backup ini dapat menjadi Node Manager utama bila Node Manager utama tidak aktif.

- Shutdown

Node Manager dapat melakukan shutdown terhadap SCP. Node Manager menotifikasi komponen SCP lain untuk menyiapkan proses shutdown yaitu menuntaskan semua proses, mengosongkan message buffer lalu menotifikasi Node Manager bahwa shutdown siap dilakukan. Bila shutdown akan dilakukan, maka sistem operasi mengirimkan message yang menunjukkan bahwa sesaat lagi sistem operasi akan non aktif. Saat message ini diterima, Node Manager memulai proses *queue* messsage.

- Rekonfigurasi

Node Manager meminta *craft* untuk mengkonfigurasi atau merekonfigurasi SCP. Node Manager mengajukan seluruh komponen SCP dan akan ditentukan oleh *craft* komponen mana yang aktif dan non aktif. Saat konfigurasi telah selesai, Node Manager memulai proses inisialisasi komponen baru. Proses ini dilakukan secara sistematik untuk mengoptimalkan unjuk kerja SCP.

d. Administrasi

Fungsi-fungsi ini meliputi :

- Security

  Sistem security meminta identifikasi/password dari user sebelum dapat mengakses Node Manager. Beberapa file memiliki password tersendiri guna mencegah penyalahgunaan akses.

- Report pengukuran

  SCP mengeluarkan report harian, setiap jam dan setiap 5 menit, dapat pula pada saat diminta atau report sesuai schedule. Informasi report ini dikelola dalam file pengontrolan parameter.

- Manajemen spesifikasi data

  Node Manager mengelola spesifikasi data node dan aplikasi yang diperoleh dari Signaling Engineering and Administration System (SEAS) dan SMS. Data ini berisi antara lain alamat saluran, alamat public switch network, identifikasi aplikasi, kode akses tujuan dan sebagainya. Proses *update* data melalui terminal craft atau berdasarkan message dari SEAS dan SMS. Node Manager mengelola pula spesifikasi data internal yang berisi elemen pengontrol operasi SCP dan berisi antara lain identifikasi atau password dari user, frekuensi statistik komponen, waktu penyimpanan data oleh komponen dan sebagainya. Node Manager mendistribusikan spesifikasi data ke komponen-komponen SCP pada proses inisialisasi atau pada saat perubahan/penggantian komponen.

- Security

  Sistem security meminta identifikasi/password dari user sebelum dapat mengakses Node Manager. Beberapa file memiliki password tersendiri guna mencegah penyalahgunaan akses.

- Report pengukuran

  SCP mengeluarkan report harian, setiap jam dan setiap 5 menit, dapat pula pada saat diminta atau report sesuai schedule. Informasi report ini dikelola dalam file pengontrolan parameter.

- Manajemen spesifikasi data

  Node Manager mengelola spesifikasi data node dan aplikasi yang diperoleh dari Signaling Engineering and Administration System (SEAS) dan SMS. Data ini berisi antara lain alamat saluran, alamat public switch network, identifikasi aplikasi, kode akses tujuan dan sebagainya. Proses *update* data melalui terminal craft atau berdasarkan message dari SEAS dan SMS. Node Manager mengelola pula spesifikasi data internal yang berisi elemen pengontrol operasi SCP dan berisi antara lain identifikasi atau password dari user, frekuensi statistik komponen, waktu penyimpanan data oleh komponen dan sebagainya. Node Manager mendistribusikan spesifikasi data ke komponen-komponen SCP pada proses inisialisasi atau pada saat perubahan/penggantian komponen.

Manager. Panel alarm remote memiliki akses ke SCP melalui jaringan sistem operasi dan diakses oleh Node Manager melalui token ring pada OSNI. Alarm dimatikan bila problem telah selesai diperbaiki.

- Test dan diagnostik

  Perangkat keras memonitor kesalahan dalam komponen SCP. Semua problem diteruskan ke Node Manager. Problem ini dianalisa kemudian dilakukan proses isolasi dan penggantian komponen bila diperlukan.

- Continuous Automatic Test

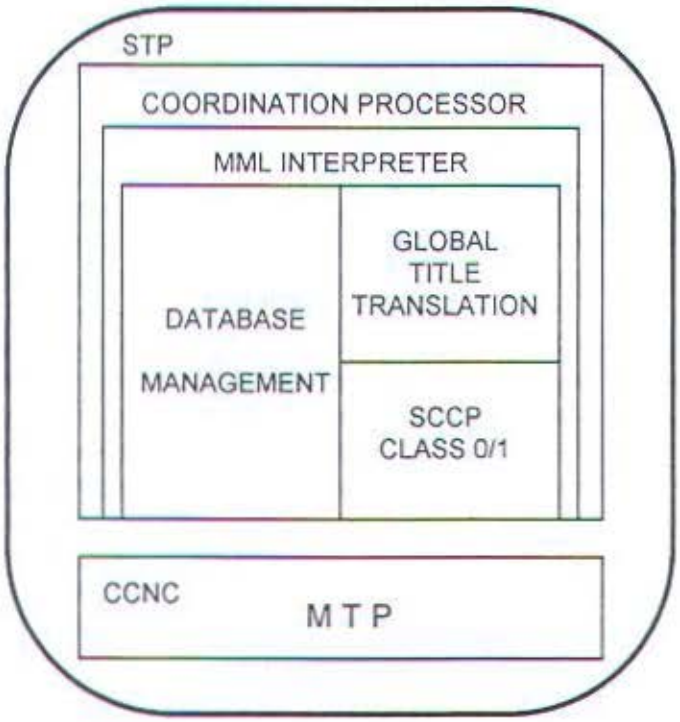
  Proses ini memonitor operasi peralatan, mengkonfirmasi operasi subsistem yang diperlukan dan melakukan test kapabilitas sistem. Dilakukan test rutin terhadap komponen SCP secara periodik dan hasilnya dilaporkan ke Node Manager sebagai bagian status report.

II.5.3. Signaling Transfer Point (STP)

Signaling Transfer Point (STP) adalah bagian dari jaringan Common Channel Signaling Number Seven (CCS#7). STP memindahkan pesan CCS#7 pada beberapa titik simpul CCS#7. CCS#7 adalah sambungan komunikasi baku agar tujuan SCP dan SSP (Service Switching Point) multivendor tercapai. Pemakaian STP mandiri atau integrated akan tergantung kepada konfigurasi jaringan spesifik. STP biasanya dibuat oleh pabrik switch tradisional.

II.5.3.1. Fungsional STP

Dalam arsitektur IN, STP memberikan jasa transfer antara SCP dan SSP dan berlaku sebagai relay point bagi protokol Signaling Connection Control Part (SCCP). STP mampu pula bertindak sebagai konsentrator trafik bagi SCP, bila jaringan CCS#7 kurang baik dalam menangani tambahan trafik pelayanan IN dan/atau tidak mampu mencapai waktu respons yang diiinginkan. Arsitektur Signaling Transfer Point (STP) dapat dilihat pada gambar 2.7.



GAMBAR 2.7[9]
ARSITEKTUR STP

---

[9] Ibid, hal. 90

Common Channel Network Controller (CCNC) membangun fungsi-fungsi protokol Message Transfer Part (MTP) dan mendistribusikan trafik keluar sistem. CCNC merupakan sebuah multiprocessor yang terdiri :

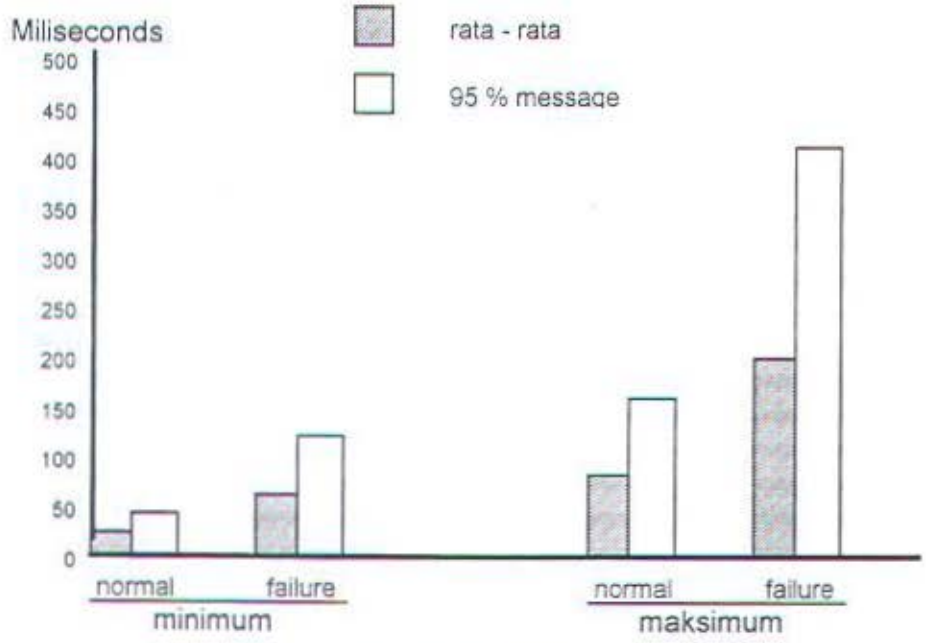
- Peralatan Multiplexing dan modem untuk interface fisik keluar komponen.
- Signaling Link Terminals (SILT) dengan fungsi MTP level 2.
- Signaling Link Terminal Controller (SILTC) sebagai interface antara SILT dan CCNP.
- Common Channel Signaling Network Processor (CCNP) dengan fungsi MTP level 3. CCNP sendiri berisi :
  - Signaling Management Processor (SIMP)
  - Signaling Periphery Adapters (SIPA), 8 buah
  - Coordination Processor Interface (CPI)

Coordination Processor (CP) melakukan fungsi koordinasi pemrosesan panggilan, administrasi dan menyediakan interface peripheral. CP digunakan dalam operasi, administrasi dan manajemen STP sekaligus menghubungkannya ke sistem operasi, administrasi dan manajemen luar.

Fungsi switching dalam STP dilakukan oleh suatu *switching network* yang menghubungkan sinyal yang masuk ke sistem menuju CCNC melalui **Line Trunk Group (LTG).** LTG ini akan melaksanakan fungsi pemrosesan panggilan

yang dikontrol lewat CP dan disalurkan ke saluran transmisi. Sistem perangkat lunak STP terdistribusi antara **Coordination Procesor (CP)** dan **Line Trunk Group (LTG)** untuk memperoleh sistem pemrosesan paralel dengan efisiensi yang tinggi.

Seperti komponen yang lain, STP memiliki delay/response time. Delay message pada STP dihitung mulai saat STP menerima bit terakhir message TCAP pada saluran pensinyalan input hingga bit terakhir dikirimkan pada saluran pensinyalan output. Delay waktu ini bergantung pada beberapa faktor seperti panjang message dan perlu tidaknya penggunaan *Global Title Translation (GTT).*



GAMBAR 2.8[10]

DELAY MESSAGE STP

[10] Ibid, hal. 40

Gambar 2.8 menunjukkan delay waktu maksimum yang diijinkan dalam komponen STP apabila seluruh message panjangnya 15 oktet dan tidak diperlukan **Global Title Translation** (kondisi minimum). Disamping itu juga delay waktu maksimum apabila diperlukan Global Title Translation dan panjang messsage diabaikan (kondisi maksimum).

II.5.3.2. Signaling Connection Control Part (SCCP)

SCCP digunakan untuk memberikan tambahan kemampuan pada **Message Transfer Part (MTP)** agar dapat melakukan transfer informasi baik yang bersifat *connectionless oriented* maupun *connection oriented* antara sentral telepon dengan sentral-sentral khusus dalam jaringan komunikasi dengan menggunakan CCS#7. Untuk connectionless oriented digunakan SCCP class 0 dan 1, sedangkan untuk connection oriented digunakan SCCP class 2 dan 3. MTP sendiri bertugas untuk memberi fungsi overhead seperti signal unit identification, deteksi error, koreksi error dan fungsi-fungsi fisikal/elektrikal.

Dalam aplikasi IN khususnya pada komponen STP, ada dua message SCCP yang paling umum digunakan, yaitu :

- Unit Data Service Message (UDTS)

  Digunakan pada saat terjadi error pada message yang dikirim dan apabila pengirim message tersebut memintanya. Pada banyak

kasus, UDTS tidak dikirim pada saat terjadi error karena memang tidak diminta oleh Service Switching Point (SSP).

- Unit Data Message (UDT)

  Digunakan untuk mentransfer informasi ke pemakai SCCP.

Paket query yang dikirim oleh SSP ke SCP harus dimasukkan dalam message SCCP Unit Data, yang berisi informasi sebagai berikut :

- Label Routing

  Label routing terdiri dari **Destination Point Code (DPC)**, **Originating Point Code (OPC)** dan **Siganling Link Selection (SLS)**. DPC berisi informasi mengenai nomor point code dari node yang akan menerima message tersebut, sedang OPC mengacu pada nomor point code dari node yang mengirimkan message tersebut. SLS digunakan untuk mengidentifikasi signaling link dalam jaringan CCS#7 pada pengiriman message.

- Called Party Address (CdPA)

  CdPA berisi informasi yang diperlukan oleh node penerima message untuk mendistribusikannya ke aplikasi user yang sesuai. CdPA juga diprlukan oleh STP untuk melakukan **Global Title Translation (GTT).**

- Calling Party Address (CgPA)

CgPA menunjukkan node yang pertama kali mengirimkan message dan tempat subsistem number (SSN) dalam node pengirim message. SSN adalah lokasi dalam sistem IN yang menunjukkan tempat suatu aplikasi atau service.

Message Transfer Part	
Destination Point Code Originating Point Code Signaling Link Selection	UDT UDT UDT
Message Type Option Protocol Class	UDT UDT
Pointer to Called Party Addr.	UDT
Pointer to Calling Party Addr.	UDT
Pointer to TCAP	UDT
Called Party Address Field	UDT
TCAP	
Message Transfer Part	

GAMBAR 2.9[11]

STRUKTUR UNIT DATA MESSAGE DALAM MESSAGE CCS#7

[11] Sulistijo, B. Widjajanto, *Advanced Intelligent Network : Arsitektur dan Protokol*, Makalah Presentasi Versis Pusrenbangti PT Telkom, Bandung, 1994, hal. 6

CgPA menunjukkan node yang pertama kali mengirimkan message dan tempat subsistem number (SSN) dalam node pengirim message. SSN adalah lokasi dalam sistem IN yang menunjukkan tempat suatu aplikasi atau service.

Message Transfer Part	
Destination Point Code Originating Point Code Signaling Link Selection	UDT UDT UDT
Message Type Option Protocol Class	UDT UDT
Pointer to Called Party Addr.	UDT
Pointer to Calling Party Addr.	UDT
Pointer to TCAP	UDT
Called Party Address Field	UDT
TCAP	
Message Transfer Part	

GAMBAR 2.9[11]

STRUKTUR UNIT DATA MESSAGE DALAM MESSAGE CCS#7

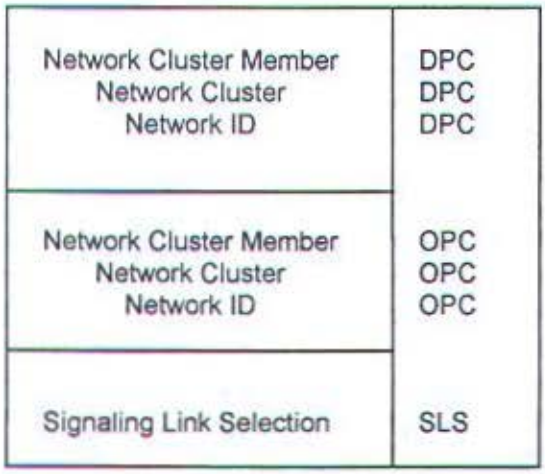
---

[11] Sulistijo, B. Widjajanto, *Advanced Intelligent Network : Arsitektur dan Protokol*, Makalah Presentasi Versis Pusrenbangti PT Telkom, Bandung, 1994, hal. 6

- TCAP Portion

Bagian ini berisi data yang akan ditransfer ke protokol TCAP.

Routing SCCP terdapat dalam routing label yang terdiri DPC, OPC dan SLS. DPC dan OPC terdiri dari bagian-bagian yang sama, yaitu *network ID* yang akan menunjukkan arah message ke jaringan CCS#7 tertentu. Dalam suatu lingkungan multi operator network ID biasanya menunjuk jaringan CCS#7 yang dimiliki operator tertentu. Network cluster mengidentifikasi suatu grup terdiri



GAMBAR 2.10[12]

LABEL ROUTING SCCP

[12] Ibid, hal. 8

beberapa *signaling point* dalam jaringan CCS#7. **Network Cluster Member** merupakan nomor unik dari satu *signaling point.*

Field **called party address** pada SCCP menambah kemampuan routing di atas label routing. Tambahan kemampuan tersebut adalah pelaksanaan proses Global Title Translation di tingkat STP. *Called party address* mempunyai satu *octet* yang menunjukkan tipe data yang tersimpan dalam field address dan bagaimana node intermediate (STP) penerima message harus melakukan routing. *Octet* ini disebut **Address Indicator**. Called party address juga berisi signaling point code, nomor subsistem (SSN) dan *translation type* atau *global title value.*

Calling party address berisi informasi mengenai node yang pertama kali mengirimkan message SCCP. Seperti CdPA, CgPA mempunyai address indicator yang menunjukkan tipe data yang berada dalam field ini. CgPA adalah return adress suatu message (dapat dibayangkan sebagai pengirim dalam surat/pos). Setiap respons atau error yang terjadi pada suatu message harus dikembalikan pada alamat yang tercantum dalam CgPA. Biasanya, CgPA terdiri dari signaling point code dan SSN dari node yang pertama kali mengirimkan SCCP message.

Perbandingan antara CdPA dan CgPA dapat dilihat pada gambar berikut :

Address Indicator	SSN tersedia, TT/GTV tersedia routing dengan GTT, coding nasional / internasional
SSN - atau berbasis aplikasi	
TT - berbasis informasi	
GTV - berbasis informasi trigger	

GAMBAR 2.11[13]

SCCP CALLED PARTY ADDRESS

Address Indicator	SSN tersedia, TT/GTV tersedia routing dengan GTT, coding nasional / international
SSN - Aplikasi tempat Message SCCP pertama kali dikirim	
GTV - Point code SSP yang melakukan query	

GAMBAR 2.12[14]

SCCP CALLING PARTY ADDRESS

Subsistem Number (SSN) secara unik menentukan fungsi aplikasi user yang terdapat dalam node jaringan. Aplikasi user tersebut dapat melakukan suatu proses tertentu seperti memberikan manajemen jaringan atau

---

[13] logcit.

[14] Ibid. hal. 9

mentranslasikan data spesifik dari suatu service. Di Amerika, Komite Standard T1 ANSI telah mendefinisikan penomoran SSN dan nomor yang telah didefinisikan tersebut tidak direkomendasikan untuk digunakan pada aplikasi lain. Pengguna ulang SSN bisa mengakibatkan masalah alarm interworking antar service yang diberikan oleh operator yang berbeda.

STP menentukan message routing untuk aplikasi-aplikasi yang menggunakan SCCP. Saat STP menerima message yang memerlukan routing khusus, STP akan melihat SCCP callled Party Address untuk menentukan bagaimana cara me-route message tersebut. Dalam banyak kasus, Global Title Translation diperlukan oleh STP untuk menentukan tujuan message selanjutnya. Untuk routing yang memerlukan global title, translation type pada field global title akan digunakan oleh STP untuk menemukan tabel translasi yang sesuai.

II.5.4. Service Switching Point (SSP)

Service Switching Point (SSP) berguna sebagai titik akses untuk pemakai layanan dan melaksanakan pelayanan yang padat (seperti penjelasan pada SCP). Pada IN/1 tidak didapatkan "user programmability" di SSP. SSP dibuat oleh produsen switch tradisional. TCAP (Transaction Capability Application Part) dipakai untuk menghubungkan SSP dan SCP.

Service Switching Point adalah komponen IN yang bertindak sebagai access point bagi service user. Dengan fungsi SSP, sentral dapat mengakses database pada SCP untuk membangun pelayanan IN. Kapabilitas SSP terletak

pada sentral telepon biasa yang merupakan perangkat keras dan lunak untuk melakukan pemrosesan panggilan IN. SSP mampu mendeteksi kondisi-kondisi yang memerlukan service logic yang dibutuhkan untuk melengkapi suatu panggilan IN dan merupakan node yang memulai komunikasi dengan SCP tempat service logic yang diperlukan oleh suatu panggilan.

II.5.4.1. Fungsional SSP

Service Switching Point (SSP) berkomunikasi dengan satu atau lebih Service Control Point (SCP) melalui *signaling transfer point* dengan menggunakan protokol CCS#7. Elemen-elemen yang membangun komponen SSP dikelompokkan dalam :

- Application parts, yang menggambarkan service yang tersedia
- TCAP, sebagai protokol pembawa data ke SCP
- Lapisan Jaringan, biasanya digunakan SCCP

Fungsi-fungsi yang dijalankan oleh SSP meliputi :

- Melakukan pemrosesan pemanggilan

  SSP adalah sentral telepon yang dapat mengenali panggilan yang memerlukan pemrosesan IN. Bila panggilan IN diterima, SSP akan menunda pemrosesan panggilan untuk sementara waktu dan melakukan query ke arah SCP. SCP kemudian akan memberi tahu SSP bagaimana proses panggilan dapat dilakukan.

- Melakukan triggering

  Triggering adalah suatu proses identifikasi panggilan yang memerlukan penanganan IN. Berdasarkan triggering tersebut, SSP akan menunda proses panggilan. SSP dapat mengenali beberapa macam triggering yang terdapat dalam suatu tahap pemrosesan panggilan.

- Automatic Call Gapping

  Setelah mendeteksi trigger dari suatu panggilan, SSP akan memeriksa kontrol call gapping yang berguna untuk mencegah SCP overload. Bila kontrol call gapping diminta oleh SCP maka SSP akan melakukan terminasi atas panggilan tersebut. Apabila tidak, SSP akan melakukan proses *query* ke SCP.

- Melakukan *query*

  Query adalah proses pengisian message *query* yang terdapat dalam protokol **Transaction Capabilities Application Part (TCAP)** dan pengiriman message tersebut ke SCP. Isi dari message *query* tersebut tergantung pada jenis trigger yang sesuai dengan profil service dan parameter panggilan.

- Interaksi dengan pemanggil

  SCP bisa meminta SSP untuk menyediakan informasi tambahan dari pemanggil dengan menggunakan message TCAP **"Conversation with Permission"**. Apabila hal ini terjadi, SSP (melalui Intelligent Peripheral) akan meminta pelanggan

memasukkan informasi yang diminta dan mengirimkan informasi tersebut ke SCP dengan memakai message TCAP **"Conversation"**.

- Aktivasi/Deaktivasi Trigger

  SCP bisa memerintahkan SSP untuk mengaktivasi atau mendeaktivasi trigger pelanggan dengan menggunakan message TCAP **"Query"** atau **"Conversation"**. Seteleh menerima perintah tersebut SSP akan menjawab dengan message **"Response"** (apabila perintah dalam message Query) atau **"Conversation"** (apabila perintah dalam message Conversation) untuk mengindikasikan bahwa aktivasi atau deaktivasi telah berhasil dilakukan.

- Pemrosesan respons

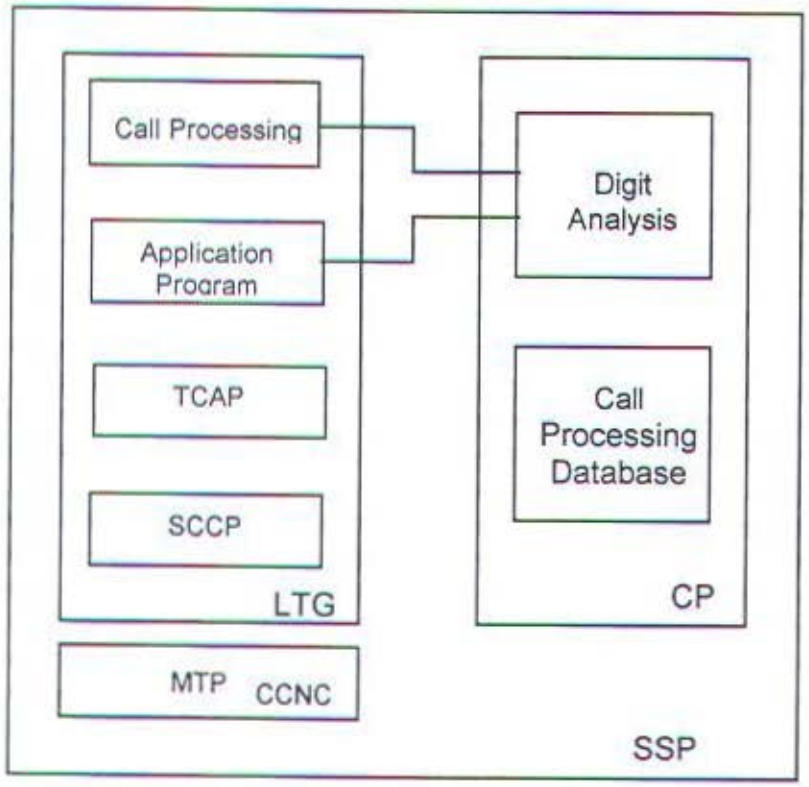
  Pemrosesan respons adalah penginterpretasian dan pelaksanaan perintah yang terdapat di dalam message TCAP yang diterima dari SCP. Perintah SCP bisa berupa routing panggilan, pemberian pengumuman (announcement) ke pemanggil atau memberikan terminasi khusus pada suatu panggilan.

- Notifikasi terhadap terminasi

  Message respons dari SCP bisa mengandung perintah kepada SSP untuk melapor pada SCP apabila panggilan telah berakhir. Apabila hal ini terjadi, SSP akan memberikan notifikasi akhir dari suatu panggilan ke SCP dengan menggunakan message TCAP **"Undirectional"**.

- Monitor resource

SCP bisa memerintahkan SSP untuk memonitor status suatu fasilitas dengan message TCAP "**Query**". Jawaban SSP atas perintah tersebut dimasukkan di dalam message TCAP "**Conversation**" dan "**Response**".

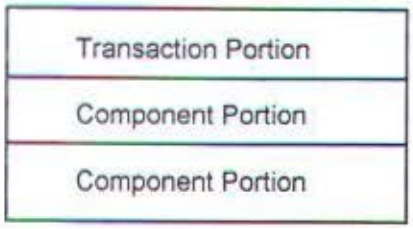


GAMBAR 2. 13[15]
KOMPONEN-KOMPONEN SSP

[15] Ambrosch, W.D., Maher A., Sasscer B., opcit. hal. 96

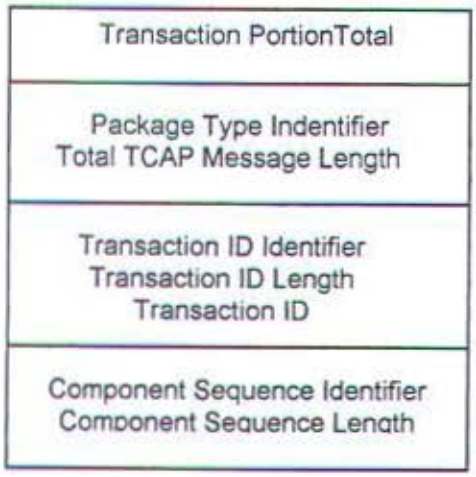
II.5.4.2. Transaction Capabilities Application Part (TCAP)

Dalam protokol CCS#7, TCAP bertugas sebagai pembawa data yang dipertukarkan antara SSP dengan SCP. Posisi TCAP dalam suatu message CCS#7 dapat dilihat pada gambar 2.9. TCAP portion dalam suatu message CCS#7 terdiri dari *transaction portion* dan beberapa *component portion*.



GAMBAR 2.14[16]

FORMAT DASAR TCAP



GAMBAR 2. 15[17]

ELEMEN TRANSACTION PORTION

---

[16] Sulistijo, B. Widjajanto, opcit. hal. 10

[17] logcit.

Transaction Portion merupakan bagian TCAP yang berisi informasi untuk identifikasi tipe data, panjang data dan data identifier. Isi transaction portion adalah :

- Package Type Identifier
- Total TCAP Message Length
- Transaction ID Identifier
- Transaction ID Length
- Transaction ID
- Component Sequence Identifier
- Component Sequence Length

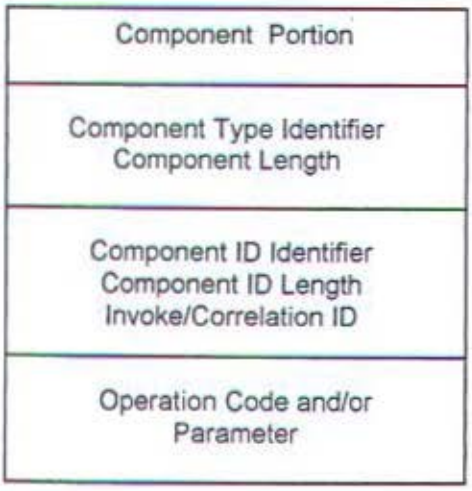
Message-message yang dioperasikan dalam portion ini diantaranya :

- **Undirectional message**, yang dikirim ke satu arah dan tidak diharapkan adanya jawaban (misalnya informasi mengenai status).
- **Query with Permission**, message TCAP yang digunakan untuk memulai sesuatu transaksi yang memberi tahu node penerima untuk mempersiapkan proses transaksi (misalnya permintaan translasi nomor).

- **Response**, suatu pesan untuk menutup suatu transaksi tertentu (misalnya jawaban dari suatu *query*).
- **Conversation with Permission**, kelanjutan dari suatu transaksi TCAP dengan mengijinkan adanya release (pembebasan hubungan).
- **Abort**, untuk memberitahukan kepada penerima bahwa pengirim melakukan terminasi atas transaksi tertentu.

Component Portion berisi informasi yang dibutuhkan oleh node penerima untuk menyelesaikan operasi. Setiap component portion merupakan satu set instruksi yang unik. Karena adanya kemungkinan satu message yang memiliki beberapa component portion, maka setiap component portion dibedakan dengan identifier. Isi component portion adalah :

- Component Type Identifier
- Component Length
- Component ID Identifier
- Component ID Length
- Invoke/Correlation ID
- Operation Code Identifier (Invoke only)
- Parameter Identifier



GAMBAR 2. 16[18]

ELEMEN COMPONENT PORTION

Component Portion merupakan basic building block dari message TCAP dan setiap *Component Portion* melakukan fungsi yang berbeda-beda, yaitu :

- **Invoke**, memulai suatu operasi tertentu, seperti translasi nomor pada data base.
- **Return Result**, mengembalikan hasil operasi invoke.
- **Return Error**, menunjukkan kesalahan yang terjadi pada suatu operasi yang tidak dapat dijalankan.

[18] Ibid. hal. 11

- **Reject**, menunjukkan alasan mengapa suatu komponen tidak dapat dijalankan.

- **Last/Not Last**, mengindikasikan apakah komponen tersebut merupakan suatu response terhadap suatu invoke.

Untuk melakukan routing antar node dan isi data dalam message yang saling dipertukarkan antara SSP dengan SCP digunakan protokol interface. Dalam prosedur normal (tidak terjadi error) message yang dipertukarkan antara SSP dengan SCP dapat dikategorikan :

- **Switch call related message**

  Message ini dikirimkan oleh SSP kepada SCP sebagai laporan bahwa SSP telah mendeteksi adanya trigger event.

- **SCP call related message**

  SCP call related message dikirimkan oleh SCP ke SSP untuk memerintahkan SSP melakukan suatu tugas tertentu. Message kategori ini dapat berupa message SCP Respons atau message Event.

- **SCP request message**

  Message kategori ini juga merupakan message "*non-call related*" dan dikirim SCP ke SSP untuk menanyakan informasi yang releven dengan SCP.

- **Switch response message**

  Message ini juga merupakan "non-call related" dan dikirim oleh SSP sebagai jawaban atas SCP request message.

- **Multiple-component message**

  Message ini terdiri dari lebih dari satu komponen TCAP dan digunakan apabila SCP ingin mengirimkan SCP response message bersamaan dengan SCP request message.

II.5.5. Intelligent Peripheral (IP)

Intelligent Peripheral (IP) menyediakan layanan-layanan tambahan, dikendalikan oleh SSP dan SCP. IP lebih ekonomis bila dipakai bersama, karena tidak semua kemampuan di IP ada di SSP atau terlalu mahal untuk memasukkan semuanya di SSP. Berikut adalah contoh fungsi IP :

- Pemberitahuan-pemberitahuan
- Sintesa Pembicaraan
- Pesanan-pesanan Suara
- Pengenalan Pembicaraan
- Informasi Database yang dapat dicapai end user.

IP biasanya diakses dari SSP melalui basis sirkuit atau paket seperti ISDN.

II.5.6. Vendor Feature Node (VFN) atau Service Provider (SP)

Vendor Feature Node (VFN) ada di luar jaringan. VFN dimiliki dan diatur oleh pelanggan. VFN menyediakan beberapa layanan seperti untuk IP dan dapat dihubungkan melalui sambungan CCS#7. Namun hubungan demikian memakai filter logic yang menghalangi VFN menggunakan pesan-pesan CCS#7 yang dapat mengganggu operasi jaringan.

II.6. MODEL PENGENALAN

Keanekaragaman jaringan telekomunikasi di berbagai negara secara langsung berarti juga terdapatnya berbagai konfigurasi teknologi, demografi pelayanan dan topografi subscriber. Sebagai suatu bentuk evolusi jaringan komunikasi, IN memiliki perbedaan dibanding jaringan konvensional. Karena itu diperkenalkan suatu strategi dalam pengenalan teknologi IN secara luas untuk memudahkan dan menyebarluaskan penggunaannya dengan didasarkan pada konfigurasi jaringan yang telah ada dan kebutuhan jasa pelayanan sebagai tujuan implementasi IN.

Strategi pengenalan teknologi IN diharapkan akan mampu mengoptimalkan sasaran-sasaran berikut :

a) meningkatkan pelayanan yang ada bagi pengguna jasa

b) tersedianya pelayanan yang lebih maju yang dibutuhkan para user

c) meningkatkan kemudahan dan profit bagi Network Operator

d) persaingan kompetitif diantara Network Operator guna meningkatkan pelayanan

e) penggunaan hardware dan software yang standar (produk dari Network Product Supplier)

f) sebagai kontrol evaluasi tercapainya sasaran-sasaran tersebut diperlukan adanya model-model kapabilitas jaringan

II.6.1. Unsur Model

II.6.1.1. Kategori Pelayanan (Services Category)

Strategi pengenalan Jaringan Pintar (IN) dipengaruhi oleh karakteristik pelayanan. Pelayanan-pelayanan yang akan diimplementasikan dapat dikategorikan sebagai berikut :

a. A-B Number (called number)

Pelayanan kategori ini hanya memerlukan informasi mengenai nomor tujuan panggilan tanpa memperhatikan asal datangnya panggilan tersebut. Untuk kategori ini pelayanan relatif lebih mudah pengenalannya dibanding kategori yang lain.

b. (A+B) Number Services

Dalam kategori ini selain nomor yang dituju diperlukan data tentang sumber atau arah datangnya panggilan tersebut. Pada kategori ini mulai dibutuhkan penetrasi CCS#7 dalam jaringan, atau penggunaan kapabiltas pensinyalan yang lain seperti Automatic Number Identification (ANI).

Contoh pelayanan dalam kategori ini :

- Emergency Response Service seperti panggilan 911
- Alternate Billing Service

c. Interactive Service

Pelayanan kategori ini lebih kompleks dibanding dua kategori yang disebutkan sebelumnya. Selain kebutuhan akan nomor panggilan yang dituju dan arah datangnya panggilan juga diperlukan data pendukung lain sesuai karakteristik service seperti password untuk akses, nomor calling card dan pesan-pesan khusus.

Contoh pelayanan dalam kategori ini :

- Calling Card Number
- Interactive Freephone

Sedangkan untuk melaksanakan fungsi pelayanan ini diperlukan :

- komponen Intelligent Peripheral (IP) atau Vendor Feature Service (VFN)
- kapabilitas pensinyalan seperti MF atau ISDN
- fungsi-fungsi yang ada pada kategori (A+B) Number Service

II.6.1.2 Jaringan Sentral (Network Base)

Model-model konfigurasi jaringan meliputi :

a. Model C1

Model ini besifat konvensional tanpa pemakaian CCS#7. Konfigurasi ini merupakan gabungan switching dan transmisi digital dan analog dan banyak dipakai dewasa ini.

b. Model C2

Pada model ini mulai digunakan CCS#7 untuk sentral tandem. Konfigurasi ini didasarkan pada C1 namun telah mengalami

pengembangan dengan implementasi CCS#7 tersebut. Model C2 ini merupakan tahap peralihan dari bentuk C1 yang konvensional menuju bentuk C3 yang berbasis ISDN.

c. Model C3

Penggunaan CCS#7 telah mencapai sentral lokal dan tandem pada skala lebih besar dengan tambahan kapabilitas dari ISDN. Konfigurasi ini merupakan pengembangan dari C2.

II.6.1.3 Akses Jaringan Pengguna Jasa (Network Services User Access)

Model akses jaringan pengguna jasa dibedakan :

1. akses POTS non ISDN, seperti MF
2. akses dengan basis ISDN

Peralatan konvensional lebih banyak digunakan meskipun saat ini telah dikenalkan ISDN. Namun demikian sentral non ISDN dapat diekuivalenkan sebagai sentral ISDN dengan penerapan CCS#7.

ISDN sendiri dimanfaatkan untuk daerah bisnis yang sering memerlukan feature khusus dari pelayanan IN. Dalam hal ini IN bertindak sebagai arsitektur kontrol pelayanan sedangkan ISDN adalah arsitektur kontrol untuk aksesnya.

Namun keduanya saling mendukung satu sama lain walaupun tidak dihubungkan secara langsung.

II.6.2. Skenario Pengenalan

Untuk mempersiapkan pelayanan IN dengan akses ISDN tidak diperlukan jaringan yang kompleks karena adanya penerapan CCS#7, kecuali untuk feature-feature tertentu dari IN yang sangat variatif.

Untuk peralatan konvensional, strategi pengenalan yang paling mudah adalah untuk kategori A B-Number Services. Namun secara umum dapat dikatakan bahwa usaha pengenalan teknologi IN akan lebih ditekankan pada penetrasi CCS#7. Hal penting yang masih harus dipertimbangkan adalah pilihan untuk menyediakan pelayanan bagi segmen POTS yang memerlukan investasi besar namun memiliki pasar yang luas atau penyediaan bagi pengguna ISDN yang pasarnya lebih kecil dengan investasi yang dikeluarkan lebih kecil pula.

Gambaran skenario pengenalan teknologi IN dapat dilihat pada tabel.

TABEL 2.1[19]

EVOLUSI SKENARIO PENGENALAN IN

Access Type	Service Category	C1	C2	C3
POTS	B Number	* Introduce C2	Basis Exist	Basis Exist
	(A+B) Number	* Introduce C2 * Introduce A forwarding/C3	* Introduce A forwarding/C3	Basis Exist
	Interactive	* Introduce C2 * Introduce A forwarding/C3 * Introduce IP / VFN	* Introduce A forwarding/C3 * Introduce IP / VFN	* Introduce IP/VFN
ISDN	B Number	* Introduce C2	Basis Exist	Basis Exist
	(A+B) Number	* Introduce C2	Basis Exist	Basis Exist
	Interactive	* Introduce C2 * Introduce IP / VFN	* Introduce IP / VFN	* Introduce IP/VFN

* Bila sentral adalah ISDN

II.7. TOPOLOGI JARINGAN

Dalam jaringan komunikasi yang konvensional, pengontrolan routing

---

[19] Ibid. hal. 18

dan feature jasa pelayanan dilakukan di sentral switchingnya. Satu kerugian dari sistem ini untuk beberapa jasa pelayanan adalah bahwa data pemakai jasa harus digandakan di setiap sentral tersebut. Dengan makin meningkatnya jasa pelayanan maka sistem pun makin menjadi kompleks. Permasalahan ini dijawab dengan hadirnya teknologi Jaringan Pintar (*Intelligent Network*) yang memudahkan administrasi jaringan dengan melakukan sentralisasi pengelolaan sehingga menekan biaya implementasi.

Jaringan Pintar (IN) sebagai suatu arsitektur pengontrolan jasa pelayanan pada jaringan komunikasi memiliki keunggulan dibanding jaringan konvensional dalam hal kemampuannya menyediakan sistem yang memudahkan *Network Operator* untuk memperkenalkan, mengontrol dan memanajemen jasa pelayanan komunikasi secara lebih efektif, ekonomis dan cepat.

II.7.1. Arsitektur Jaringan Pintar (IN)

Secara umum arsitektur Jaringan Pintar bertujuan untuk memungkinkan perubahan dan peningkatan jumlah serta pengembangan jasa pelayanan baru. Hal ini ini terutama dirasakan di daerah dengan kebutuhan jasa pelayanan yang tinggi sedangkan untuk daerah lain, IN dijadikan dasar bagi pengembangan sistem telekomunikasi, baik untuk jangka waktu pendek maupun jangka panjang.

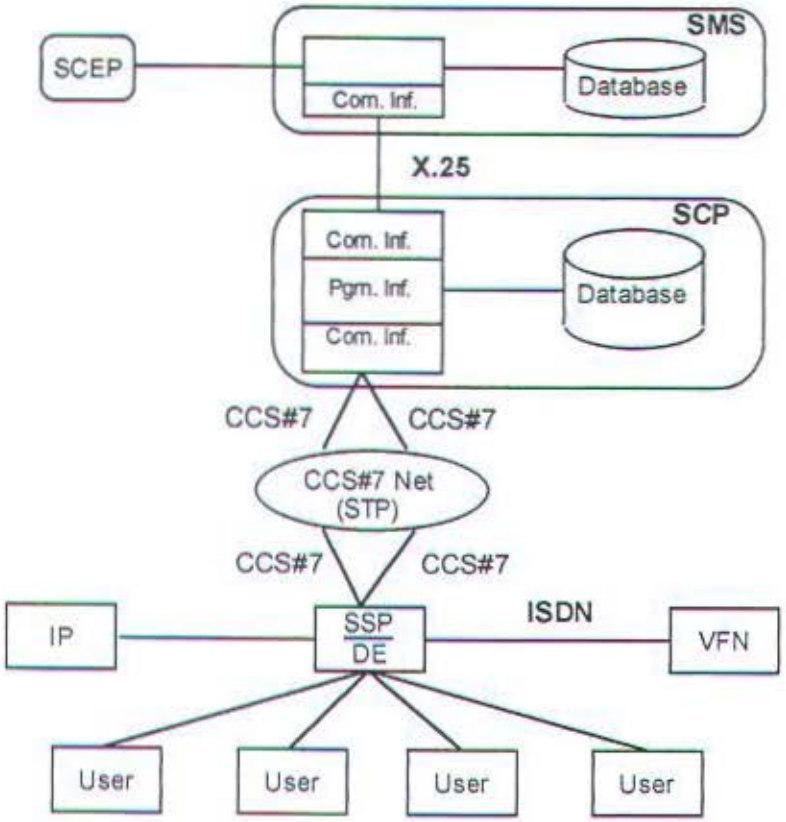
Feature teknik yang harus ada dalam arsitektur Jaringan Pintar (IN) adalah :

- Hubungan kontrol jaringan yang bersifat intelijen pada sentral. Node ini dinamakan **Service Control Point (SCP)**
- Node yang melakukan fungsi switching dengan dikontrol oleh SCP. Node ini adalah **Service Switching Point (SSP)**
- Interface jaringan yang standar, seperti CCS#7 dan ISDN. Interface ini akan memacu persaingan antara penyedia jaringan dan penyedia pelayanan untuk memberikan pelayanan yang terbaik.
- Kemampuan melakukan kreasi service dengan cepat dan ekonomis.

II.7.1.1. Tinjauan Teknik Jaringan Pintar

Keunggulan dari Jaringan Pintar (IN) adalah kemampuannya untuk mengelola eksekusi sentral pelayanan lewat suatu komponen kecil IN yaitu **Service Control Point (SCP)**. SCP dihubungkan ke sentral jaringan (yang dinamakan Service Switching Point - SSP) melalui suatu *interface* standar CCS#7. SSP akan melakukan deteksi pada saat SCP menangani suatu pelayanan. SSP menyalurkan suatu pesan (TCAP) yang berisi informasi service yang bersangkutan. Melalui TCAP ini **service control logic** dalam SCP mengarahkan SSP untuk membentuk fungsi khusus sesuai service yang dimaksud, seperti menghubungkan ke nomor subscriber.

Gambaran teknik fungsi dan kontrol dalam IN ditunjukkan seperti gambar 2.17 di bawah ini :



GAMBAR 2. 17[20]

GAMBARAN TEKNIK IN

Keterangan gambar :

SMS : Service Management System

SCP : Service Control Point

SSP : Service Switching Point

IP : Intelligent Peripheral

VFN : Vendor Feature Node

---

[20] Ambrosch, W.D., Maher A., Sasscer B., opcit. hal. 8

Com. Inf. : Communication Interface

Pgm. Inf. : Program Interface

DE : Digital Exchange

SCEP : Service Creation Environment Point

Karakter utama **Intelligent Network (IN)** adalah ketersediaan satu atau lebih **Service Control Point (SCP)** dimana SCP merupakan **Physical Entities (PE)** yang terletak terpusat, yang berisi **Service Logic Program (SLP)** dan digunakan untuk menyediakan pelayanan IN. Fungsi-fungsi SCP disebut sebagai **Service Control Function (SCF)**. SCF mampu untuk menginterogasi **Service Data Function** dalam suatu data base (SDP), yang berisi data yang digunakan oleh SCP untuk menyediakan pelayanan-pelayanan yang berdiri sendiri. SCP juga diinterkoneksikan oleh CCS#7 dengan satu atau lebih **Service Switching Point (SSP)** menurut protokol yang telah distandarkan (INAP). SSP umumnya sentral ISDN atau sentral digital yang dilengkapi dengan **Service Switching Function (SSF)** serta normal **Call Control Function (CCF)**. SSF mendeteksi kondisi-kondisi trigger pada proses penyambungan normal.

Pada saat SSF menemui suatu trigger, yang menunjukkan bahwa pelayanan telah diminta, suatu pertanyaan (*query*) standar kemudian dikirimkan ke SCF, untuk memproses permintaan pelayanan tersebut. SCF menerima, mengkode balik, dan menterjemahkan pertanyaan tersebut dalam konteks pelayanan yang didukung *Capability Set - 1 (CS-1)*. SCF memformulasikan, mengkodekan dan mengirimkan tanggapan standar ke SSF. Formulasi tanggapan dapat melibatkan logic pelayanan kompleks, yang membawa ke

penterjemahan dan permintaan prompt dan mengumpulkan digit-digit tambahan dari pihak pemanggil dengan menggunakan pelayanan **Specialized Resource Function (SRF)** yang ada dalam **Intelligent Peripheral (IP)**.

SSF menerima, mengkode balik dan menterjemahkan tanggapan dari SCF. SSF kemudian memberikan instruksi eksplisit ke CCF tentang cara menyelesaikan proses membangun hubungan.

SRF dan IP umumnya diperlukan untuk penyesuaian pelayanan. SRF juga mendukung interaksi informasi yang fleksibel antara pemakai dan jaringan. Contoh dari komponen khusus yang mungkin adalah pemberitahuan untuk pengumpulan digit-digit DTMF yang diperlukan dalam penyelenggaraan pelayanan **Credit Card Calling**.

Arus informasi pada pelayanan IN yang dimulai pada waktu pemakai meminta pelayanan, dapat dijelaskan dengan pembahasan suatu contoh, yaitu pelayanan 800 atau *Freephone*. Akses pemakai ke pelayanan dengan memutar/menekan 800 S1S2 ... Sm (Digit-digit S1S2 ... Sm di belakang kode akses 800 adalah fiktif). Sentral yang diakses mengenali kode akses dan mentransfer nomor yang diputar/ditekan (akhirnya dengan nomor pemanggil) ke SSF. SSF kemudian mengirim pertanyaan (*query*) ke SCF. Setelah menerima *query*, SCF menginterogasi SDF untk memperoleh nomor direktori yang berkaitan dengan S1S2 ... Sm (Misal : ABCN1N2 ... Nm).

SCF mengirim balik nomor direktori sebagai tanggapan ke SSF. SSF, melalui CCF, kemudian mulai membangun hubungan ke tujuan yang

dikehendaki. Untuk advanced service 800, penterjemahan dari nomor 800 ke nomor direktori dapat tergantung dari waktu, tanggal dan nomor pemanggil. Parameter-parameter tersebut juga dapat dimodifikasi oleh pelanggan pelayanan melalui **Service Management Point (SMP)**, yang diperkirakan dengan suatu **Service Management Function (SMF)**.

SMP juga menjadi platform untuk penciptaan pelayanan baru. Sebagai alternatif, pelayanan dapat dibuat dalam bagian fisik yang terpisah yang disebut **Service Creation Environment Point (SCEP)** yang dilengkapi dengan suatu **Service Creation Environment Function (SCEF)**. SCEF yang berinteraksi langsung dengan SMF, memberikan peluang untuk menciptakan pelayanan (baru) secara mudah dengan menggunakan **Service Independent Building Blocks (SIBs)**. SCEF kemudian memasukkan pelayanan baru tersebut ke SMF. Kemampuan operator jaringan untuk menciptakan pelayanan (baru) merupakan salah satu faktor kunci bagi berhasilnya penyelenggaraan IN.

SMF juga mencakup fungsi-fungsi untuk pengawasan dan pengujian, manajemen trafik jaringan, dan pencatatan data untuk *charging*. Oleh karena itu SMF harus mampu mengakses semua FE lain dari IN.

Sasaran jangka panjang IN adalah kemampuan untuk meluncurkan jasa pelayanan baru atau mengubah yang telah ada secara cepat tanpa harus melakukan adaptasi pada perangkat lunak SSP secara menyeluruh. Penyesuaian kecil yang akan dilakukan dikonfirmasikan ke SCP. Sasaran itu akan dicapai secara bertahap, sebagai berikut :

a. Tahap 1 IN/1

IN/1 memerlukan penyesuaian dalam SSP dan SCP untuk mengantisipasi peluncuran jasa pelayanan baru. Suatu bentuk jasa pelayanan yang merupakan tipikal dari IN/1 adalah *Virtual Private Network (VPN)*. Peralihan dari IN/1 ke IN/2 ditandai dengan perubahan pada SSP untuk mengakomodasi jasa pelayanan baru.

b. Tahap 2 IN/2

Dengan penerapan IN/2 tidak diperlukan lagi pengubahan pada perangkat lunak SSP ketika dilakukan peluncuran jasa pelayanan baru. IN/2 memiliki kemampuan dalam mentrigger SSP untuk mengijinkan SCP menangani permintaan pelayanan atau untuk menanganinya sendiri. SCP dan SSP memiliki elemen pelayanan dasar misalnya penyambungan dan pemutusan saluran. SCP juga berisi data-data yang relevan dengan service yang diperlukan. Elemen pelayanan dasar ini dikenal dengan istilah **Functional Components (FCs)** sebagai tahap awal pembangunan jasa pelayanan.

II.7.1.2. Topologi Jaringan Pintar (IN)

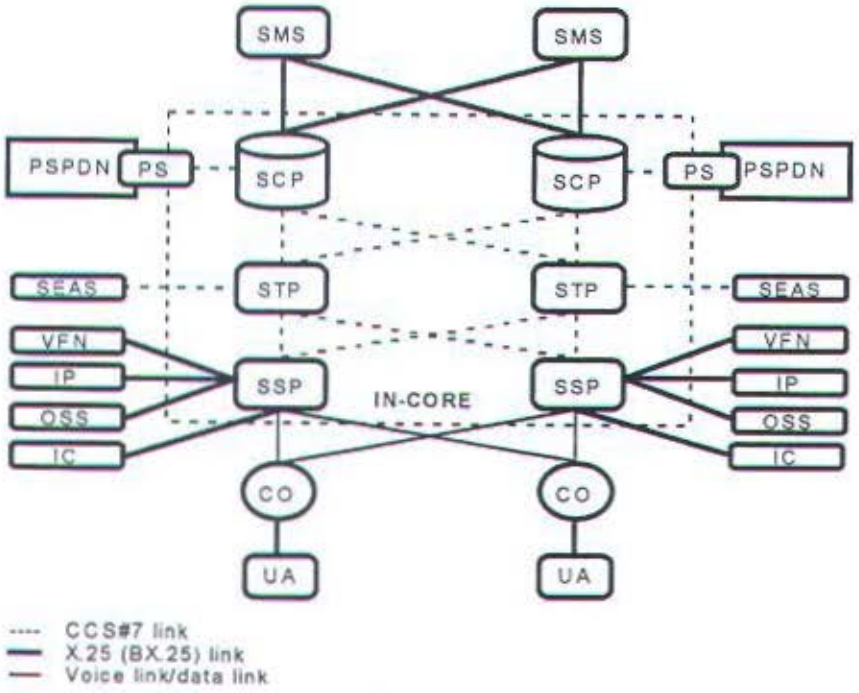
Jaringan Pintar (IN) terdiri dari beberapa elemen jaringan yang memiliki kemampuan untuk mengidentifikasi panggilan yang berkaitan dengan pelayanan IN. Setiap elemen jaringan ini memiliki fungsi yang berbeda dan mempunyai metode yang berbeda pula dalam melakukan komunikasi dengan jaringan telekomunikasi.

II.7.1.2.1. Komponen Jaringan

Komponen-komponen yang membangun Jaringan Pintar (IN) dibedakan kedalam dua golongan, yaitu :

1) Jaringan Inti (Core Network)
2) Jaringan Peripheral (Peripheral Network)

Secara skematis komponen-komponen tersebut dapat digambarkan pada gambar 2.18.



GAMBAR 2.18[21]

KOMPONEN-KOMPONEN IN DAN HUBUNGAN ANTARMUKA

[21] Ibid. hal. 71

Keterangan gambar :

- Service Control Point (SCP)
- Service Transfer Point (STP)
- Service Switching Point (SSP)
- Service Management System (SMS)
- Vendor Feature Node (VFN)
- Intelligent Peripheral (IP)
- Signaling Engineering and Administration System (SEAS)
- Operating Support System (OSS)
- Interexchange Carrier (IC)
- Packet Switched Public Data Network (PSPDN)
- Packet Switch (PS)
- Central Office (CO)
- User Access (UA)

Komposisi komponen IN secara individual dapat diuraikan sebagai berikut:

a. SSP menggunakan produk standar *hardware* dan *software EWSD*, seperti sentral lokal dan sentral tandem yang dilengkapi CCS#7, dengan dukungan subsistem sebagai berikut :

- SSP triggers
- SSP application part

- Signal Connection Control Part (SCCP)
- Transaction Capabilities Application Part (TCAP)

b. STP menggunakan produk standar hardware dan software EWSD, pada arsitektur jaringan dilengkapi subsistem :

- Signal Connection Control Part (SCCP) class 0 dan 1

c. SCP menggunakan produk standar *hardware* dan *software EDP*, seperti IBM/370, PS/2, Siemens 7.5xx dengan dilengkapi subsistem sebagai berikut :

- Software Signal Connection Control Part (SCCP)
- Software Transaction Capabilities Application Part (TCAP)
- Interface hardware dan software SMS/OSS
- Hardware dan software dengan fungsi CCS#7
- Software Node Manager
- Software platform aplikasi
- Software aplikasi

d. SMS sebagai sistem administrasi jaringan dengan menggunakan **Operation Systems Network Interface (OSNI)**. Komponen SMS dan aplikasinya bersifat spesifik pada tiap negara.

II.7.1.2.2. Syarat-syarat Unjuk Kerja

Unjuk Kerja jaringan ditunjukkan dengan **Call Setup Time (CST)** yaitu periode waktu antara selesainya proses dialing secara keseluruhan sampai diterimanya nada ringing (*audible ringing*). Oleh karena kapasitasnya yang lebih besar dibanding sistem pensinyalan lain, CCS#7 mampu menekan **Call Setup Time** ini. Namun dipihak lain model pengenalan arsitektur IN cenderung memperbesar CST. Hal ini disebabkan oleh beberapa hal, diantaranya :

- Sistem pengiriman *virtual number* ke SSP dalam model *network base* C2, dimana jaringan CCS#7 hanya tersedia pada sentral tandem.
- SSP mendeteksi panggilan khusus (*virtual number*), mendeteksi *table trigger*, dan *query* data untuk melengkapi pembangunan panggilan. Periode waktu maksimal antara pengiriman *query* tersebut dari SSP ke SCP sampai diperoleh respons adalah 3 detik. Bila diperlukan dialog antara SSP dan SCP, maka waktu respons mencakup waktu untuk satu step dialog tersebut.
- CCS#7 melakukan routing *query* ke SCP dan merespon kembali ke SSP menggunakan satu atau lebih STP, bergantung pada topologi CCS#7. Delay yang diijinkan untuk proses di STP ini 20-100 ms, tergantung panjang pesan (message) dan proses penterjemahan yang dilakukan di SSP. Bila terjadi kegagalan, disediakan toleransi waktu 100-400 ms, sedangkan delay transmisi dalam CCS#7 dapat diabaikan.

- Untuk SCP yang dihubungkan ke CCS#7, proses interogasi data pelayanan dan penyaluran pesan respons ke saluran CCS#7 serta waktu respons untuk tiap dialog, tidak lebih dari 1 detik. Waktu ini dihitung sejak pesan diterima di SCP sampai disalurkan ke saluran CCS#7. Sedangkan waktu respons untuk service subscriber dipengaruhi oleh interface service subscriber itu ke SMS dan interface antar SMS-SCP.
- Interface subscriber ke SMS adalah interface dialog dengan persyaratan waktu respons yang sama seperti sistem informasi dan manajemen yang lain, seperti waktu respons untuk transaksi minor (perubahan menu dan permintaan informasi pelayanan) yang membutuhkan waktu 1 detik. Waktu respons untuk update informasi pelayanan tergantung pada kompleksitasnya, umumnya kurang dari 15 detik.
- Waktu respons untuk penerimaan pesan SMS di SCP adalah 8 detik.
- Diperlukan fungsi untuk menginformasikan update pelayanan dari SMS ke SCP. Delay waktu antara input dari service subscriber sampai tersedianya update data di SCP database adalah 15 menit.

Dengan berbagai persyaratan yang harus dipenuhi untuk operasi jaringan, diharapkan dapat dicapai beberapa hal berikut :

- Volume trafik untuk pelayanan yang tersedia dapat dipenuhi oleh kemampuan produk SSP, STP dan SCP.

- SCP harus mampu melayani lebih dari satu macam pelayanan.
- Fleksibilitas produk yang berarti range database yang lebar dan kemampuan memenuhi volume trafik yang tinggi.
- *Upgrade* pada database SCP tidak mengganggu penyediaan pelayanan.
- Arsitektur jaringan harus mampu menangani jumlah SCP, SSP dan STP yang bervariasi.

II.7.1.2.3. Syarat-syarat Pengadaan

Syarat Pengadaan jaringan tergantung pada standar kualitas yang ditetapkan oleh masing-masing operator jaringan. Syarat pengadaan tersebut adalah sebagai berikut :

- SSP dan SCP

  Komponen ini harus tersedia 24 jam per hari, setahun penuh dengan maksimum *downtime* 3 menit per tahun.

- CCS#7

  Downtime untuk satu signaling point ke titik yang lain maksimal 10 menit per tahun.

- Aplikasi SCP

  Downtime untuk satu aplikasi SCP adalah 10 - 20 jam per tahun untuk satu sisi.

- SMS

  SMS harus tersedia 7 hari per minggu, dan 22 jam sehari. Setiap hari disediakan waktu 2 jam untuk proses pemeliharaan SMS.

II.7.2. DATABASE

Kapasitas database SMS dan SCP tergantung pada jumlah service subscriber dan user serta panjangnya catatan data. Untuk beberapa jasa pelayanan, kapasitas database juga ditentukan oleh data konfigurasi jaringan service subscriber. Jumlah service subscriber atau service user didasarkan pada jumlah total saluran telepon yang diharapkan untuk periode waktu tertentu. Panjangnya catatan data dipengaruhi oleh elemen data yang diperlukan untuk menyediakan service, dengan asumsi isi data adalah identik antara SCP dan SMS, hanya saja pada SMS ditambah dengan data administrasi subscriber.

Ukuran panjang data dalam database dapat diubah-ubah menurut fungsi dan feature yang dipakai subscriber untuk pelayanan tertentu. Karena itu selain range kapasitas database, diperhitungkan juga ukuran maksimalnya. SMS dan SCP harus mampu mendukung berbagai variasi kapasitas database, dari megabyte sampai beberapa gigabyte.

II.7.2.1. Syarat Integrasi Database

Prosedur self-checking harus disediakan untuk mendeteksi kesalahan

pada data dalam database. SCP membentuk sistem checking secara konsisten dan periodik bersama SMS untuk memeriksa data di SCP. SMS memiliki back-up seluruh data yang disediakan SCP, untuk menjaga kemungkinan kerusakan data yang terjadi pada SCP.

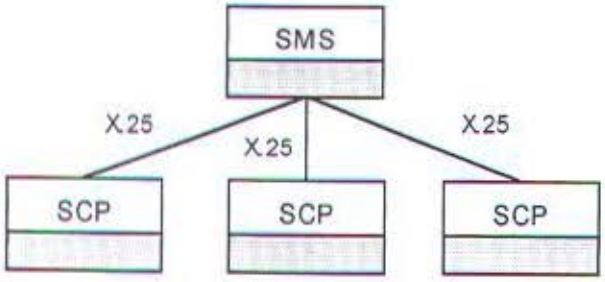
Konsistensi dan integrasi data dalam database tetap dijaga pada saat dilakukan update data. Diperlukan sistem transaksi data yang mampu memback-out dan melakukan mekanisme perbaikan, untuk menjaga akurasi data. Service Subscriber tidak menginginkan terjadinya kesalahan pada sistem tersebut, dan bila terjadi kesalahan, sistem harus mampu memperbaikinya serta menyelesaikan pembangunan panggilan segera setelah perbaikan selesai. Hal inilah yang merupakan konsep dasar integrasi database.

II.7.2.2. Lokasi Database

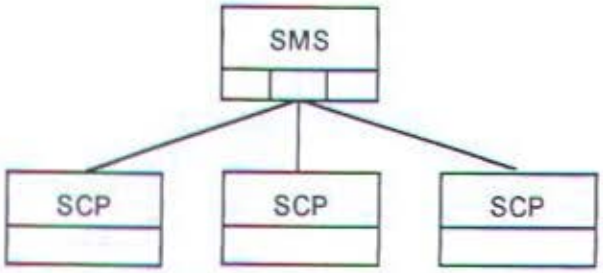
Database Jaringan Pintar (IN) dapat ditempatkan pada lebih dari satu SCP, secara terdistribusi (setiap SCP berisi sebagian atau keseluruhan data yang ada). Dengan demikian tidak ada data yang tersimpan di dalam SSP. Data dalam tiap SCP spesifik sesuai service yang ditawarkan, dan disimpan dalam bentuk disk dan juga residen pada memory. Database tersebut tersimpan pula dalam SMS dan bertindak sebagai master database.

Distribusi database pada SCP dan SMS dilakukan dengan 2 metode seperti terlihat pada gambar 2.19. Pada gambar a) diperlihatkan bahwa seluruh data yang terdapat pada SMS digandakan pada seluruh SCP. Dengan demikian

setiap SCP yang terdapat dalam jaringan memuat database yang sama dengan database yang ada dalam SMS. Sedangkan pada gambar b) hanya sebagian data SMS yang direplika di suatu SCP. Dalam hal ini SMS bertindak sebagai master database untuk semua SCP dalam jaringan tersebut.



a) Replikasi Database di seluruh SCP



b) Replikasi Sebagian Database di tiap SCP

GAMBAR 2.19[22]

DISTRIBUSI DATABASE

[22] Ibid. hal. 33

II.7.2.3. Administrasi Database

SMS mampu membentuk *initial load* untuk database yang disimpannya atau database SCP yang relevan. *Initial loading* membutuhkan paralelisme tingkat tinggi karena database dapat mencapai ukuran yang besar. Proses utama dalam SMS mengendalikan sejumlah subproses (sesuai jumlah peralatan fisik yang dibaca dari initial load). Proses utama beroperasi lebih cepat daripada subproses, karena itu semua disk di-update pada kecepatan penuh.

Database pada SCP dapat dipanggil dengan dua cara, yaitu :

a. Loading melalui saluran X.25
    1. File untuk loading dikirimkan ke SCP menggunakan kapabilitas file transfer.
    2. Software aplikasi distart melalui perintah dari SCP pada terminal lokal.
    3. Apabila initial store "disabled", berarti hubungan normal SMS-SCP tidak terbentuk.
    4. File load SMS di-load.
    5. File respons dibangkitkan, berisi satu respons setiap pesan dalam file load SMS. File respons disimpan dalam tape magnetik dan ditransfer ke SMS melalui file transfer.
    6. SMS memproses file respons dan menandai panggilan yang sukses.

7. SMS mencetak listing laporan data yang tidak dapat di-load.

b. Loading melalui tape

Proses loading dapat dilakukan secara lebih mudah dengan mentransfer database pada tape ke SCP, memanggilnya secara lokal melalui terminal tape magnetik. Cara ini dilakukan untuk database berukuran besar yang membutuhkan proses loading dalam waktu lama.

Proses update database meliputi tiga jenis perubahan, yaitu :

- Penambahan data baru
- Penghapusan data yang telah ada
- Perubahan fields dalam data

Setelah menerima seluruh hasil update data, SMS melakukan query untuk proses editing dan validasi. Bila proses ini selesai berarti proses update telah dilakukan dan berlaku bagi data yang relevan pada database lain. Proses ini dilakukan secara asinkronous ke input subscriber dibawah kendali SMS, menggunakan proses pertukaran antara SMS dan SCP. Update batabase dapat diajukan dengan 3 cara, yaitu :

- Service Subscriber mengisi permintaan pelayanan.

- Subscriber menghubungi Network Operator (NO) untuk meng-update parameter service. Network Operator meng-update parameter pelayanan menggunakan data terminal data yang dihubungkan ke SMS.
- Service Subscriber meng-update parameter pelayanan secara langsung.

BAB III

VIRTUAL PRIVATE NETWORK (VPN)

III. 1. UMUM

Pelanggan bisnis dengan lokasi yang berjauhan membutuhkan suatu jaringan komunikasi yang benar-benar efisien. Pada umumnya bisnis-bisnis ini menggunakan jaringan-jaringan pribadi sejenis PABX/Centrex. Pelanggan bisnis biasanya membeli peralatan transmisi dan switching tersebut dengan biaya yang pasti mahal. Dengan menggunakan jaringan pribadi, pelanggan-pelanggan ini memiliki beberapa keuntungan, yaitu :

Pertama, dengan jaringan pribadi diperlukan biaya yang efektif untuk mentransmisikan informasi.

Kedua, juga menyediakan kontrol yang lebih besar dari telekomunikasi lainnya dengan mengijinkan pelanggan bisnis tersebut untuk membatasi panggilan sehingga mengurangi biaya yang dikeluarkan.

Ketiga, adalah menyeragamkan nomor untuk meningkatkan fungsi dari jaringan pribadi dan memberikan para pelanggan beberapa kemampuan yang belum ada sekarang ini.

Virtual Private Network (VPN) adalah jasa yang memungkinkan pelanggan melakukan hubungan telepon baik nasional maupun internasional melalui jaringan PSTN biasa, akan tetapi seakan-akan menggunakan jaringan

pribadi (leased line).

Perusahaan atau badan usaha yang berlangganan jasa ini akan dapat mendefinisikan format penomoran, mengatur profile grupnya, mengubah feature, melihat statistik trafik dan kemampuan lain yang membuat pelanggan seakan-akan memiliki kontrol penuh atas fasilitas komunikasinya. Semuanya ini dimungkinkan dengan manipulasi routing dan database pada sistem Inteligent Network (IN).

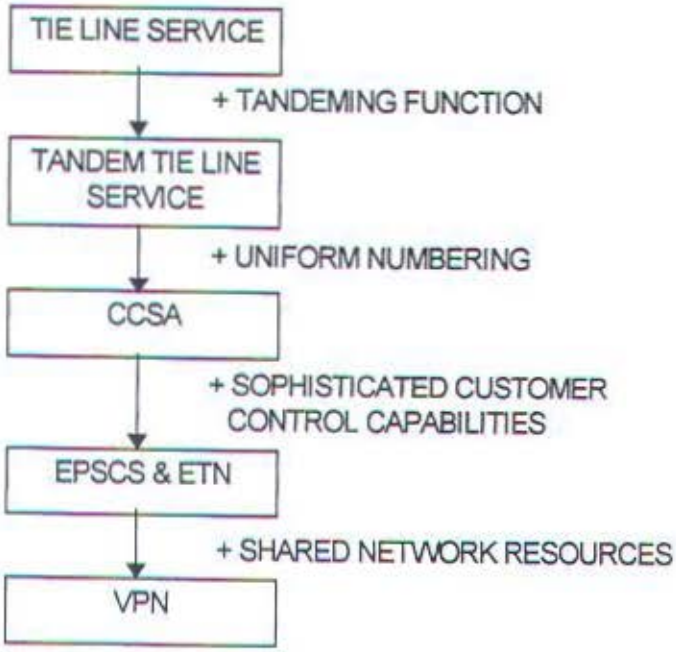
III. 2. KONSEP VPN

Jumlah layanan jaringan pribadi pada dekade terakhir akan berkembang menjadi beberapa kali dan jenis layanannya menjadi berbeda sama sekali tergantung pada :

a) Perkembangan teknologi

b) Pertambahan permintaan para pelanggan yang berbeda-beda.

Seperti terlihat pada gambar 3.1, layanan Tie-Line dapat dipertimbangkan sebagai yang utama, merupakan bentuk layanan jaringan pribadi yang paling sederhana. Jaringan yang lebih penting terdiri atas dua PABX/Centrex yang dihubungkan oleh fasilitas transmisi. Sebagai perluasan yang umum dari layanan Tie-Line, ditambahkan layanan Tandem Tie-Line, yang menyediakan layanan lebih dari dua lokasi dengan sentral tandemnya. Sebagai gambaran operasinya, ambil sebuah jaringan yang terdiri dari PBXs A, B dan C,



GAMBAR 3.1[23]

PERSPEKTIF SEDERHANA PADA EVOLUSI VPN

suatu panggilan dari A ke C, pemanggil pertama kali memanggil suatu kode akses untuk mencapai PBX B. Setelah menerima nada panggil dari PBX B, kemudian pemanggil memasukkan kode akses yang lain untuk menginstruksikan PBX B untuk membangun hubungan dengan PBX C, kode akses yang berbeda dibutuhkan untuk mencapai stasiun yang sama tergantung dari lokasi panggilan. Untuk meringankan masalah penomoran yang tidak seragam, diperkenalkan CCSA (Common Control Switching Arrangement) sebagai layanan jaringan pribadi pertama yang menawarkan layanan dialing yang seragam diatas fasilitas-fasilitas pribadi. Lebih jauh dicontohkan

---

[23] Wedemeyer, D.J., Bissel, M.S., *Pasific Telecommunications Users : A Spectrum of Requirements*, Elsevier Science Publishers B.V., North-Holland, 1987, hal.29

pengembangan peralatan layanan jaringan pribadi, suatu bentuk yang lebih canggih dari layanan pribadi yang disebut Enhanced Private Switched Communication Service (EPSCS), yang dikenalkan pada tahun 1978. Beberapa keistimewaan EPSCS adalah sistem transmisi 4-wire (untuk memperbaiki kualitas transmisi) dalam jaringan pribadi dan suatu pusat pengontrol jaringan pelanggan dimana pelanggan dapat menggunakannya untuk mengontrol beberapa operasi jaringan dan untuk memperoleh status atau fungsi informasi jaringan pribadi. Kemudian diperkenalkan Electronic Tandem Network (ETN) pada tahun 1979 dengan banyak keistimewaan seperti EPSCS. Secara keseluruhan ETN menawarkan kepada pelanggan bahwa kemampuan kontrol pelanggannya sedikit lebih canggih dengan biaya yang lebih rendah. Dengan cara yang sama, pada daerah komunikasi data, ditawarkan sejumlah layanan yang semakin bertambah. Ada beberapa daftar sebagai berikut seperti layanan digital DATAPHONE (menawarkan data komunikasi yang lebih terpercaya dengan arah point to point atau multipoint dengan kecepatan data 2,4; 4,8; 9,6; dan 56 Kbps), stasiun pilihan DATAPHONE (aplikasi yang utama adalah untuk remote telemetry), dan lain lain.

Bagaimanapun juga jaringan pribadi ini terjadi dari sejumlah perubahan. Di antaranya adalah :

Pertama, Operation, Administration and Maintenance (OA & M) yaitu suatu tipe yang bertanggung jawab atas kebutuhan penting sumber pelanggan.

Kedua, bisnis untuk lokasi-lokasi geografis yang terpisah sering ditemukan termasuk lokasi remotenya dalam jaringan pribadi yang sangat mahal dengan arah akses yang jauh.

Pada akhirnya jaringan yang berdasarkan hardware tidak dapat berkembang dengan perubahan teknologi dan lalu lintas permintaan yang berubah-ubah. Jadi banyak pelanggan mencari alternatif untuk kebutuhan telekomunikasi yang lebih nyaman.

Dengan menggunakan jaringan pribadi disamping memiliki keuntungan juga mempunyai kerugian. Beberapa keuntungannya yakni :

- Dari aspek security, dengan menggunakan jaringan pribadi, komunikasi yang dilakukan oleh user akan lebih terjamin keamanannya.
- Dari aspek manajemen, memiliki konfigurasi jaringan yang pasti, fleksibilitas serta peningkatan pengetahuan mengenai jaringan.

Sedangkan kerugian-kerugiannya antara lain :

- Dari segi manajemen, beragamnya pilihan dan keruwetan dari sistem meninggikan biaya dari perawatan alat. Dan lebih susah lagi bila saat mengatur sirkuit pribadi secara internasional.
- Dari segi biaya, tidak seperti halnya pada jaringan publik yang dikenai biaya hanya selama pemakaian oleh pelanggan.
- Dari segi routing, tidak ada pilihan routing yang lain bila terjadi suatu kerusakan pada jalur pribadi tersebut.
- Dari segi kesulitan pengaturan pada jaringan internasional, memerlukan persetujuan dari penyelenggara jasa yang berbeda. Hali ini harus dikoordinasikan lebih lanjut dengan kondisi serta pelayanan yang berbeda.

Untuk mengurangi masalah-masalah yang berkaitan dengan konfigurasi

jaringan pribadi, maka ditawarkan layanan yang berdasarkan pada konsep jaringan virtual pribadi (VPN). Kata "virtual" berarti bahwa pada VPN tidak terdapat fasilitas transimisi atau peralatan switching pada pelanggan tertentu. Jika pelanggan (berdasarkan pada loop atau PABX) memulai suatu panggilan suara atau data, suatu komunikasi dibangun hanya jika ada suatu sirkuit publik yang tidak bekerja ke sentral tujuan. Sama seperti suatu rangkaian yang berubah-ubah alokasinya ke pelanggan hanya untuk suatu selang waktu panggilan. Jadi, pada saat permintaan layanan di antara pelanggan yang berbeda-beda pada tipe VPN atau POTS ada skala ekonomis yaitu penghematan dari pembagian jaringan publik.

Sejak VPN disimulasikan oleh software dalam suatu jaringan publik, arsitektur jaringan untuk VPN secara fundamental sama seperti untuk jaringan publik. Jaringan ini berisi sejumlah perlatan sentral umum dengan kemampuan khusus untuk mengatur dan memroses panggilan VPN. Bagaimanapun juga keistimewaan VPN dipisahkan dari pemusatan database terutama untuk menangani panggilan VPN, sering disebarkan dalam lingkungan Common Channel Signalling (CCS). Penyebaran database terpusat banyak memudahkan proses OA & M seperti menambah titik baru pada jaringan, hanya diperlukan memperbarui pusat database, tidak perlu memperbarui seluruh switching.

Keuntungan jaringan pribadi dengan menggunakan jaringan publik adalah :

- Fleksibilitas : service provider dapat menawarkan layanan yang murah pada klien yang membutuhkan. Hal ini termasuk hal biaya seperti tarif murah yang

ditawarkan pada subscriber yang menggunakan layanan secara teratur, atau biaya yang lebih rendah untuk penggunaan secara teratur pada tujuan tertentu.

- Fleksibilitas pada routing : routing dilakukan oleh jaringan publik, ini termasuk routing alternatif bila memang diperlukan.
- Flesibilitas bandwidth : kapasitas jaringan yang digunakan optimal.
- Aspek Manajemen : permintaan untuk pengertian secara teknik dan kemampuan dalam mengorganisasi para pelanggan sangat berkurang. Pemakai jaringan menjadi lebih sedikit diperhatikan oleh bagaimana cara service disediakan dan lebih difokuskan pada mengatur tingkat-tingkat layanan daripada segi teknologinya.
- Pemeliharaan : service user tidak dibebani oleh pemeliharaan dan perawatan peralatan. Hal ini menjadi tanggung jawab dari service provider.
- Penggantian yang mudah dan cepat dalam implementasi : sebagai contoh yaitu penambahan dan penghapusan lokasi pada jaringan.

III. 3. SERVICE SUBSCRIBER DAN KEUNTUNGANNYA

Para user umumnya tertarik pada VPN untuk komunikasi suara. Hal ini disebabkan oleh penghematan biaya dibandingkan dengan menggunakan jaringan pribadi. Penghematan biaya ini diperoleh dari :

- penggantian leased circuit oleh jalur-jalur dimana VPN lebih murah.
- perbaikan kontrol oleh routing user yang berakibat pada optimasi trafik on-net.

III. 3. 1. Jenis User

Awalnya VPN ditargetkan untuk user jaringan suara pribadi yang ingin memperbesar atau mengganti jaringan pribadi mereka. Belakangan ini, perusahaan kecil yang memiliki banyak cabang juga mulai tertarik. Bagi perusahaan tersebut jaringan pribadi sulit untuk diterapkan tetapi pilihan yang mungkin yaitu dengan memakai VPN. Itu dapat menjadi keadaan yang wajar bila 25 persen dari trafiknya adalah intra perusahaan yang bekerja sama yang merupakan pemakai potensial VPN.

III. 3. 2. Keuntungan-keuntungan

Sebagai solusi dalam penghematan biaya pada pemakaian jaringan pribadi, VPN juga memiliki beberapa keuntungan yang lain bagi para user. Di antaranya adalah :

- kontrol pada routing user : routing ditentukan dengan banyak cara, hal ini mengarah pada optimasi trafik on-net.
- manajemen jaringan : service provider dapat menawarkan pada perusahaan pemakai akses ke database, sebagai contoh mengenai informasi tentang jaringan dan statistik layanan terpakai. Informasi ini biasanya dapat untuk mengatasi masalah dan mencari jalan keluarnya. Database yang lain dapat diguanakan untuk beberapa keperluan, seperti mengubah akses kode otorisasi atau menambah rencana penomoran yang baru.

- rencana penomoran pribadi : beberapa perusahaan user mempunyai kemungkinan dalam penerapan dan menggunakan penomoran yang cocok bagi perusahaan user tersebut. Penomoran tersebut seragam bagi seluruh perusahaan.
- fungsional yang luas bagi lingkup daerah yang kecil : VPN memberi kesempatan pada perusahaan-perusahaan untuk melengkapi daerahnya dengan semua feature yang digunakan di tempat lain pada lokasi utama tanpa tambahan biaya.
- fleksibilitas yang lebih besar : perusahaan-perusahaan user dapat membuat perubahan-perubahan mengenai konfigurasi jaringan sesuai dengan keinginannya agar lebih cepat bila dibandingkan dengan jaringan pribadi biasa.
- billing : billing terpusat dan penagihan dapat diwujudkan pada VPN.

Jadi dapat disimpulkan bahwa service VPN merupakan gabungan antara pengontrolan dan pengaturan suatu jaringan pribadi dengan fleksibilitas seperti jaringan publik dan tanpa mengatur masalah switching. Karena layanan intelijen khusus pelanggan berada dalam jaringan publik, sehingga user VPN dapat menikmati perkembangan feature service tersebut, yang tadinya hanya tersedia dalam jaringan pribadi. Penghematan biaya merupakan suatu keuntungan dari penerapan VPN pada jaringan publik.

III. 4. IMPLEMENTASI VPN PADA IN

Seiring dengan permintaan kebutuhan para pelanggan ketika mempersatukan teknologi baru dan keahlian dalam lingkungan multi-vendor, industri telekomunikasi telah mengembangkan suatu konsep IN mengenai kreasi, pelaksanaan dan perlengkapan dari pengembangan beberapa layanan telekomunikasi.

Konsep IN sudah tercakup dalam rancang bangun aplikasi VPN. Service Switching Function (SSF) mampu untuk mendeteksi panggilan service VPN. Selanjutnya proses panggilan diteruskan pada Service Control Function (SCF). SSF secara fisik berada dalam switch digital yang disebut Service Switching Points (SSP), sedangkan SCF secara fisik berada dalam Service Control Point (SCP). Keduanya merupakan kesatuan komunikasi yang menggunakan Transaction Capabilities Application Part (TCAP) dari protokol pensinyalan Common Channel Signalling System Nr. 7.

Intelligent Peripheral Function, yang juga terdapat dalam SSP, memberi petunjuk dalam membimbing para user VPN selama fase set-up sebaik pada fase terminasi jika keadaan seperti ketidaksiapan atau ketidaklancaran terjadi.

Service Management Point (SMP) merupakan kesatuan jaringan dimana perlengkapan dan pengontrolan service diberikan. Dalam databasenya informasi dikumpulkan dan diperbarui oleh service subscriber dan service provider atau network operator.

III. 4. 1. Terminologi

VPN memiliki beberapa elemen yang menunjang beroperasinya dan keberadaannya pada jaringan publik, yaitu :

- NETWORK PROVIDER adalah merupakan penyelenggara telekomunikasi yang bertanggung jawab atas jaringan telekomunikasi (switch, trunk, line dan lain-lain).

- VPN SERVICE PROVIDER adalah merupakan penyelenggara telekomunikasi atau perusahaan pengoperasi yang menawarkan service VPN sebagai salah satu aplikasi dari Intelligent Network (IN). Hal ini akan diatur persetujuan antara network provider yang bersangkutan guna mengumpulkan beberapa sumber untuk membangun sebuah jaringan. Jaringan ini dapat dibagi di antara VPN service subscriber yang berbeda.

- VPN SERVICE SUBSCRIBER adalah merupakan perusahaan atau organisasi yang berlangganan service VPN dimana mempunyai hak untuk mengatur sendiri konfigurasi jaringannya dan bertanggung jawab pada kontrak persetujuan dengan service provider.

- VPN MEMBER (VPN SERVICE USER) adalah merupakan user individu atau sebuah grup para user (seperti PABX) yang dapat membuat dan menerima panggilan yang berasal dari sumber VPN. Anggota VPN dihubungkan pada VPN melalui PABX atau melalui sebuah line tunggal. Anggota VPN dapat menjadi milik lebih dari satu VPN.

- VPN GROUP adalah merupakan sekumpulan anggota dimana service

subscriber telah meminta dan menentukan akses dan penggunaan service VPN.

- VPN ATTENDANT adalah merupakan Anggota VPN khusus yang menyediakan informasi layanan.
- ON-NET CALL adalah merupakan panggilan yang berasal dari anggota VPN dan dirouting ke tujuan VPN.
- OFF-NET CALL adalah merupakan panggilan yang salah satunya bukan sebagai anggota VPN.
- SUB-NET CALL adalah merupakan panggilan keluar dari group tetapi menggunakan format penomoran VPN.

III. 4. 2. Feature Service VPN

Kemungkinan feature service VPN seperti yang diterima oleh service user, service subscriber merupakan bagian dari rencana service model konsep IN. Untuk menjelaskan service dengan seluruh featurenya, hal ini berkaitan dengan proses kreasi layanan.

VPN dapat menyediakan beberapa feature atau beberapa kombinasi dari beberapa feature yang berhubungan dengan kebutuhan service subscriber.

III.4.2.1. Private Numbering Plan (PNP)

Karakteristik yang penting dari VPN adalah Private Numbering Plan (PNP). Nomor pribadi dialokasikan pada tiap anggota VPN (on-net number) tetapi dapat juga dialokasikan pada lokasi off-net (off-net number).

Karena masing-masing service subscriber bebas menentukan sendiri rencana penomorannya. Jumlah digit yang digunakan untuk PNP dapat beragam. Biasanya terdiri dari 3 sampai 7 digit dengan maksimum 14 digit. Digit terakhir dari perusahaan dengan penomoran telepon jaringan publik yang normal dapat juga digunakan untuk menyusun rencana penomoran pribadi.

Semua nomor yang diberikan PNP memiliki panjang yang sama, yang artinya bahwa PNP mempunyai penomoran yang uniform. PNP adalah nomor yang menggantikan nomor terminal PSTN. Nomor ini yang akan dipanggil pada jaringan VPN. Format penomoran ditentukan oleh pelanggan sendiri. Sedangkan format panggilan dengan PNP adalah :

Kode Akses + PNP tujuan

III.4.2.2. Personal Identification Number (PIN)

Fungsi PIN ini ialah mengijinkan untuk mengenali para user dengan memeriksa kecocokan antara User Identity (UI) dan PIN mereka.

Fungsi ini tidak memerintahkan untuk mengalokasikan User Identity tiap anggota VPN tetapi jika fungsi ini dialokasikan untuk anggota VPN, maka harus

berupa pengidentifikasi yang khusus dalam VPN. Panjang digit User Identity maksimum 6 digit dan alokasinya dikerjakan oleh service subscriber. Personal Identification Number atau PIN merupakan kode rahasia.

III.4.2.3. Abbreviated Dialling (ABD)

Setiap service subscriber dapat memperkenalkan suatu daftar yang berisi nomor-nomor Abbreviated Dialling. Nomor abbreviated dapat terdiri dari 1sampai 9 digit, tetapi hal itu merupakan panjang yang tetap dalam grup VPN (misalnya PNP uniform numbering plan).

Pelanggan menggunakan nomor ini untuk menyingkat nomor panggilan menjadi hanya 2 atau 3 digit untuk terhubung ke tujuan. Untuk itu pelanggan mendefinisikan ABD untuk setiap nomor tujuan dan kode ABD yang merupakan digit pembeda dengan panggilan PNP biasa. Kode ABD yang dipakai ialah "9". Format panggilannya adalah :

Kode Akses + Kode ABD + ABD tujuan

III.4.2.4. Forced On Net (FOO)

Fungsi FOO ini ialah mengijinkan anggota VPN untuk memaksa panggilan sumber dengan nomor langsung publik yang dirouting melalui jaringan VPN, akan diterima sebagai panggilan VPN, seperti jika halnya nomor PNP yang diputar.

Feature ini memberikan keuntungan bagi para user pengguna layanan VPN, walaupun mereka tidak begitu memahami PNP. Ini berarti tidak hanya feature-feature istimewa dari VPN itu saja yang sanggup digunakan user, tetapi juga berarti menghemat biaya, karena panggilan-panggilan yang dirouting melalui jaringan VPN lebih murah bila dibandingkan panggilan-panggilan yang dirouting melalui jaringan publik.

Bila nomor yang diputar ada di dalam database maka panggilan tersebut dianggap On-Net bila tidak maka panggilan tersebut dianggap Off-Net. Pada grup VPN Forced On-net diawali dengan digit "0". Format panggilannya adalah :

Kode Akses + Kode FOO + CC + AC + DN

Keterangan : CC = Country Code

AC = Account Code

DN = Directory Number

Karena sentral lokal umumnya hanya dapat mengakomodasi 16 digit, maka panggilan ini lebih baik jika dilakukan melalui Remote Access atau Account Call.

III.4.2.5. Call Screening

Service subscriber boleh melakukan pembatasan tertentu terhadap para user, mengenai set up dari panggilan-panggilan sumber.

Setiap nomor PNP (nomor lengkap atau prefix) dan setiap nomor Abbreviated Dialling merupakan milik grup screening tertentu.

Setiap anggota VPN dihubungkan dengan PNP dan ABD grup-grup screening dimana tiap anggota dapat mengakses ketika melakukan suatu panggilan. Sifat-sifat grup screening menentukan pembatasan yang sesuai dan hal itu diserahkan sepenuhnya pada service subscriber untuk mengaturnya. Beberapa tingkatan pembatasan pada panggilan yang dituju dapat dimasukkan dalam kategori pembatasan tertentu, misalnya :

- pembatasan secara geografik : on-net call, zonal, national dan lain-lain.
- pembatasan secara fungsional : department, customers dan lain sebagainya.

Setiap panggilan dari setiap anggota VPN disaring. Screening berdasarkan pada kemudahan akses grup screening dan panggilan dapat diijinkan atau ditolak sesuai pada hasil screening.

Setiap nomor PNP mungkin hanya milik satu PNP grup screening. Setiap nomor ABD mungkin hanya milik satu ABD grup screening. Jumlah dari grup screening ditentukan oleh service subscriber. Kemungkinan maksimum dapat mencapai 60 grup.

III.4.2.6. Override Restriction (OVR)

Jika anggota VPN mengakses VPN melalui peralatan dari anggota yang lain dan bertemu dengan pembatasan screening, maka fungsi OVR ini ialah akan mengijinkan anggota pertama untuk mengesampingkan pembatasan yang dikenakan pada anggota lain tadi. OVR ini berlaku untuk set up satu panggilan. Anggota yang memanggil harus memasukkan kode otorisasi, User Identity dan

PIN. Dengan demikian, anggota tadi akan memperoleh tingkat pembatasannya sendiri. Feature ini memberikan fasilitas untuk membuka keterbatasan pada Closed User Group. Misalnya bila General Manajer akan menghubungi Direksi maka dia harus memasukkan digit tertentu untuk melakukan panggilan tersebut. Format panggilannya adalah :

Kode Akses + PNP/ABD tujuan

Dengan mengikuti petunjuk announcement, user memasukkan nomor VPN card dan PIN.

III.4.2.7. Automatic Call Distribution (ACD)

Fungsi ACD ini ialah menyediakan anggota-anggota VPN dengan beberapa fasilitas untuk mendapatkan pertolongan panggilan. Fungsi ACD ialah mendistribusikan panggilan-panggilan kepada sejenis operator VPN yang tersedia, sesuai dengan seleksi yang berdasarkan pada dua peraturan dasar :

- pilihlah operator terdekat untuk mengoptimalkan biaya dan unjuk kerja.
- hindari pemilihan operator jika telah dipastikan 'x' detik sebelumnya.

Posisi operator dapat dicapai jika user membutuhkan pertolongan atau ketika tujuan yang dipanggil sibuk atau tidak menjawab atau terjadi kerusakan. Service subscriber mampu untuk mengalokasikan fungsi dari operator tersebut pada beberapa anggota VPN.

III.4.2.8. Remote Access (RMTA)

Fungsi RMTA ini ialah mengatur akses ke layanan VPN oleh user VPN dari posisi non VPN. Setelah mensahkan panggilan dengan memeriksa User Identity dan PINnya, user akan memiliki hak yang sama seperti jika user tersebut memanggil dari posisi VPNnya. Panggilan akan diteruskan seperti panggilan VPN yang normal.

III.4.2.9. Account Code (ACC)

Fungsi ACC ini ialah mengijinkan para user untuk menandai panggilan-panggilan mereka dengan suatu Account Code. Account Code ini melampui kesalahan Account Code yang dihubungkan pada user. Account Code digunakan setelah memproses data panggilan untuk maksud charging.

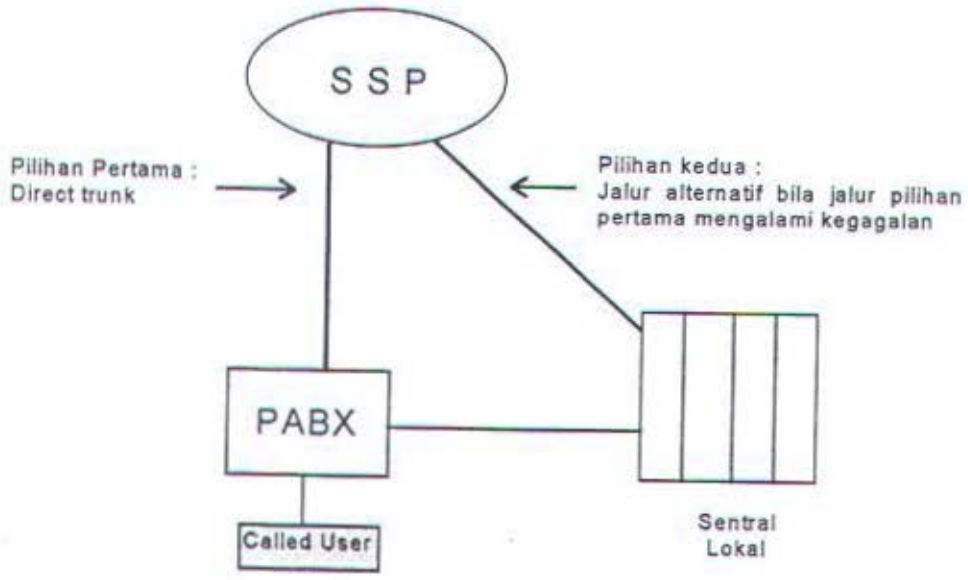
Untuk keperluan statistik biaya telepon grup VPN, pelanggan diberikan keleluasaan untuk mengatur account bagi sub-grupnya atau anggotanya. Berdasarkan account ini pelanggan dapat melihat statistik biaya per sub-grupnya. Panggilan ini dilakukan bila seorang anggota menelepon dari terminal anggota lain yang accountnya berbeda, agar biaya tertagih tetap menjadi beban accountnya. Untuk itu pelanggan mendefinisikan nomor account untuk setiap anggota dan kode ACC yang merupakan digit pembeda dengan panggilan PNP biasa. Kode ACC yang dipakai adalah "8". Format panggilannya adalah :

Kode Akses + Kode ACC + ACC yang bersangkutan

Dengan mengikuti petunjuk announcement untuk memasukkan nomor VPN card, PIN dan nomor tujuan.

III.4.2.10. Direct Trunk Overflow (DTO)

Fungsi DTO ini ialah mengalokasikan suatu jalur alternatif untuk tujuan yang sama saat jalur pertama yang dipilih (direct trunk) pada tujuan ini mengalami kegagalan, seperti yang terlihat pada gambar 3.2. Untuk beberapa tujuan, otorisasi dari user yang memanggil ditanyakan guna melaksanakan pengulangan routing.



GAMBAR 3.2[24]

FEATURE DIRECT TRUNK OVERFLOW

---

[24] ____, Hand Out Intelligent Network Service Implementation : VPN Detailed Description, Bell Education Centre, Alcatel, 1995, hal. 19.

III.4.2.11. Call Limiter (CAL)

Fungsi CAL ini ialah membatasi jumlah panggilan-panggilan yang bersamaan tiap tujuan atau grup dari tujuan-tujuan. Panggilan ditolak atau diteruskan ke tujuan yang banyak atau pemberitahuan sampai jumlah dari panggilan-panggilan yang bersamaan tadi berada dibawah limitnya. Pembatasan dapat diatur oleh service subscriber.

III.4.2.12. Alternative Destination On Busy (ADOB)

Fungsi ADOB ini ialah mengijinkan untuk merouting panggilan ke tujuan alternatif saat jalur tersebut dalam keadaan sibuk. User yang memanggil akan diberitahu bahwa routing khusus ini sedang sibuk.

Service subscriber dapat mengalokasikan untuk setiap tujuan VPN sebagai tujuan alternatif.

III.4.2.13. Alternative Destination On No Reply (ADONR)

Fungsi ADONR ini ialah mengijinkan untuk merouting panggilan ke tujuan alternatif saat user yang dipanggil tidak menjawab dalam batas waktu tertentu. User yang memanggil akan diberitahu bahwa routing khusus sedang sibuk.

Service subscriber dapat mengalokasikan untuk tiap tujuan VPN sebagai tujuan alternatif.

III.4.2.14. Customized Terminating Announcements

Fungsi ini ialah memberikan dukungan fasilitas operasi layanan VPN. Announcement dibuat ketika mengakhiri panggilan atau dalam kasus prosedur interaktif. Hal ini mungkin untuk penerapan customized announcements tertentu oleh service subscriber.

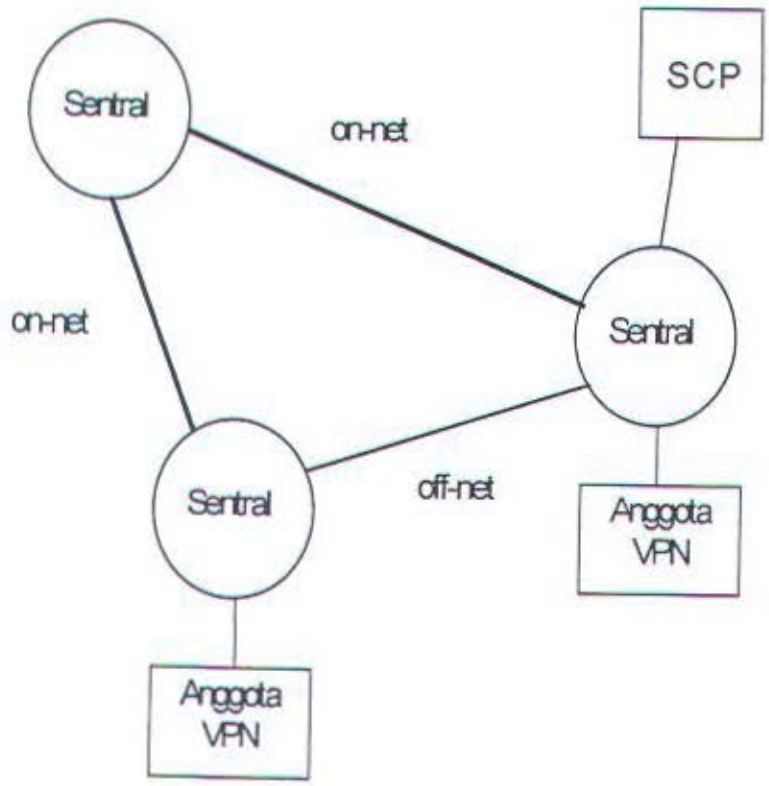
III.4.2.15. Statistical Reporting

Fungsi ini ialah mengijinkan service subscriber untuk memperoleh informasi atas layanan VPN, seperti informasi pada trafik (on-net, off-net), pemakaian beberapa feature yang berbeda (ABD, CAL, DTO). Laporan statistik merupakan proses off-line dari data yang tercatat pada sentral-sentral dan diatur sesuai pada format yang berbeda.

III.4.2.16. On Net / Off Net Call

Secara umum service provider menentukan apakah tujuan panggilannya on-net atau off-net. Ciri dari panggilan on-net VPN adalah panggilan antara dua user VPN yang berada dalam perusahaan yang sama yang dihubungkan pada VPN melalui PABXs yang berbeda. Sebagai contoh dari panggilan VPN off-net ialah bila user yang sedang dalam perjalanan menggunakan kartu kredit VPN untuk melakukan panggilan dari telepon umum ke daerah VPN.

Pada gambar 3.3 panggilan diset up antara dua anggota VPN. Ada dua jalur yang mungkin; panggilan dapat dirouting melalui jaringan yang kedua-duanya jaringan VPN (on-net call) atau melalui jaringan publik (off-net call). Hal ini tergantung pada hasil dari jumlah translasi dan/atau pada kesiapan dari trunk.



GAMBAR 3.3[25]
TUJUAN ON-NET DAN OFF-NET UNTUK CARRIERS

[25] Ibid, hal. 21

Suatu kemungkinan bahwa panggilan antara anggota VPN dirouting melalui jaringan publik dan oleh karena itu cara lain dari panggilan on-net adalah off-net.

III.4.2.17. Closed User Group (CUG)

Pelanggan mendefinisikan beberapa sub-grup untuk pembatasan. Pada umumnya grup VPN dibuat dua group, yaitu Direksi dan General Manajer. Direksi dapat mengakses Direksi lain dan General Manajer, sedangkan General Manajer hanya dapat mengakses General Manajer lain.

III.4.2.18. Call Distribution

Panggilan yang diterima dapat didistribusikan ke nomor-nomor tertentu. Misalnya 30% panggilan ke bagian A dan 70% panggilan ke bagian B.

III.4.2.19. Pre Sorting

Panggilan yang diterima dapat didistribusikan sesuai dengan digit yang ditekan pelanggan. Misalnya menekan '1' untuk panggilan ke Direksi, menekan '2' panggilan ke General Manajer, dan seterusnya.

III.4.2.20. Day or Time Dependent Routing

Panggilan dapat dirouting sesuai dengan hari atau jam tertentu. Misalnya Hari Senin sampai Jumat jam 08.00 sampai 16.00 panggilan dirouting ke bagian operator, jam 16.01 sampai 07.59 panggilan akan dirouting ke bagian piket. Sedangkan pada Hari Sabtu dan Minggu panggilan akan dirouting ke announcement 'LIBUR'.

III.4.2.21. VPN Mobility

VPN Mobility ini merupakan prospek masa depan. Meskipun VPN merupakan service yang modern, penomoran PNP biasanya disatukan dengan sekumpulan terminal base yang telah ditentukan pada PABX bersama atau dihubungkan pada jalur akses atau jalur-jalur pada jaringan publik. Beberapa mobilitas memiliki kemungkinan menggunakan panggilan lama untuk feature yang akan datang.

Tidak seperti service Universal Personal Telecommunications (UPT), memungkinkan tiap user UPT untuk menandai dan menerima panggilan pada basis tertentu, nomor pribadi malalui beberapa jaringan dan pada tiap terminal ditentukan, mobile atau movable. Terminal mobile ditangani oleh service GSM (Global System for Mobile communication).

Kebebasan bergerak ini dapat juga ditawarkan pada end user service VPN. Service ini menawarkan service campuran yang nyata, yaitu service VPN, GSM dan UPT.

III. 5. KONFIGURASI VPN

Aspek-aspek yang berhubungan dengan implementasi fisik layanan pada IN telah ditetapkan dalam physical plane dari model konsep IN. Saat penerapan layanan VPN internasional, masalah utama mengenai distribusi fisik dari layanan intelijen tertentu pelanggan (SCF dan service/pelanggan data tertentu) harus dipecahkan, karena service harus disediakan dengan feature yang ada dimana-mana pada basis internasional.

III. 5. 1. Akses User dan Trunk Yang Digunakan Dalam VPN

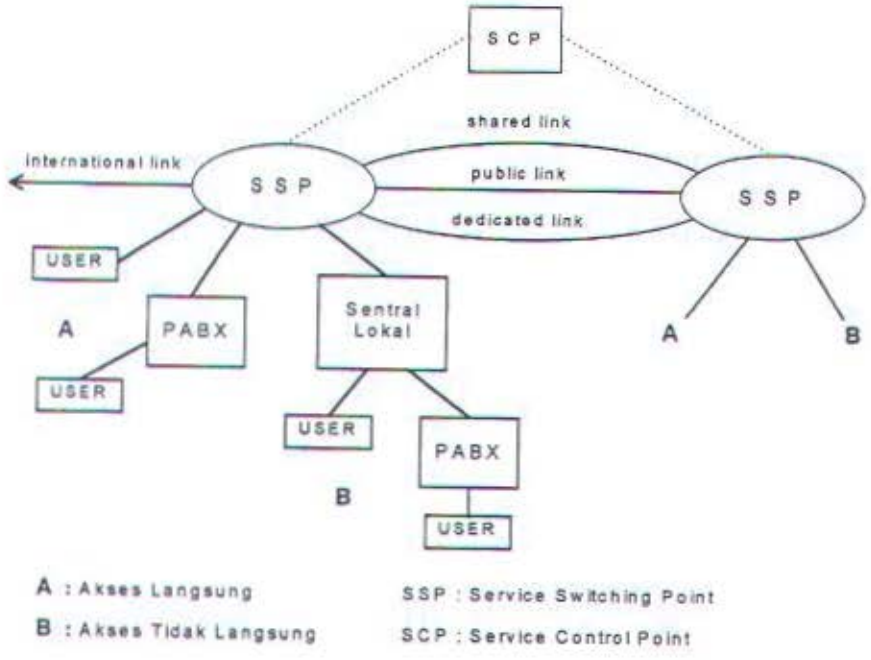
Gambar 3.4 menunjukkan konfigurasi yang mungkin dari VPN. Jaringan VPN mengijinkan tipe akses user sesuai :

- Direct Access : anggota VPN memiliki akses langsung ke VPN, yang berarti bahwa secara langsung anggota VPN tersebut terhubung pada sentral dengan fungsional SSF. Jenis A pada gambar 3.4.
- Switched Access : anggota VPN dihubungkan pada VPN melalui jaringan telepon sambungan publik; jadi sentral lokal yang dihubungkan pada anggota tidak memiliki implementasi fungsional SSF. Jenis B pada gambar 3.4.

Kemungkinan alternatif ketiga adalah akses user melalui jalur yang sudah ada yang disebut sebagai **Dedicated Access**.

Beberapa trunk jaringan VPN yang menghubungkan beberapa SSP, dapat mempunyai tingkat assignment yang berbeda terhadap trafik VPN, yaitu :

- Dedicated Link : trunk (grup) ini diperuntukkan hanya untuk satu grup VPN. Trunk akan membawa trafik secara eksklusif untuk grup VPN tunggal tersebut.
- Shared Link : trunk (grup) ini membawa trafik untuk beberapa grup VPN. Grup VPN tersebut membagi kapasitas dari link ini.
- Public Link : trunk (grup) ini juga sejenis dengan shared link, tetapi kapasitas dibagi antara user VPN dan user publik. Link kemudian membawa trafik VPN dan trafik publik (non VPN). Ada kapasitas tertentu yang ditetapkan untuk trafik VPN, dalam bentuk Selective Trunk Reservation (STR). Saat ini hanya link publik saja yang baru diterapkan.



GAMBAR 3.4[26]
KONFIGURASI VPN

[26] Ibid, hal. 24

Untuk yang akan datang, trunk internasional jaringan IVPN adalah dedicated, sedangkan shared trunk untuk trafik IVPN.

III. 5. 2. Kode Akses

Kode akses untuk melakukan panggilan VPN internasional hanya tersedia melalui metode akses switched baik melalui terminal PSTN terdaftar atau dapat juga dari terminal tidak terdaftar pada database VPN. Kode akses switched tersebut ada dua, yaitu kode akses On-net switched dan Off-net switched.

III.5.2.1. Akses On-net Switched

Terminal yang telah terdaftar sebagai anggota menggunakan kode akses **080515**. Panggilan dengan kode akses ini dapat langsung diikuti dengan nomor tujuan VPN. Anggota VPN dapat mengakses ke jaringan VPN melalui PSTN dari on-net extension. Prosedur aksesnya adalah sebagai berikut :

a. On-net ke On-net (On-net)
   Dialed digit : 080515 + XXX XXXX
   Routing number : KP(1)+SID+CID+XXXXXX

b. On-net ke Off-net (Sub-net)
   Dialed digit : 080515 + XXX XXXX
   Routing number : KP(1)+AC+DN

c. On-net ke Off-net (Off-net)

Dialed digit : 080515+0+CC+AC+DN

Routing number : KP(1)+AC+DN

Keterangan : KP(1) = Kode National to Internastional

SID = Service ID (3-5 digit)

CID = Customer ID (3-4 digit)

AC = Account Code

DN = Directory Number

XXXX = Private number (7 digit)

III.5.2.2. Akses Off-net Switched

Terminal yang tidak terdaftar sebagai anggota menggunakan kode akses **080512**. Panggilan dengan kode ini (disebut juga Remote akses) akan dituntun voice guidance untuk melakukan hubungan telepon. User harus memutar kode akses remote VPN, yaitu :

080512 + LD (LD = language code)

User memasukkan nomor kartu VPN-nya, yaitu kombinasi antara ID grupnya dan User ID dan memasukkan PIN-nya saat diminta. Berikutnya user diminta untuk memasukkan nomor tujuannya. User dapat menempatkan panggilannya pada panggilan On-net, Sub-net atau Off-net tanpa perlu memutar kode akses. Untuk nomor routingnya sama seperti pada akses On-net switched.

III. 5. 3. Konfigurasi International VPN (IVPN)

Satu tantangan yang besar untuk service IVPN adalah menyediakan semua feature yang dimilikinya untuk semua user yang terhubung melalui beberapa jaringan yang berbeda. Kunci masalah ini adalah mempunyai kemampuan untuk menyimpan dan mengakses service intelijen tertentu pelanggan dalam jumlah yang besar (kedua service, yaitu logic dan data) dalam jaringan, dan untuk mengatur informasi ini secara efisien. Kebutuhan service intelijen dari para user dalam satu jaringan dibagi dengan jaringan lain yang ikut berpartisipasi. Jaringan harus mampu membuat keputusan yang cepat untuk memproses panggilan VPN.

Service intelijen disimpan dalam database terpusat, seperti Service Control Point (SCP), dalam jaringan struktur IN. Untuk Internasional VPN, diberikan tingkat berbeda yang tidak sesungguhnya dari jaringan yang berpartisipasi, service intelijen tertentu pelanggan dari semua user dari semua jaringan ini mungkin ada dalam database dari jaringan tunggal (satu SCP terpusat), atau dalam database terpisah (beberapa SCP) dari setiap atau beberapa jaringan yang berpartisipasi.

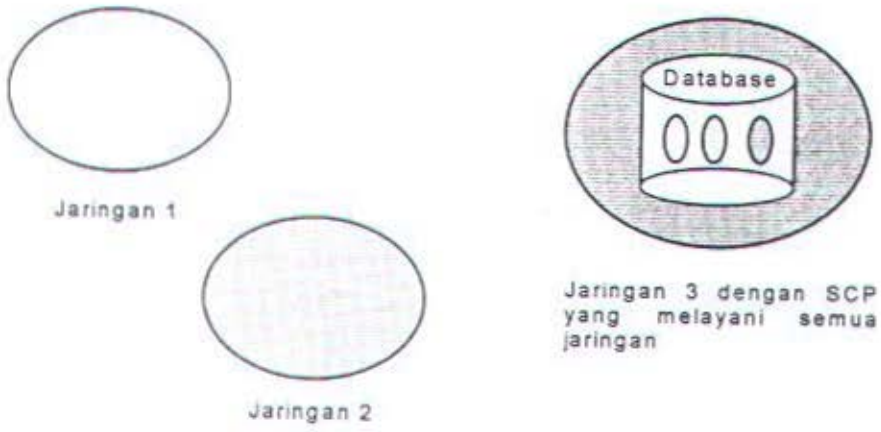
Kemampuan interaksi SCP menghendaki :

- satu jaringan untuk memulai pertanyaan pada jaringan lain untuk mengakses informasi (seperti informasi langsung).
- jaringan yang menerima pertanyaan untuk memeriksa masa berlakunya untuk alasan keamanan dan untuk merespon pertanyaan.

- pertanyaan melewati kontrol mekanisme.

III. 5. 4. SCP Tunggal Melewati Semua Jaringan

Pada kemungkinan pertama arsitektur untuk merealisasikan IVPN ini, tunggal, SCP terpusat akan melayani banyak jaringan. Untuk jaringan atau penyedia jasa yang tidak memiliki jaringan SCP terdedikasi, service intelijen tertentu pelanggan awalnya dapat disimpan dalam jaringan SCP yang lain. Dari pengelola dan operasional yang diharapkan, jaringan mandiri yang terlibat dalam penawaran kebutuhan IVPN bertanggung jawab hanya untuk informasi langsung tertentu jaringannya. Gambar 3.5 sebagai contoh konfigurasi jenis ini, saat SCP hanya berada dalam satu jaringan. SCP ini berisi informasi mengenai semua user dalam semua jaringan.



GAMBAR 3.5[27]
SCP TUNGGAL UNTUK SEMUA JARINGAN

[27] Ibid, hal. 26

Untuk semua panggilan yang masuk pada jaringan yang menyediakan SCP, jaringan mengenali panggilan IVPN yang berdasarkan pada identitas grup trunk atau service kode akses yang dibawa oleh jaringan pengirim. Jaringan akhir akan menjalankan lookup database untuk pengolahan lebih lanjut (seperti screening, routing).

Untuk semua panggilan yang keluar dari jaringan yang memproses SCP, jaringan menjalankan lookup database untuk menentukan screening panggilan dan informasi routing sebelum membawa panggilan ke jaringan yang lain. Konfigurasi ini membuat kemungkinan pengenalan service menjadi cepat untuk para user dari semua jaringan yang berpartisipasi.

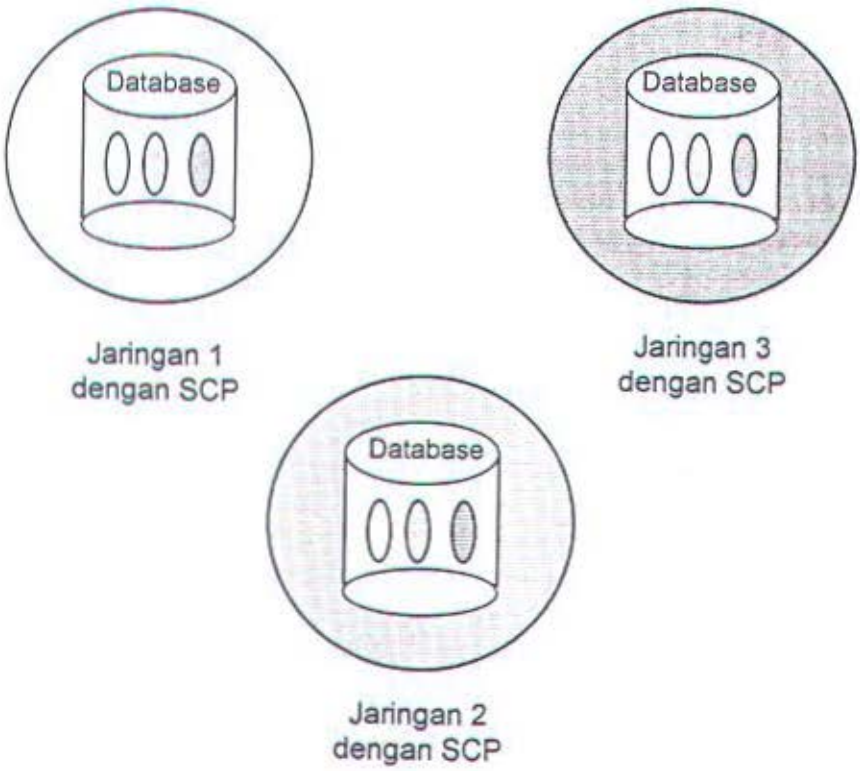
III. 5. 5. SCP Terpisah Dalam Beberapa Jaringan

Untuk jaringan yang berpartisipasi atau penyedia jasa yang menyebar sendiri database jaringannya sebagai hasil dari konfigurasi IVPN berisi lebih dari satu database. Jadi SCP yang diimplementasi dalam setiap jaringan, berisikan informasi tentang semua user dalam semua jaringan. Keuntungan dari jenis konfigurasi ini adalah bahwa pengolahan panggilan IVPN selalu dapat diselesaikan di jaringan pemanggil.

Bagaimanapun juga jika tiap database berisi service logic tertentu pelanggan pada user dari semua jaringan, pengelola harus memelihara ketetapan informasi database yang mendekati waktu sesungguhnya yang akan meninggi saat jumlah dari jaringan yang berpartisipasi yang memiliki service

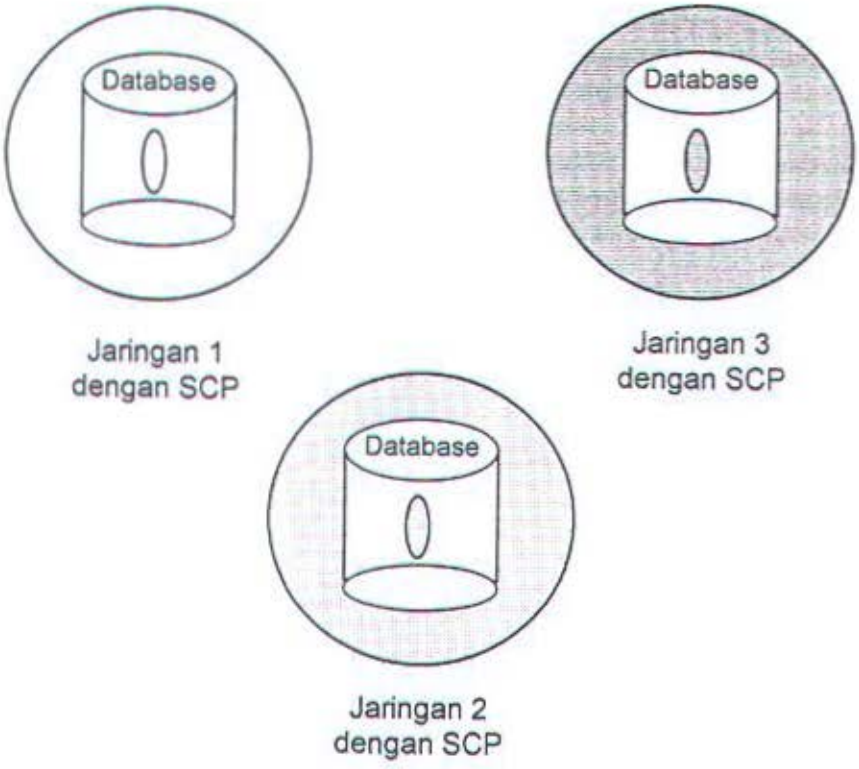
IVPN meningkat. Gambar 3.6 menjelaskan konfigurasi jenis ini, saat tiap SCP berisi informasi pada user dari semua jaringan.

Solusi untuk masalah pengelolaan dan penyediaan service ini adalah mengijinkan setiap jaringan untuk bertanggung jawab atas service intelijen tertentu pelanggan hanya untuk user pada jaringan tersebut. Kemudian, setiap jaringan yang berpartisipasi dapat secara efisien mengelola service intelijen tertentu pelanggan untuk usernya. Gambar 3.7 sebagai contoh konfigurasi ini, saat setiap SCP berisi informasi pada user dari jaringannya sendiri.



GAMBAR 3.6[28]
SCP DALAM SETIAP JARINGAN DENGAN INFORMASI TENTANG SETIAP USER

[28] Ibid, hal. 27



GAMBAR 3.7[29]
SCP DALAM SETIAP JARINGAN DENGAN INFORMASI TENTANG SETIAP USER

Bagaimanapun juga, data PNP digandakan dan ditemukan dalam semua SCP.

III. 6. VPN CALL

Panggilan VPN diaktifkan oleh service user. Kode akses layanan tertentu, ditujukan ke service VPN, harus didial guna men-trigger service. Service

---

[29] Ibid, hal. 28

user harus secara alami sadar akan kode ini.

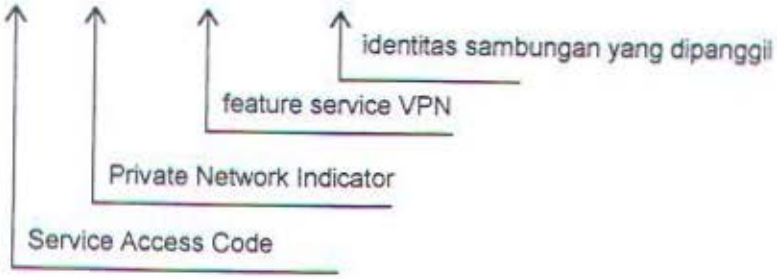
Ketika user milik lebih dari satu grup VPN, user harus memutar suatu digit yang disebut Private Network Indicator (PNI) untuk menunjukkan grup VPN mana yang akan user akses. Jika user hanya milik satu grup VPN, user tidak harus memutar digit ini. Jika feature tambahan (misalnya ABD, FOO) juga menghendaki digit ini, maka kode service tambahan juga harus ditambahkan pada aliran digit. Untuk melengkapi deretan sambungan user harus memutar nomor PNP dari sambungan yang dipanggil. Beberapa kemungkinan lain ialah untuk contoh nomor abbreviated atau nomor E164. Habisnya waktu interdigital akan memberi sinyal untuk mengakhiri sambungan.

Dari sudut pandang jaringan dapat disimpulkan bahwa panggilan VPN tertentu, setelah diketahui bahwa ada panggilan VPN, pertama discreen oleh SCP untuk validitasnya, pembatasannya, setelah itu digit yang diputar diolah oleh SCP. Pengolahan ini dapat berupa translasi dari nomor PNP ke dalam nomor routing, yang dapat berupa nomor E164 pada nomor routing tertentu pelanggan atau nomor routing tertentu jaringan.

Deretan sambungan yang berbeda digambarkan dala gambar berikut. Perbedaan-perbedaannya yaitu presentasi dari kode feature service VPN dan jenis nomor sambungan yang dipanggil.

Hanya range digit pertama yang ada dalam gambar. Untuk beberapa service feature, seperti Remote Access, Override Restriction, user diminta oleh jaringan intelijen untuk memperkenalkan lebih lanjut, tambahan informasi (misalnya kode otorisasi). Range digit selanjutnya ini tidak ditunjukkan disini.

VPN call no features	: SAC + (PNI) + + PNP number
Remote access call	: RMTA + SAC + VPN group identity
Override restriction	: SAC + (PNI) + + PNP number
Account code call	: SAC + (PNI) + ACC code + ACC number
Forced on net call	: SAC + (PNI) + FOO code + E164 number
Abbreviated dialling	: SAC + (PNI) + ABD code + ABD number



GAMBAR 3.8[30]
NOMOR VPN YANG DIDIAL (CONTOH)

Indikator Jaringan Pribadi ialah nomor referensi yang menunjukkan identitas grup VPN. Misalnya PNI = 1 maka identitas grup VPNnya adalah 1357.

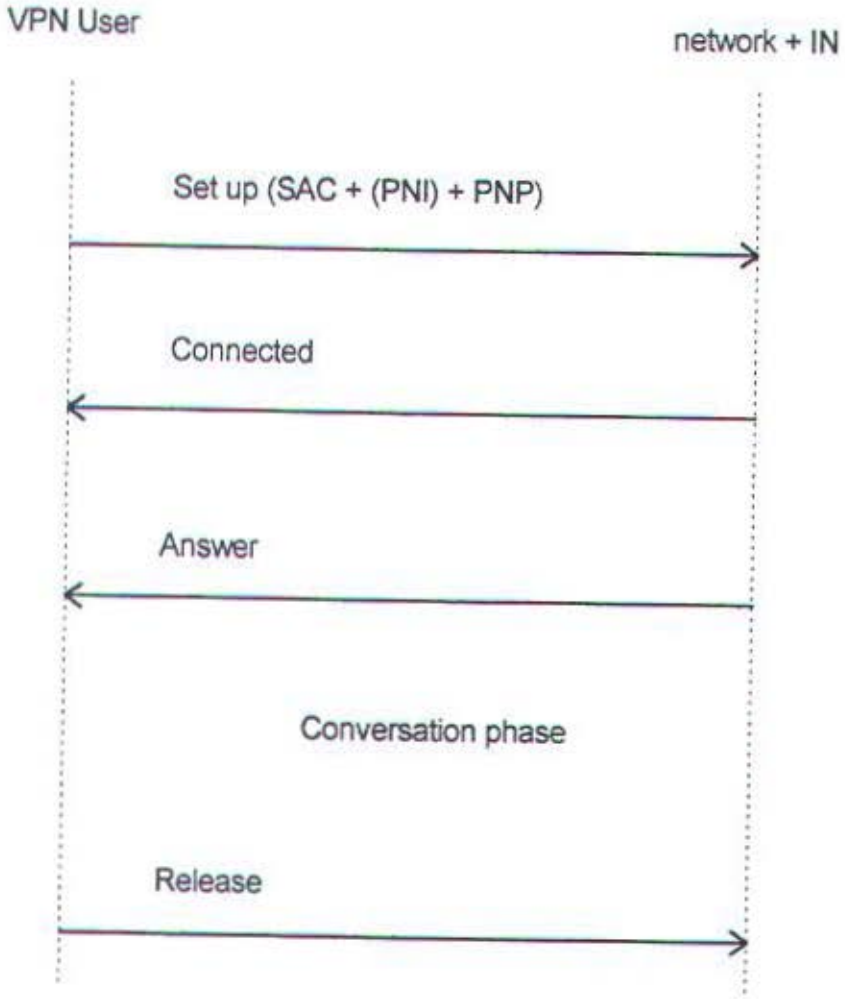
Remote Access : Adanya kemungkinan perbedaan implementasi.

1. Keberadaan kode RMTA yang khusus untuk mengaktifkan feature, seperti untuk feature yang lain.
2. Kode SAC untuk feature ini berbeda dari kode akses service VPN yang normal. Nomor kode RMTA yang khusus digunakan dalam kasus ini. Misalnya SAC untuk RMTA ialah 07899 untuk panggilan nasional; 07099 untuk panggilan internasional, diikuti oleh identitas grup VPN.

---

[30] Ibid, hal. 30

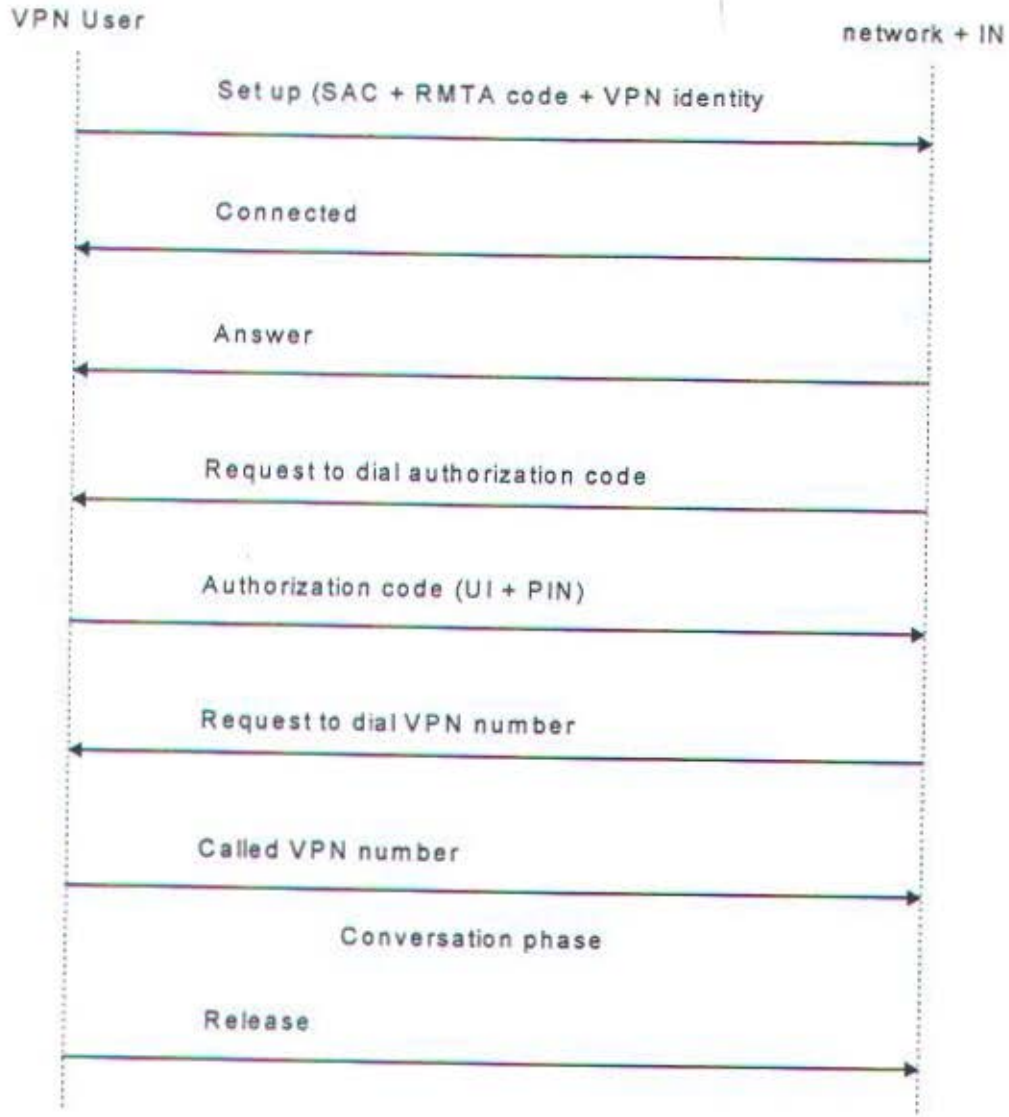
Forced On Net : tergantung pada penerapannya, hal ini mungkin bahwa tidak ada kode FOO eksplisit. Dalam kasus ini awalan dari nomor publik internasional dapat dikenali dan diolah seperti kode FOO. Misalnya nomor publik yang didial ialah 00 33 1 2345 67 89 maka kode FOO adalah 00.



GAMBAR 3.9[31]
CALL VPN TANPA FEATURE

[31] Ibid, hal. 31

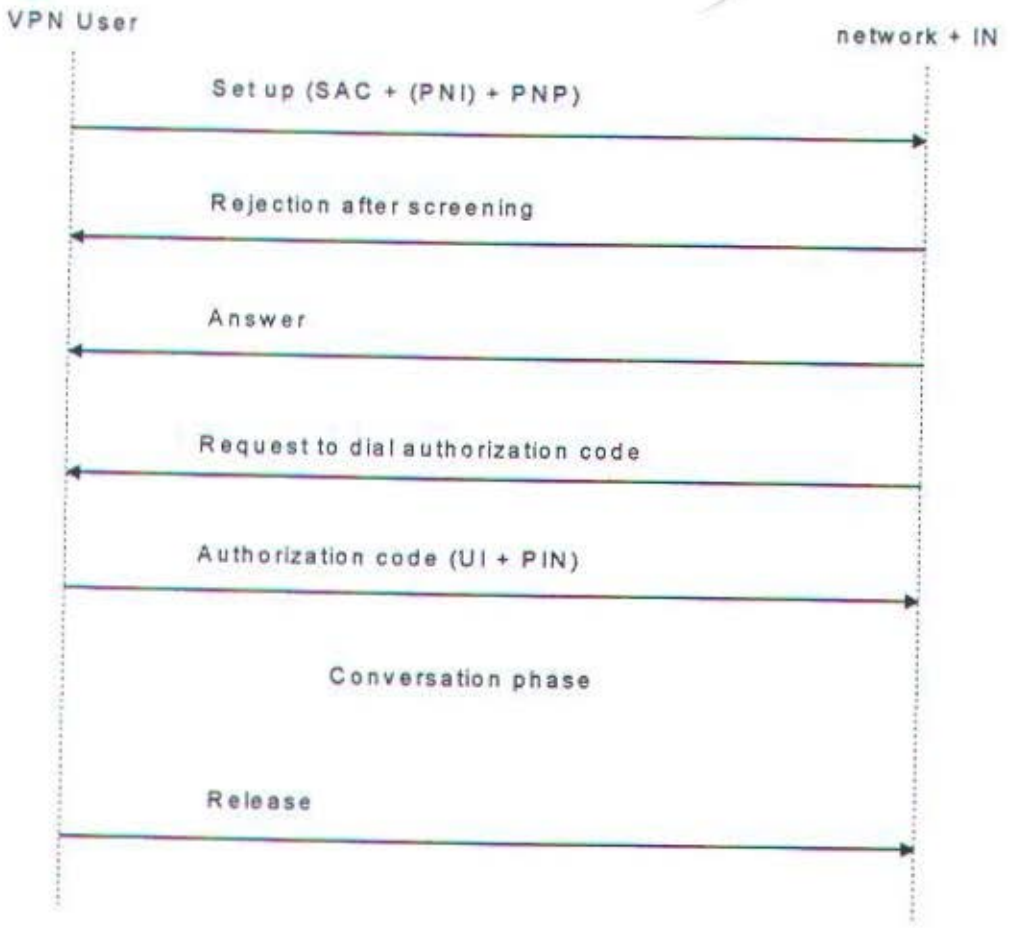
Aliran digit yang diputar memberikan informasi yang cukup untuk SSP dan SCP untuk menangani panggilan. Oleh karena itu tidak ada digit tambahan yang diminta dari user.



GAMBAR 3.10[32]
CALL REMOTE ACCESS

[32] Ibid, hal. 32

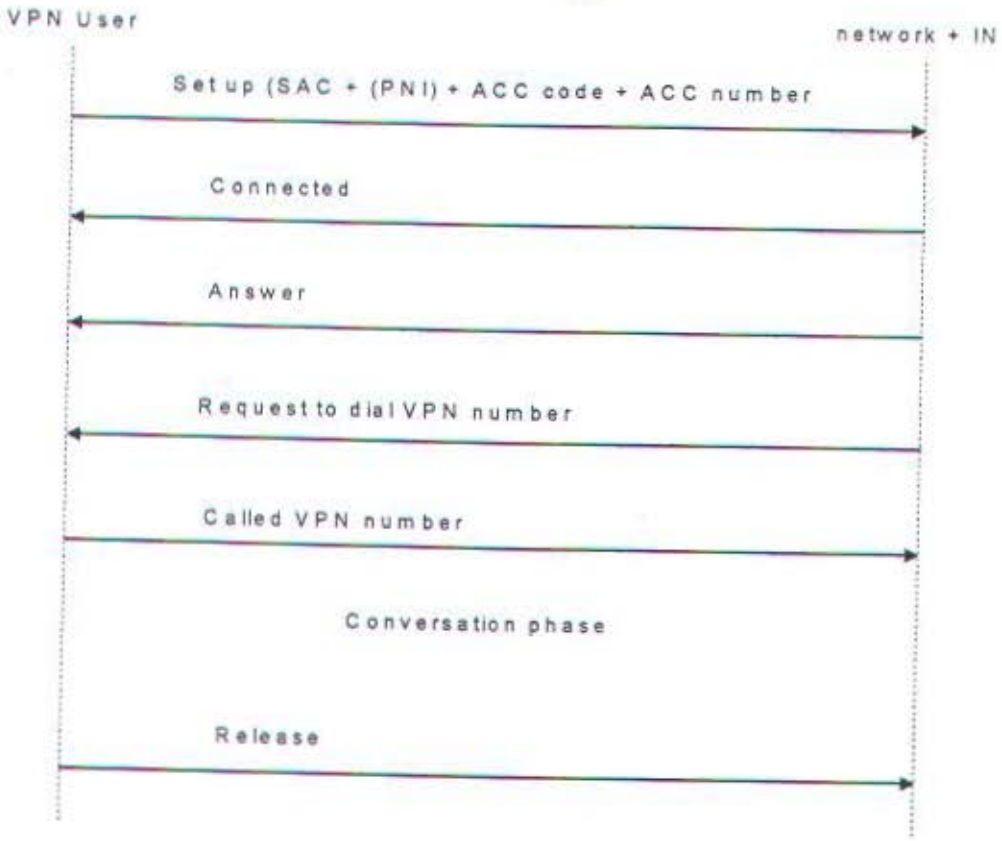
Kode otorisasi berisi User Identity (UI) dan Personal Identification Number (PIN). Nomor sambungan yang dipanggil ditunjukkan sebagai nomor VPN, dapat seperti berikut : nomor PNP, kode feature + nomor feature (misalnya kode ABD + nomor ABD).



GAMBAR 3.11[33]
OVERRIDE RESTRICTION

[33] Ibid, hal. 33

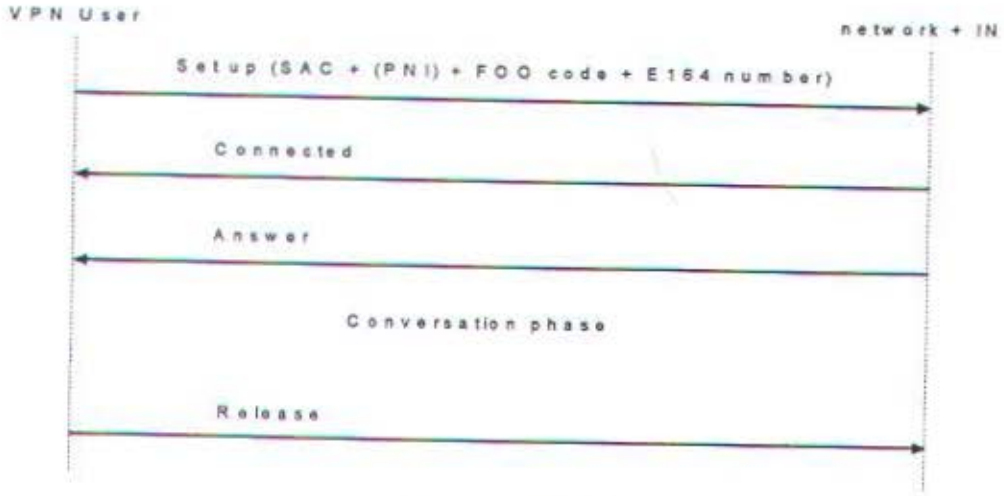
Awalnya, setelah menscreening user akses ditolak pada nomor PNP yang diputar. Bagaimanapun juga user ditawarkan kemungkinan untuk memutar kode otorisasi, yang mana user dapat mengesampingkan pembatasan yang ditentukan. Setelah pengesahan dari kode ini, panggilan berlangsung secara normal.



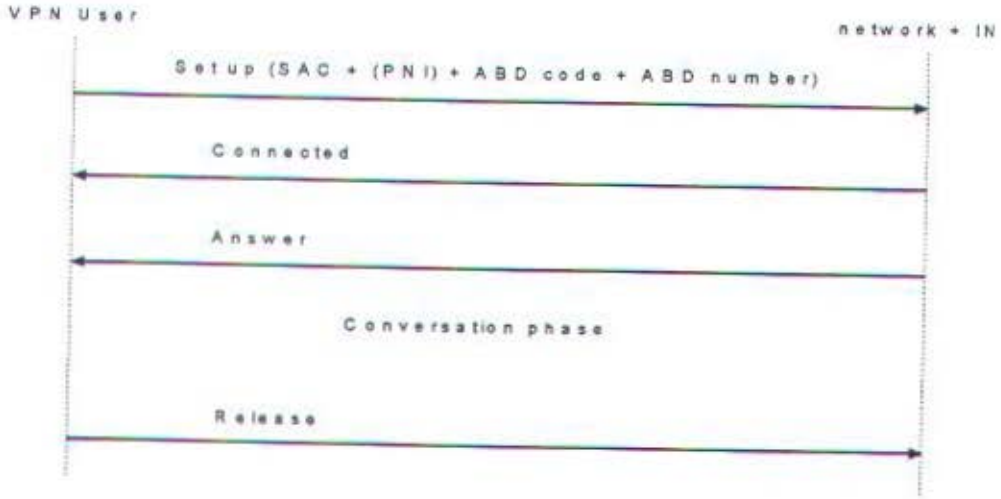
GAMBAR 3.12[34]
ACCOUNT CODE CALL

[34] Ibid, hal. 34

Sekali informasi dihubungkan pada service feature (kode ACC dan nomor) akan diperiksa oleh SCP, user diminta untuk memutar nomor VPN.



GAMBAR 3.13[35]
FORCED ON NET CALL



GAMBAR 3.14[36]
ABBREVIATED DIALLING

[35] Ibid, hal. 35
[36] Ibid, hal. 35

III. 7. SERVICE TRIGGERING DALAM SSP

Service triggering dalam Service Switching Point (SSP) memiliki tiga jenis, yaitu Originating Trigger, Incoming International Trunk dan Incoming National Trunk.

III. 7. 1. Originating Trigger

Originating trigger sendiri memiliki dua macam akses, yaitu :

- Akses langsung ke SSP, seperti dapat dilihat sebelumnya, service user mulai mendial dengan kode akses service VPN (SAC). Mekanisme triggering berdasarkan pada informasi ini. Service user secara langsung dihubungkan ke sentral dengan SSF secara fungsional. Sentral menerima semua digit yang didial oleh service user. Jumlah digit dapat bervariasi, tergantung dari feature service user yang ingin untuk diaktifkan atau PNP yang digunakan. Oleh karena itu aliran digit ini milik rencana penomoran terbuka. Biasanya, jumlah digit berkisar antara 4 dan 18. Ketika waktu interdigital telah habis, maka inilah kesempatan SSP untuk mengirim operasi Provide Instruction ke SCP. Dengan demikian service VPN diaktifkan. SSP juga harus mengirim parameter Calling Party Number dalam operasi Provide Instruction, maka dari itu SCP dapat mengenali user milik dari grup VPN yang mana, untuk melaksanakan screening dan lain-lain.

- Akses tidak langsung ke SSP, pada prinsipnya penerapan dari akses tidak langsung ini sama seperti akses langsung. SSP selalu menerima aliran digit yang utuh. Misalnya, SAC + PNI + PNP. Mekanisme triggering berdasarkan pada kode akses service VPN (SAC).

III. 7. 2. Incoming International Trunk

Incoming international trunk ini memiliki dua jenis link, yaitu :

- Shared Link, ditujukan untuk trafik IVPN, digunakan untuk semua incoming trafik IVPN internasional (panggilan on-net internasional). Mekanisme triggering berdasarkan pada identitas incoming grup trunk. Semua panggilan yang masuk seperti grup trunk akan mentrigger service IVPN. SSP menerima aliran digit sebagai berikut : identitas grup VPN + nomor PNP. Informasi ini dikirim dalam operasi Provide Instruction ke SCP.
- Public Link, panggilan IVPN dapat juga mencapai SSP melalui incoming trunk publik internasional (panggilan off-net internasional). Mekanisme triggering berdasarkan pada kode akses service IVPN, digabung dengan identitas incoming grup trunk. SSP menerima aliran digit sebagai berikut : kode akses IVPN + identitas grup VPN + nomor PNP. Informasi ini dikirim dalam operasi Provide Instruction ke SCP.

Untuk kedua jenis link incoming dalam operasi Provide Instruction :

- Parameter Calling Party Number tidak digunakan.

- Parameter National/International Call Indicator diset pada internasional.

III. 8. ROUTING

Pada dasarnya sekali service(I)VPN diaktifkan, maksud utamanya adalah merouting panggilan sampai ke suatu tujuan. Jaringan mungkin mempunyai rencana routing yang digunakan untuk panggilan (I)VPN. Ini berarti bahwa panggilan (I)VPN dirouting pertama kali melalui dedicated trunk. Jika hal ini tidak mungkin (dedicated trunk tidak ada atau mengalami kegagalan), maka pilihan berikutnya ialah merouting panggilan melalui shared trunk. Jika hal ini juga tidak mungkin, maka panggilan dirouting melalui trunk publik.

Service VPN memiliki kemungkinan untuk menyatakan pada jaringan atas basis 'per call' dari rencana routing (rencana routing normal atau VPN) yang mana yang digunakan. Hal ini dicapai melalui penggunaan parameter Reserved Trunk Indicator dalam operasi Create. Secara bebas, identitas grup VPN akan ditentukan dalam operasi Create untuk mengijinkan pemilihan dedicated trunk untuk grup VPN tertentu ini.

Pengaturan routing untuk telekomunikasi internasional memiliki dua elemen yang penting guna menunjang suksesnya panggilan VPN, yaitu circuit dan format nomor routing internasional. Untuk circuit, semua jenis circuit harus tersedia atau siap pakai untuk merouting panggilan-panggilan VPN internasional. Sedangkan format nomor routing internasional mempunyai dua bagian, yakni

inbound dan outbound. Untuk format nomor routing internasional inbound adalah sebagai berikut :

KP(1) + 179 + CID(3digit) + XXX XXXX(7digit)

Sedangkan untuk format nomor routing internasional outbound adalah sebagai berikut :

KP(1) + SID + CID + XXX XXXX

seperti diketahui bahwa SID ialah Service ID yang panjangnya antara 3 sampai dengan 5 digit, CID adalah Customer ID yang panjangnya 3 sampai 4 digit dan XXX XXXX yang merupakan nomor private atau pribadi yang panjangnya 7 digit.

III. 9. ANALISA EKONOMI

Paket biaya VPN adalah tarif yang tidak standar yang dipotong dan ditujukan pada kelompok pelanggan tertentu. Walaupun layanan ini difokuskan pada layanan suara, hal tersebut tetap dianggap bahwa biaya VPN adalah bagian dari paket biaya multi service.

Pemakai layanan VPN ingin mengurangi biaya telepon. Perusahaan tak akan memakai VPN bila biayanya melebihi biaya telepon, walaupun ada feature dan fasilitas tambahan. Karenanya, masalah harga layanan sangat diperhatikan bila pemakai menelaah layanan VPN dari penyelenggara jasa.

Pengurangan harga yang dikaitkan dengan perkenalan VPN akan mengurangi keuntungan penyelenggara, kadang-kadang sampai batas yang tak

dapat diterima. Karena itu penyelenggara jasa tidak hanya harus menawarkan potongan kepada pelanggannya, tetapi juga harus menambah investasi baru pada infrastruktur jaringan dan fasilitas untuk layanan VPN. Tapi pada pasar kompetitif, penyelenggara jasa tidak mempunyai pilihan lain. Mereka harus menawarkan layanan itu kalau ingin mempertahankan pangsa pasar. Paket biaya adalah alat dasar penyelenggara jasa untuk menyeimbangkan keuntungan terhadap pangsa pasar. Dalam merancang paket biaya, pihak penyelenggara harus mempertimbangkan kebutuhan :

a. pemakai, untuk meningkatkan pangsa pasar
b. diri sendiri, untuk meningkatkan keuntungan
c. pengaturan, untuk dapat bertahan

Ditinjau dari kebutuhan pemakai ada beberapa unsur yang perlu diperhatikan, yaitu :

1. Penurunan Biaya

Pemakai ingin mengurangi pengeluaran untuk telepon suara. Kebanyakan pengurus telekomunikasi mempunyai kendala untuk menambah budget telekomunikasi secara keseluruhan. Beberapa menghadapi pengurangan budget. Dilema untuk kebanyakan pengurus telekomunikasi ialah bahwa dengan kendala-kendala ini mereka harus menampung ledakan pertumbuhan komunikasi data. Untuk pelanggan perusahaan besar, penggantian komputer mainframe ke sistem layanan klien, akan mengakibatkan kenaikan berarti dalam jumlah trafik data, terutama LAN ke LAN, dengan volume tinggi dan

sifat tak dapat diramalkan. Pengeluaran untuk telepon suara diteliti ketat, sehingga penghematan pada suara dapat menutupi biaya data tambahan. Kebanyakan perusahaan merasa bahwa mereka ditagih lebih untuk layanan suara. Pada kebanyakan pasar, layanan suara tetap di bawah kendali tunggal sampai sekarang. Perusahaan percaya, dengan justifikasi tertentu bahwa mereka kelebihan tagihan untuk telepon suara sampai 50% dan waktunya sudah tiba untuk mengupayakan keseimbangan. Kini ada harapan baru bahwa tarif akan turun.

2. Stabilitas Harga

   Perusahaan besar ingin mengetahui proporsi terbesar dari biaya di masa yang akan datang. Paket biaya VPN dikombinasi dengan kontrak yang menawarkan suatu jadwal biaya total yang diketahui selama beberapa tahun, adalah menarik. Pada saat yang sama, perusahaan menyadari bahwa biaya suara secara umum akan turun di tahun-tahun mendatang sehingga mereka tak mau menerima jadwal jangka panjang yang mengikat mereka pada biaya awal yang tinggi. Kebanyakan pelanggan besar dengan kebutuhan data cukup besar mencari kontrak yang memberikan pada mereka harga yang stabil untuk seluruh layanannya. Mereka ingin kembali menyeimbangkan harga suara yang menurun terhadap biaya data yang berkembang.

3. Pelanggan Berharga

   Organisasi besar ingin merasa sebagai pelanggan khusus. Mereka mengeluarkan uang banyak pada penyelenggara jasa dan ingin perlakuan yang setara. Paket biaya VPN yang memenuhi kebutuhan khusus mereka, dan yang melebihi kondisi dan kebiasaan normal yang ditawarkan

penyelenggara jasa, memenuhi perasaan itu. Namun ada batasnya, seberapa jauh penyelenggara dapat memanjakan pelanggan besar, sebelum pengatur menyadari bahwa hal itu akan merugikan pelanggan kecil.

Pelanggan ingin mempunyai kemitraan khusus dengan suppliernya, terutama bila pelanggan menginginkan multiple service dengan penyelenggara dalam suatu kontrak tunggal. Pelanggan tahu bahwa biaya akan mahal untuk pindah antar supplier, bila penyelenggara gagal memberikan harga layanan atau kinerja yang dijanjikan. Karena itu banyak perusahaan menuntut, bahwa pihak penyelenggara menjamin bahwa akan tetap sebagai supplier terbaik.

4. Memanfaatkan Daya Beli

Perusahaan besar biasanya menerima potongan volume besar untuk sebagian besar pembeliannya dari supplier. Harapannya dari supplier telekomunikasi sama saja. Namun, penyelenggara dominan dalam pasar yang mengalami deregulasi, terbatas kemampuannya dalam menawarkan potongan volume. Merancang paket biaya yang mengatur harapan dari pelanggan besar mungkin adalah salah satu tantangan tersulit dari penyelenggara jasa baru.

Ditinjau dari kebutuhan komersial penyelenggara jasa ada beberapa unsur yang perlu diperhatikan :

1. Pendapatan Bersih yang Positif

Penyelenggara jasa prlu memastikan bahwa paket biaya VPN-nya adalah komersial. Tekanan dari pelanggan besar untuk potongan volume sulit ditolak dan seringkali dapat melampaui kebutuhan evaluasi komersial yang keras. Paket biaya yang tak dibenarkan atas dasar komersial mengakibatkan perang

harga yang makin meningkat. Kebutuhan untuk lolos tes pendapatan bersih adalah pusat dalam paket biaya. Tes pendapatan bersih menentukan bagaimana perkenalan paket biaya baru mengubah baiya dan pendapatan penyelenggara. Apabila efek pengenalan paket baru positif, maka paket adalah komersial. Bila negatif, alasan untuk memperkenalkan paket baru harus sangat kuat. Pertimbangan kualitatif utama untuk pihak penyelenggara baru seperti itu adalah :

a. memakai biaya paket akan menghambat pelanggan baru, yang tentunya memfokuskan pada pelanggan besar. Pelanggan baru akan mencari paket yang sesuai atau lebih baik biaya paket yang dipotong, untuk menjaga kelangsungan bisnisnya.
b. mengunci pelanggan pada layanan dasar yang dapat merupakan fundamen untuk penyelenggara dalam menawarkan layanan lebih mahal. Misalnya banyak penyelenggara jasa mengharap mendapat tambahan pendapatan dari layanan lebih mahal, seperti call centre support diatas layanan dasar VPN.
c. membantu memenuhi keinginan pelanggan besar dan dengan begitu mengurangi tekanan politis pada penyelenggara dari lobby yang kuat ini.
d. mengurangi ancaman pelanggan besar untuk membangun jaringan pribadi sendiri sehingga nilai layanan penyelenggara bergeser.

Paket biaya multi service, multi lokasi jangka panjang memungkinkan penyelenggara memerangi kompetisi dengan mencegah larinya pelanggan pada layanan atau jalur tertentu. Sebagai contoh, penyelenggara dapat melawan re-seller, karena walupun re-seller mampu menawarkan harga lebih

rendah untuk layanan suara untuk 2 atau 3 daerah besar, penyelenggara dapat memberikan harga menyeluruh yang lebih baik apabila semua daerah (dan semua layanan) diperhitungkan dalam paket biaya.

2. Kendali Account Lebih Baik

Hubungan berharga tidak hanya penting bagi pelanggan, bahkan lebih penting untuk penyelenggara jasa. Mengerti dan mengadakan kontak dengan lapisan banyak dalam perusahaan memungkinkan penyelenggara meramalkan kebutuhan perusahaan itu dan mempersiapkannya lebih dahulu. Hal ini memungkinkan penyelenggara merancang paket biaya untuk pelanggan individual berdasar pengertian penuh dari posisi komersial pelanggan, dengan demikian membantu mencapai loyalitas pelanggan jangka panjang.

3. Kendali Harga Masa Depan

Kebanyakan harga VPN dibuat dengan acuan harga yang ada dari PSTN atau IDD. Di seluruh dunia ada kecenderungan menurun dari harga-harga ini, terutama di negara-negara dimana harga dibuat terlalu tinggi. Bila harga telepon menurun, paket biaya VPN yang menawarkan potongan besar terhadap harga telepon, akan merugi. Karena itu setiap paket biaya VPN harus mempertimbangkan pelepasan diri dari tarif IDD dan PSTN.

Ditinjau dari kebutuhan pengaturan mempunyai beberapa unsur antara lain :

1. Tanpa Perbedaan

Pengatur harus diyakinkan bahwa komponen kunci dari paket biaya VPN penyelenggara dominan tersedia sama untuk semua pelanggan pada

keadaan yang sama. Khususnya tiap potongan volume yang ditawarkan oleh penyelenggara dominan perlu diterbitkan dan dapat diperoleh di seluruh negeri.

Persoalan diskriminasi lain yang memaksa penyelenggara bersikap ialah adanya potongan volume yang ditawarkan re-seller dan integrator sistem. Re-seller dapat saja mengurangi keuntungan penyelenggara jasa.

2. Tanpa Subsidi Silang

Pengatur perlu diyakinkan bahwa potongan volume terutama di kontrak multi service tidak disubsidi oleh pelanggan kecil yang memakai layanan yang sama atau layanan yang lain. Untuk menguji persoalan ini, pengatur memakai 2 macam tes pendapatan bersih :

a. before & after test. Yang diuji harus menunjukkan bahwa ada peningkatan pendapatan. Tes ini nyata tetapi ada 2 kelemahannya :
   - penghasilan bersih mungkin dikaburkan oleh pasar yang meningkat cepat.
   - pengatur memperbolehkan paket tarif khusus sebelum tes dapat dilaksanakan.

b. with & without test. Yang diuji harus menunjukkan bahwa pendapatannya akan bertambah dengan paket khusus dari pada tidak dengan paket khusus. Misalnya pendapatan menurun tapi akan lebih cepat menurun bila tanpa paket tarif khusus.

3. Tidak Anti Kompetisi

Acuan pengatur adalah kompetisi telekomunikasi. Regulator harus mengawasi pemakaian carrier dominan mencapai posisinya. Dalam keadaan

ini pengatur menguji paket biaya untuk mengetahui apakah merugikan kompetisi sampai merugikan pemakai. Khusus ini berarti menilai apakah paket harga pre empts competition atau menggunakan harga predatory yaitu menawarkan potongan volume untuk mencapai harga di bawah biaya minimal. yang terakhir diuji dengan tes pendapatan bersih yaitu per definisi, pendapatan bersih positif tak mungkin dicapai bila potongan volume didasarkan atas harga di bawah biaya marginal.

Komponen paket biaya adalah sebagai berikut :

- tagihan layanan individual, misalnya untuk VPN.
- potongan volume layanan individual, misalnya potongan untuk layanan VPN.
- potongan pengeluaran multi service.
- persetujuan kontrak.

Dalam membuat paket biaya perlu diketahui 3 hal sebagai berikut :

- merupakan cara terbaik untuk memenuhi kebutuhan pelanggan.
- secara komersial baik untuk penyelenggara jasa.
- memenuhi aturan main.

Paket biaya VPN harusnya menarik untuk pelanggan. Keuntungannya yang utama ada 3 macam, yaitu :

a. mengurangi pengeluaran telepon suara dari pelanggan secara keseluruhan.
b. memberikan harga stabil dan biaya yang dapat diramalkan.
c. memberikan pada pelanggan perasaan diistimewakan.

Dari sudut pandang komersial penyelenggara jasa, tes utama untuk paket biaya VPN yang diajukan ialah apakah penyelenggara akan meningkatkan pendapatan. Untuk itu paket biaya harus melakukan satu atau lebih dari hal berikut ini :

- membendung kerugian pada pesaing eksternal maupun internal.
- merangsang pemakaian untuk mengimbangi kerugian dari pendapatan unit.
- memungkinkan penyelenggara membuat pemakaiannya lebih fleksibel.

Untuk regulator, paket biaya VPN harus memenuhi 3 kriteria, yaitu tak ada diskriminasi, tak ada subsidi silang dan tak ada feature anti kompetisi.

III.9.1. Tagihan Layanan VPN

Tagihan pemakaian VPN berkaitan erat dengan harga telepon. Seringkali harga VPN adalah potongan langsung atas dasar harga telepon. VPN hanya dapat berkembang pada pasar kompetitif. Pengalaman dari pasar-pasar yang mengalami deregulasi selama 10 tahun terakhir menunjukkan bahwa persaingan memaksa penyelenggara jasa untuk bergerak ke penentuan harga atas dasar biaya. Muncul 3 kecenderungan, yakni :

a. tagihan pemakaian variabel menurun relatif terhadap tagihan tetap. Tagihan pemakaian menurun lebih cepat pada pasar kompetitif dibanding pada pasar non kompetitif. Di lain pihak, tagihan tetap rata-rata lebih tinggi dalam pasar kompetitif.

b. tagihan internasional dan jarak jauh turun terhadap tagihan lokal. Ini karena para pesaing menganggap internasional dan jarak jauh lebih dulu, lebih menguntungkan, lebih mudah aksesnya dan paling sedikit dasar biayanya.
c. biaya layanan secara keseluruhan menurun.

Selain 3 kecenderungan ini, kompetisi di pasar global memaksa harga internasional menjadi seragam. Ketidaksamaan harga antara tagihan-tagihan internasional akan berkurang, karena :

- re-seller dan operator call-back akan memanfaatkan ketidaksamaan ini secara maksimal.
- Pelanggan domestik baru akan mengarah ke layanan internasional sebagai layanan paling menguntungkan dengan akses paling mudah.

Tagihan layanan individu terdiri atas :

- Tagihan non recurrent. Ini meliputi tagihan untuk sambungan layanan, pengadaan akses dedicated atau switched, pengadaan feature dan rencana penomoran pribadi dan tagihan yang berkaitan dengan rekonfigurasi dari peralatan pelanggan (seperti PBX).
- Tagihan fixed recurrent. Ini meliputi tagihan akses untuk sambungan sewa dedicated, tagihan langganan service VPN dan tagihan untuk kontrak khusus pemeliharaan langganan.
- Tagihan variable recurrent. Tagihan untuk per menit panggilan untuk layanan pemakaian VPN, yang berdasar pada jarak atau jalurnya.

Kebutuhan primer penyelenggara jasa dari paket biaya ialah bahwa

mereka akan mengendalikan harga dikemudian hari. Karena itu penyelenggara berusaha melepaskan harga VPN dari harga telepon, karena harga telepon yang begitu tinggi, sulit untuk turun. Selama masa penurunan harga cepat, penyelenggara dapat kehilangan kendali terhadap harga-harga.

Namun tak begitu mudah melepaskan harga VPN dari harga telepon. Pemakai mengharap biaya panggilan VPN lebih rendah dari telepon. Karena itu dianjurkan pada penyelenggara VPN untuk mengarah ke harga telepon secara leap-frog yaitu membuat struktur harga VPN yang menggambarkan harga telepon di masa depan.

Bila harga telepon pasti menjadi dasar biaya dalam pasar kompetitif, penyelenggara dapat meramalkan tingkat dan struktur dari harga-harga ini dalam 5 tahun. Dengan menyusun struktur harga yang menggambarkan harga telepon di masa depan bila diubah berdasar atas biaya, penyelenggara tak perlu kuatir lepas kendali atas harga-harga di masa depan, walaupun suatu ketika harga telepon sama dengan harga VPN, karena itu dianjurkan agar :

- Paket dasar biaya VPN kembali menyeimbangkan harga akses dan harga pakai terhadap biaya.
- Penyeimbangan kembali dilakukan antara harga panggilan internasional, jarak jauh dan lokal untuk menggambarkan biaya.
- Operator global membuat tagihan panggilan internasional atas dasar jarak dan tidak atas dasar negara, sehingga tarif VPN tidak terikat pada tarif lokal telekomunikasi di negara asal. Bila tarif internasional sudah seragam, operator global bergerak ke arah pemberian harga "perangko", dimana

panggilan dalam satu wilayah diberi harga sama, tak peduli jarak negara asal.

- Pada setiap saat, pengeluaran keseluruhan pelanggan VPN harus kurang dari pengeluaran setara pada telepon.

Semua panggilan memulai dari jaringan ke service VPN akan dikenai biaya di tingkat SSP. Kemudian dalam kasus akses user yang diswitch, pada panggilan sentral lokal dengan kode akses service VPN harus bebas dari tagihan. Penentuan charging dilakukan oleh SSP yang meliputi :

- Parameter charging diberikan untuk setiap grup VPN dan untuk setiap tujuan.
- SCP dapat menyesuaikan penentuan tagihan SSP atas persetujuan SSP, melalui operasi Update, dengan informasi tambahan pada parameter tagihan.

Pembangkitan tagihan dan pencatatan tagihan dilakukan oleh SSP. Pencatatan tagihan pada SSP awal berisi :

- Jenis akses awal : langsung atau tidak langsung
- Jenis akses akhir : langsung atau tidak langsung
- Jalur histori : Sumber VPN dedicated atau sumber Public Switched Telephone Network (PSTN) yang digunakan untuk merouting panggilan.

SSP mengirim operasi Update ke SCP pada akhir dari setiap panggilan dengan informasi tagihan. Informasi ini akan digunakan dalam Service Management Point (SMP) untuk tujuan statistik.

III.9.2. Potongan Volume VPN

Prinsip potongan adalah memberi nilai uang pada hubungan pelanggan dan merangsang pelanggan untuk meningkatkan volume bisnisnya juga memakai skala ekonomi untuk pemanfaatan maksimal untuk pelanggan maupun supplier. Selain memberi potongan pada tagihan pemakaian dasar (bila dibandingkan dengan dengan pelayanan alternatif), potongan VPN dapat didasarkan atas :

- pemakaian VPN pada masing-masing daerah, dengan memberi potongan pada jumlah panggilan dari masing-masing daerah. Potongan ini efektif untuk melawan re-seller yang biasanya mempunyai sasaran daerah luas saja.
- jumlah pemakaian VPN, dengan memberi potongan pada pemakaian pelanggan secara keseluruhan oleh pelanggan. Ini mampu mencegah pelanggan baru untuk menyerobot jalur, terutama yang internasional. Pelanggan mendapat harga lebih baik dari operator global karena potongan atas pemakaian menyeluruh akan lebih baik dan lebih besar dari pada potongan dari pelanggan baru yang hanya meliputi beberapa daerah terbatas.
- jumlah pengeluaran pelanggan atas semua layanan penyelenggara jasa, yang memungkinkan operator dengan macam pelayanan yang luas (terutama yang berkewajiban dan operator global baru) untuk melawan pemberi layanan tunggal.
- masa kontrak, yang memungkinkan kenaikan potongan untuk volume bisnis yang disetujui selama masa yang lebih panjang.

Potongan volume VPN berlaku untuk pengeluaran atau volume panggilan pada daerah individual atau jalur tertentu antar daerah, untuk jumlah panggilan on net dan off net, atau untuk jumlah panggilan domestik dan internasional. Potongan volume dapat berubah bertahap atau secara kontinyu.

Potongan berlanjut dengan jumlah bervariasi memberikan kenaikan yang mulus dari potongan bila pemakaian bertambah. Rencana potongan terbatas meningkatkan potongan pada tahap-tahap yang sudah ditentukan. Keputusan dini dalam merancang rencana harga VPN adalah apakah potongan akan berubah secara kontinyu atau bertahap. Walaupun kebanyakan rencana kini memakai variasi bertahap, variasi kontinyu mempunyai beberapa keuntungan :

- pelanggan dan regulator dapat menganggap lebih adil, karena menghindari pembuatan tahap yang berubah-ubah.
- dapat membantu pelanggan untuk meramalkan lebih tepat pengeluarannya.

Potongan bertahap merangsang pelanggan untuk pindah dari satu supplier ke yang lain untuk mendapat potongan terbesar. Beberapa penyelenggara percaya bahwa potongan bertahap merangsang pelanggan untuk lebih banyak memakai layanan. Ini tidak benar, karena kebiasaan pemakai telepon sulit dipengaruhi oleh potongan yang diterima dari bagian-bagian telekomunikasi.

Sesudah menentukan kerangka rencana potongan, berapa jumlah yang akan dimasukkan :

- Potongan awal dibawah 5% tidak wajar. Ini merupakan ambang, potongan dibawahnya dianggap tidak artinya.
- Pihak multi nasional mengharap potongan sedikitnya 10% dan sampai 30% dibawah tarif serupa terbaik dari telekomunikasi lokal.
- Tahap-tahap potongan biasanya adalah angka bulat yang mudah diingat, misalnya $ 100.000. Tiap tahap dalam struktur potongan bertahap biasanya 2 kali dari tahap sebelumnya.

Potongan pengeluaran multi service berlaku untuk pengeluaran seluruhnya dari pelanggan pada penyelenggara jasa. Ini dapat meliputi hanya layanan suara, misalnya VPN, PSTN dan layanan 800, atau semua layanan termasuk suara, data dan mobile.

Tiga macam layanan dasar dapat dimasukkan dalam paket biaya VPN :

a) Layanan VPN tunggal.
b) Sekelompok layanan suara. Layanan ini dapat meliputi layanan VPN maupun PSTN dan layanan 800.
c) Semua layanan telekomunikasi.

Keuntungan menawarkan potongan multi service adalah bahwa penyelenggara membangun hubungan strategis khusus dengan pelanggannya. Ini memungkinkan penyelenggara mencegah pelanggan mencuri pakai daerah atau layanan individual.

Kerugian dari potongan multi service adalah :

- tujuan komersial untuk layanan berbeda mungkin sangat berbeda, sehingga

tidak cukup produktif untuk mengimbangi rencana potongan.

- regulator tak mudah diyakinkan akan justifikasi biaya untuk rencana potongan kombinasi.

Struktur organisasi banyak penyelenggara menyulitkan persetujuan internal untuk potongan antar layanan. Kebanyakan penyelenggara diorganisasikan sekitar layanan dan bukan di sekitar pelanggan, seringkali dengan bagian yang terpisah antara layanan data dan layanan suara. Dalam hal ini, integrasi layanan dicapai pada tingkat manager accounting, yang masih punya kewenangan untuk menawarkan potongan antar layanan.

III.9.3. Persetujuan Kontrak

Kesepakatan kontrak adalah kontrak antara penyelenggara jasa dan pelanggan. Hal ini meliputi layanan yang ditawarkan pada pelanggan meliputi semua daerahnya. Pelanggan menyetujui untuk tingkat pelayanan minimum dari layanan tertentu dalam suatu periode tertentu, misalnya 3-5 tahun. Bila pemakaian kurang dari batas minimum, pelanggan membayar untuk jumlah minimum yang sudah disepakati atau harus didenda. Sebaliknya, penyelenggara jasa menyetujui kondisi yang tidak standar dalam memberikan layanan tertentu. Ini dapat meliputi :

- potongan volume atas tarif standar.
- stabilitas harga atas dasar tahunan atau periode tertentu.
- jaminan terhadap mutu dan ketersediaan layanan.

- fasilitas tagihan khusus.
- fasilitas pemeliharaan pelanggan khusus, seperti kontrak tunggal.
- janji untuk pindah ke layanan baru bila ada.

Adalah penting membedakan term agreement dan potongan volume. Kontrak tak perlu meliputi potongan volume dan juga kontrak tak merupakan satu-satunya cara dalam menawarkan potongan volume. Namun pada umumnya kontrak merupakan cara yang wajar untuk menawarkan potongan volume ketika hal itu penting untuk mempertahankan atau menambah pelanggan yang bisa saja berpaling pada layanan lain.

Bagian yang penting dan sering tersembunyi dari paket biaya VPN ialah bagian rinci dari kontrak yang mengatur pelaksanaannya, yang meliputi :

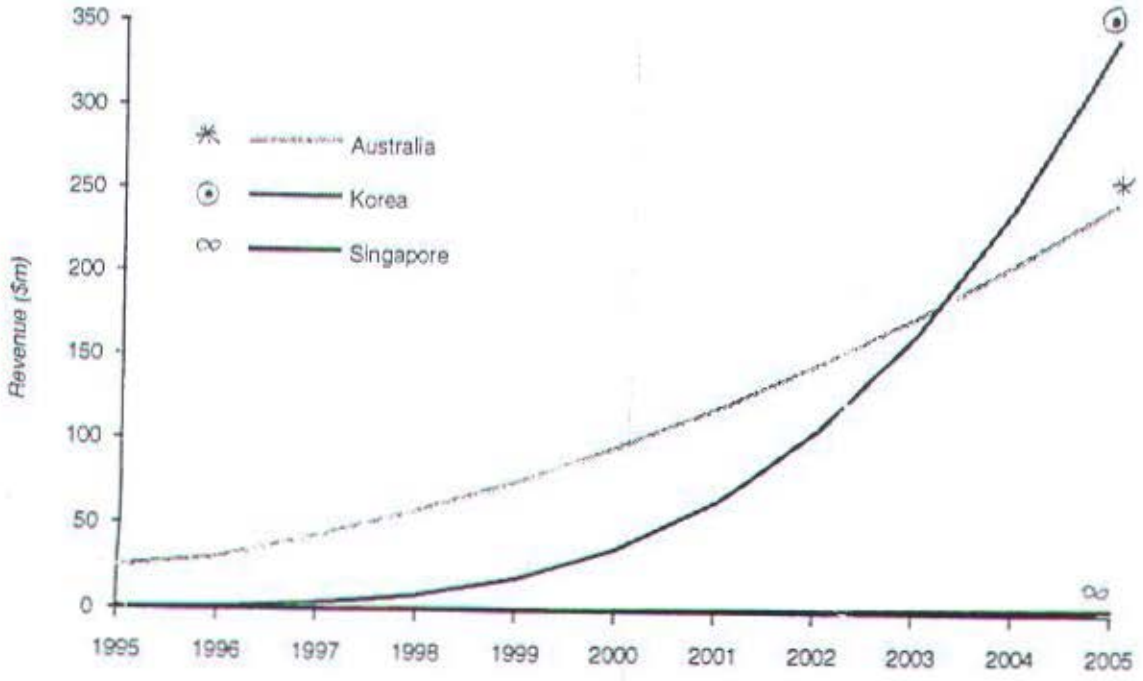
- bila pelanggan gagal memenuhi tingkat jumlah yang disepakati.
- hal yang dapat diberikan untuk mendorong pelanggan yang mencapai jumlah yang sesuai dengan potongan lebih besar. Sistem tagihan penyelenggara dilakukan secara otomatis atau tidak.
- perubahan pendapatan yang disebabkan oleh perubahan harga penyelenggara dan bukan oleh perubahan pemakaian pelanggan.
- potongan periodik otomatis berlaku untuk pelanggan yang setia untuk suatu masa tertentu atau perlu diminta seperti pada awal.
- hukuman yang pantas untuk menghentikan kontrak sebelum waktunya.

III.9.4. Ramalan Pendapatan ASIA-PASIFIK

Pada gambar 3.15 dapat dilihat bahwa Korea akan mengungguli Australia. Ini dikarenakan oleh lebih banyaknya kepadatan populasi dan jumlah jalur di Korea dari pada di Australia. Saat Korea Telecom diijinkan untuk menawarkan layanan secara nasional, pertumbuhan nasional yang tinggi akan segera dimulai. Sedangkan untuk pasar nasional Singapore dapat diabaikan.

Pada wilayah Asia-Pasifik, Singapore akan mengungguli Australia dalam pasar yang lebih besar untuk layanan VPN internasional. Singapore Telecom masih terus membangun layanan VPN internasionalnya; bila layanan tersebut sudah diterima secara luas oleh bisnis-bisnis yang ada di Singapore, maka keuntungan pulau itu dan hubungan ekonomi dengan Malaysia dan Indonesia yang baru muncul akan meningkatkan pendapatan seperti yang terlihat pada gambar 3.16.

Layanan VPN global tumbuh dari $ 150 juta pada tahun 1995 menjadi $ 2,3 miliyar pada tahun 2005. Pada tahun 2000, 60% dari berbagai negara akan sudah memakai layanan VPN. Bila perusahaan menyelesaikan uji coba dan lebih banyak layanan dan daerah yang tersedia, pengeluaran setiap perusahaan akan meningkat dari rata-rata $ 3 juta setahun pada tahun 1995 menjadi rata-rata $ 4,5 juta pada tahun 2000. Pengeluaran rata-rata tiap perusahaan akan meningkat menjadi $ 5 juta setahun pada tahun 2005 seperti pada terlihat pada gambar 3.17.

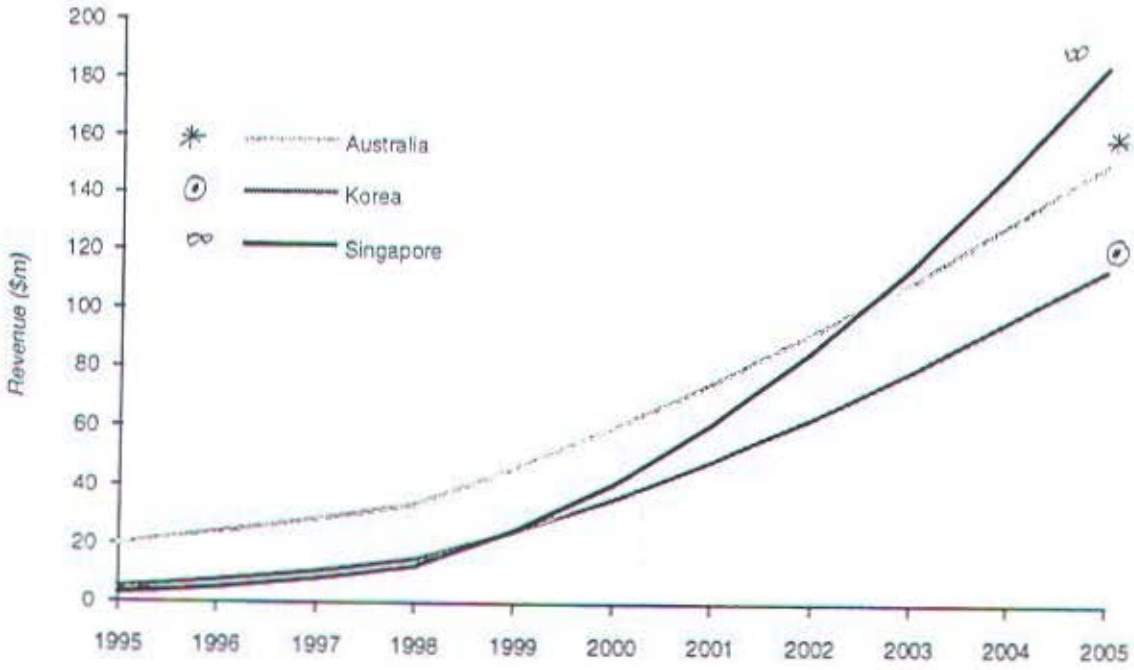


GAMBAR 3.15[37]

PENDAPATAN VPN NASIONAL ASIA-PASIFIK

---

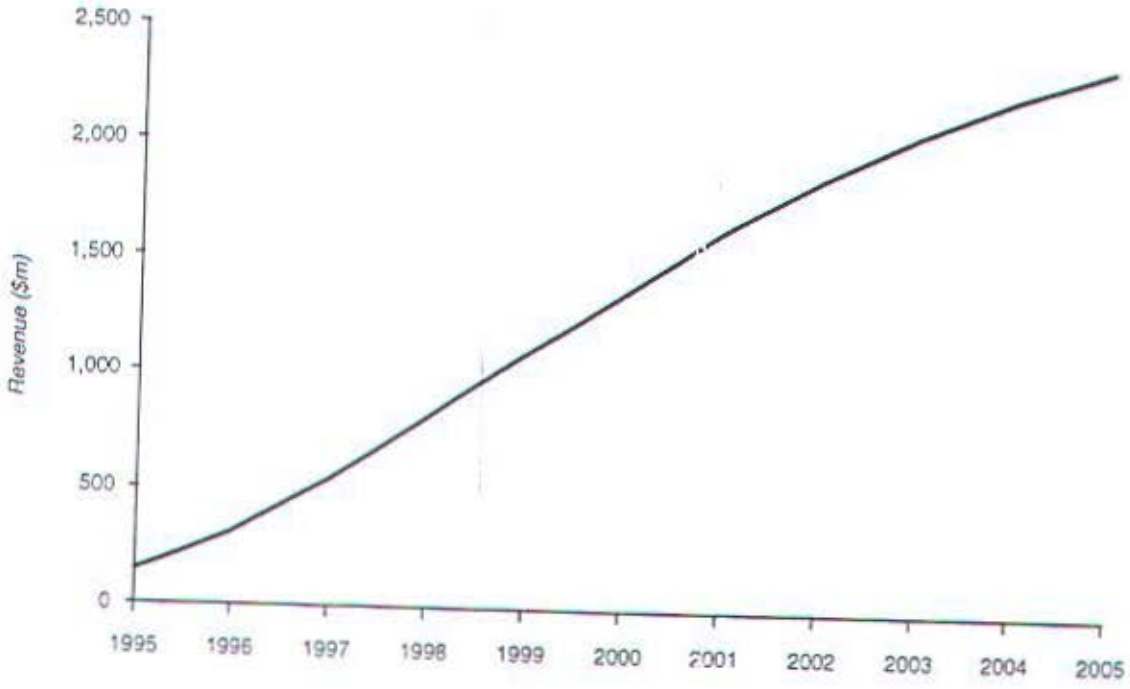
[37] McCarthy, C., Darabi, F., *VPN Services Market Strategies by Ovum Reports*, London, 1995, hal. 132



GAMBAR 3.16[38]

PENDAPATAN VPN INTERNASIONAL ASIA-PASIFIK

[38] Ibid, hal. 134



GAMBAR 3.17[39]

PENDAPATAN VPN GLOBAL

[39] Ibid, hal. 135

III.9.5. Prospek VPN di Indonesia

Menghadapi era globalisasi yang juga akan melanda Indonesia, dapat diramalkan bahwa hubungan antar negara di masa depan akan semakin meningkat, baik frekuensi maupun intensitasnya. Karena itu maka komunikasi dalam segala bentuknya akan meningkat seiring dengan meningkatnya kebutuhan akan informasi. Maka masa depan VPN sebagai salah satu pilihan komunikasi diduga juga akan meningkat.

Peningkatan ini sudah akan terjadi dalam masa dekat, karena :

- Akan makin banyak bisnis internasional yang akan masuk ke Indonesia dengan membuka cabang-cabang atau mencari mitra kerja, baik dalam kaitan kebutuhan investasi maupun dalam mencari perluasan pasar.
- Disamping itu, juga bisnis domestik akan makin banyak memasuki dunia internasional, baik untuk investasi, maupun terutama untuk merebut pasaran internasional.

Karena itu arus informasi akan semakin deras, dan layanan VPN akan mampu merebut pangsa pasar tersendiri, terutama bila selisih tarif antar komunikasi telepon dan VPN masih cukup besar. Kecenderungan demikian sudah dapat kita lihat di Singapore, Korea dan negara-negara kawasan ASIA-PASIFIK.

III. 10. NETWORK TEST

Pihak penyelenggara telekomunikasi internasional yang mengadakan jasa pelayanan VPN secara internasional akan melakukan beberapa tes antara lain adalah tes jaringan yang dilakukan dengan maksud untuk mengetahui unjuk kerja dari jaringan tersebut dan tes kesiapan secara operasional yang dilakukan untuk menjajaki seluruh kemungkinan serta seluruh aspek dari performan operasional sebelum jasa layanan VPN berjalan sepenuhnya sesuai keinginan para user. Tes Pre-Service juga akan dilakukan bagi semua customer baru yang ingin memulai jasa layanan VPN ini.

III.10.1. Network Validation Test (NVT)

Network Validation Test (NVT) merupakan suatu tes yang bertugas memeriksa keadaan jaringan dan kualitas dari end to end yang akan menggunakan jasa layanan VPN internasional yang menghubungkan pihak penyelenggara lokal dengan pihak penyelenggara luar negeri.

Tes akan dilakukan untuk pembicaraan dan faksimil, yaitu untuk memeriksa kesempurnaan panggilan, kualitas pembicaraan, post dial delay dan kualitas transmisi dari faksimil. Parameter tersebut di atas sudah termasuk kerusakan-kerusakan yang terjadi selama tes berlangsung. Hal ini dicatat dan diberitahukan kepada dua carrier agar dievaluasi dan segera diambil tindakan untuk memperbaiki kerusakan yang terjadi. Tes jaringan ini dilakukan dengan

persetujuan antara penyelenggara telekomunikasi yang sebelumnya sudah didiskusikan apa saja yang akan dilakukan dalam pengujian.

III.10.2. Operational Readiness Test (ORT)

Operational Readiness Test (ORT) adalah suatu tes yang dilakukan untuk mengetahui keadaan secara umum dari kedua penyelenggara jasa layanan VPN internasional. Maksud dari tes ini adalah untuk memeriksa bahwa semua metode dan prosedur yang diterapkan bagi jasa layanan VPN internasional ini berfungsi dengan baik.

Tes kesiapan operasional ini akan dilakukan dengan menggunakan grup user tertutup secara sementara yang telah ditentukan oleh penyelenggara jasa dan pelanggan tes terpilih yang setuju untuk menerima kejadian yang terburuk akibat jasa layanan baru yang digabungkan ke pelanggan tersebut. Pelanggan tes ini harus disetujui oleh kedua pihak penyelenggara jasa telekomunikasi yang bersangkutan.

Tes kesiapan operasional ini akan menguji beberapa metoda dan prosedur antara lain :

- implementasi penjualan dan ketentuan layanan
- logging panggilan
- pengujian pre-service
- pemeliharaan
- billing

III.10.3. Pre-Service Test (PST)

Tes ini sebaiknya dilaksanakan maksimum selama 5 hari dan akan dilakukan sebelum menentukan setiap pelanggan baru. Lamanya tes ini tergantung pada jumlah dari lokasi pelanggan dan kompleksitas feature. Urutan pengujian tersebut adalah sebagai berikut :

a. Tes pada sisi domestik

- Penentuan akses
- Pengujian database
- Pengujian feature layanan
- Logging panggilan.

Semua tes pada sisi domestik merupakan tanggung jawab tiap carrier dan dilaksanakan sebelum tes pada sisi internasional.

b. Tes pada sisi internasional

- Koordinasi pengujian secara keseluruhan
- Pengujian pada sisi internasional dari penyelenggara jasa layanan VPN ke sistem VPN lainnya.

Pengujian ini sebaiknya dilakukan selama 1 hari atau maksimum 2 hari.

c. Tes end to end

- Koordinasi pengujian pelanggan end to end
- Tes panggilan end to end ke atau dari extention tes terpilih
- Pemberitahuan pengaktifan layanan.

Tes ini sebaiknya diselesaikan dalam waktu satu hari.

BAB IV

PENUTUP

IV.1. KESIMPULAN

Berdasarkan pembahasan dalam tugas akhir ini, maka dapat diambil kesimpulan :

1. Implementasi jaringan pribadi melalui VPN memerlukan biaya investasi yang sangat murah dibandingkan dengan jaringan pribadi yang menggunakan leased circuit.

2. Dengan menggunakan jasa layanan VPN dapat menghubungkan beberapa lokasi yang berjauhan tanpa tambahan perangkat hardware.

3. Untuk telekomunikasi ke luar negeri dengan memakai VPN internasional akan lebih menghemat tarif telepon dibandingkan dengan SLI biasa.

4. Pelanggan pengguna jasa layanan VPN dapat mengatur VPN grup sesuai dengan keinginannya, yaitu mendefinisikan format penomorannya, mengubah routing, menambah atau mengurangi feature dan masih banyak lagi yang lainnya.

5. Jasa layanan VPN dapat meningkatkan efisiensi bisnis pelanggan melalui berbagai feature jasa.

6. Menggunakan layanan VPN juga memiliki kemampuan dalam mengatur manajemen trafik.

7. Dengan karakteristik jaringan publik di Indonesia yang memiliki sentral-sentral ISDN akan lebih memudahkan dalam menerapkan layanan VPN yang merupakan salah satu aplikasi dari Intelligent Network.

IV.2. Saran

Dari Tugas Akhir Studi tentang Virtual Private Network sebagai Aplikasi Jaringan Pintar dan Penerapannya di Indonesia diharapkan dapat menjadi bahan pertimbangan dalam mengoptimalkan operasi jaringan telekomunikasi khususnya jaringan telekomunikasi digital dalam memenuhi kebutuhan trafik yang padat dengan berbagai layanan jaringan yang dibutuhkan baik pada saat sekarang maupun pada masa yang akan datang terutama dalam transfer informasi antar komponen IN serta pengembangan lebih jauh dari VPN sebagai salah satu bentuk aplikasi layanan Jaringan Pintar (IN).

DAFTAR PUSTAKA

1. Ambrosch, W.D., Maher, A., Sasscer, B., ***The Intelligent Network; A Joint Study by Bell Atlantic, IBM and Siemens,*** Springer-Verlag, Berlin, 1989.

2. McCarthy, C., Darabi, F., ***VPN Services Market Strategies by Ovum Reports***, London, 1995.

3. Sulistijo, B. Widjajanto, ***Advanced Intelligent Network : Arsitektur dan Protokol,*** Makalah Presentasi Versis Pusrenbangti PT Telkom, Bandung, 1994.

4. Sutanto, Agung, A. S., ***Standard Intelligent Network (IN); Pentingnya Bagi Penyelenggara Telekomunikasi,*** Gematel, PT Telkom, Desember 1994.

5. Wedemeyer, D.J., Bissel, M.S., ***Pasific Telecommunications Users : A Spectrum of Requirements,*** Elsevier Science Publishers B.V., North-Holland, 1987.

6. ____, ***Hand Out Intelligent Network Service Implementation : VPN Detailed Description***, Bell Education Centre, Alcatel, 1995.

7. _____, ***Intelligent Network; Sebagai Solusi Jaringan Jasa Telekomunikasi,*** Makalah Presentasi Teknologi Komunikasi, PT Telkom, Desember 1994.

Figure G1.3 National VPN revenue – Europe

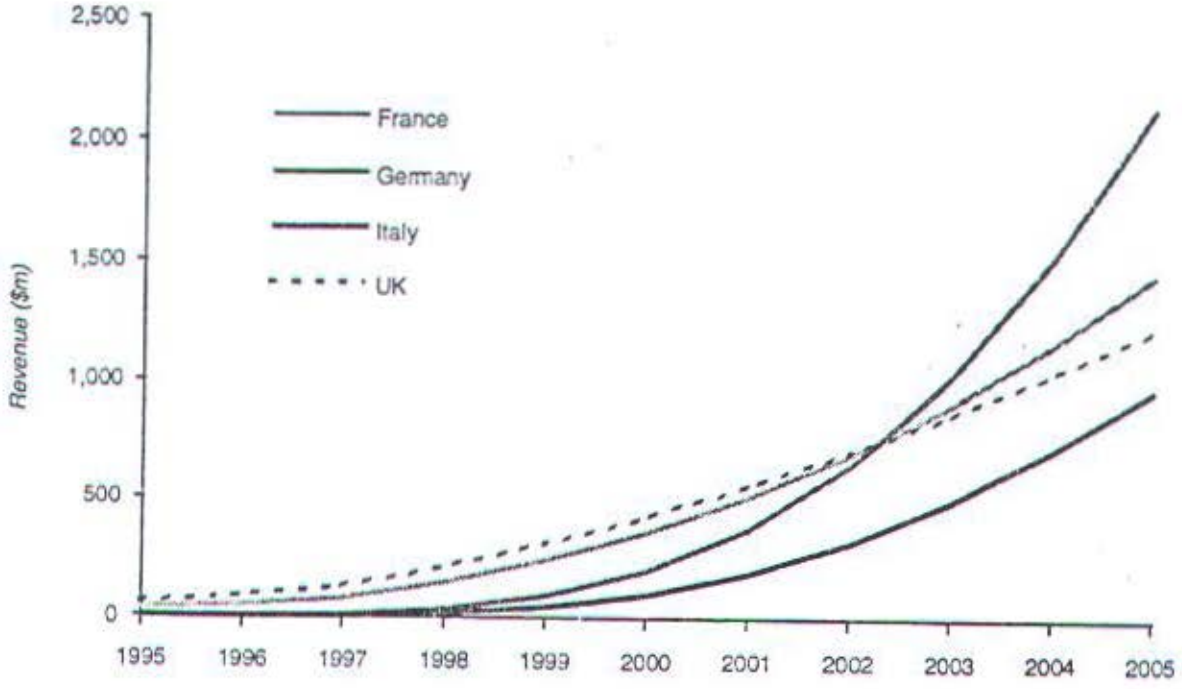


Figure G1.4 National VPN revenue – Asia-Pacific

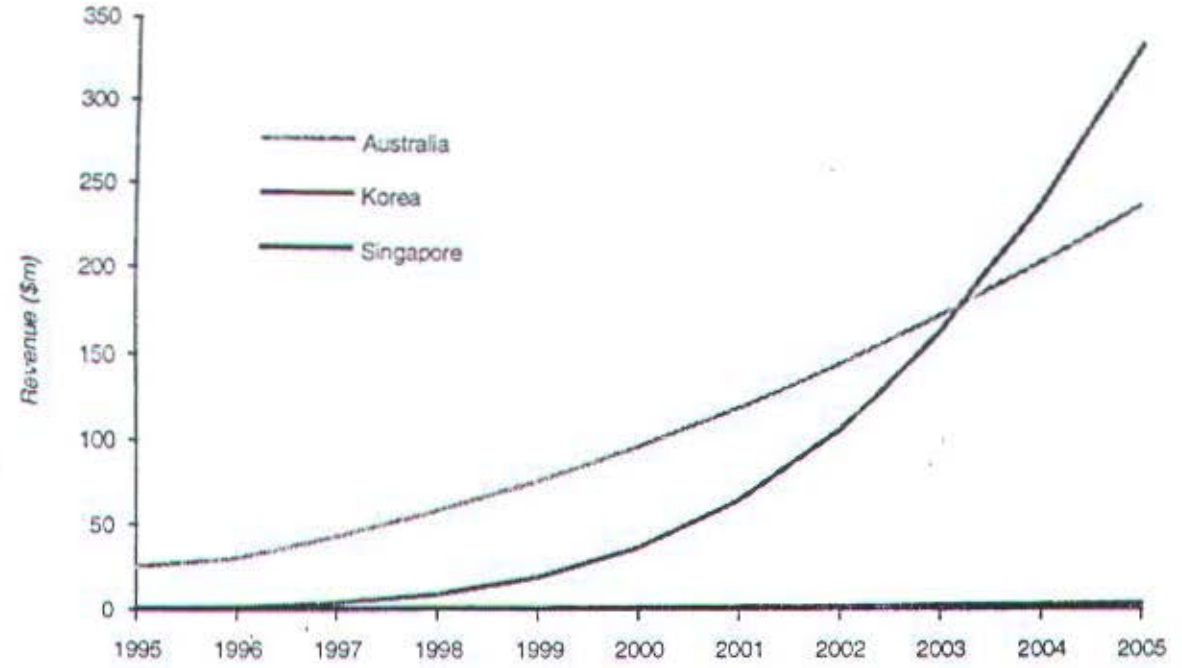


Figure G1.6 International VPN revenue – Europe

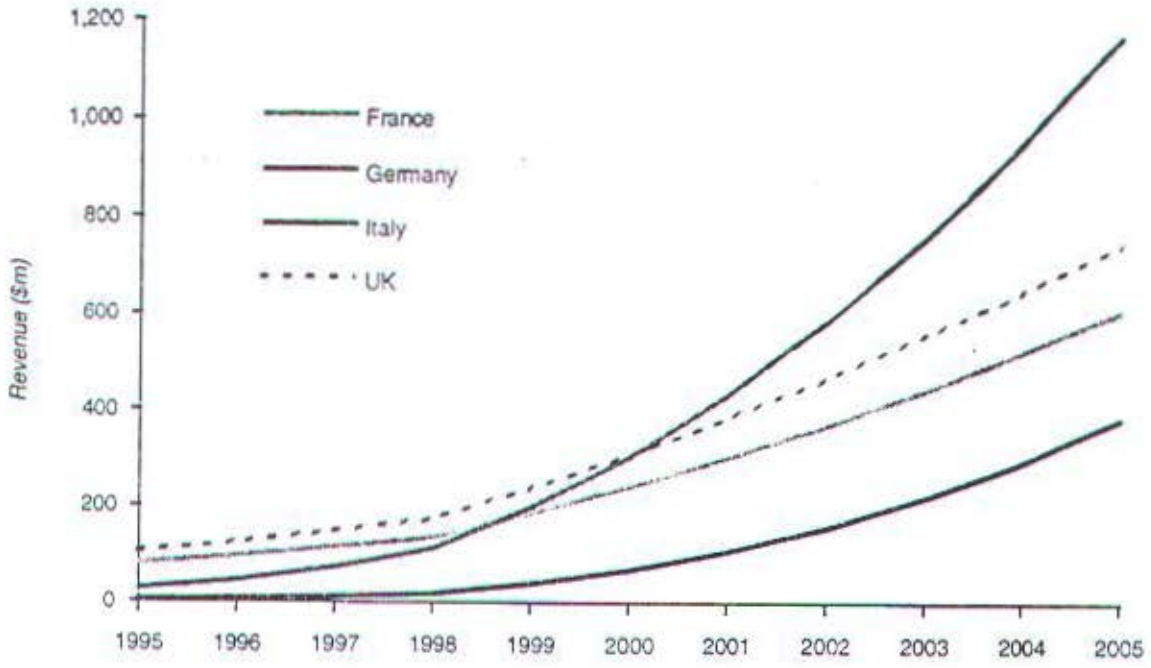
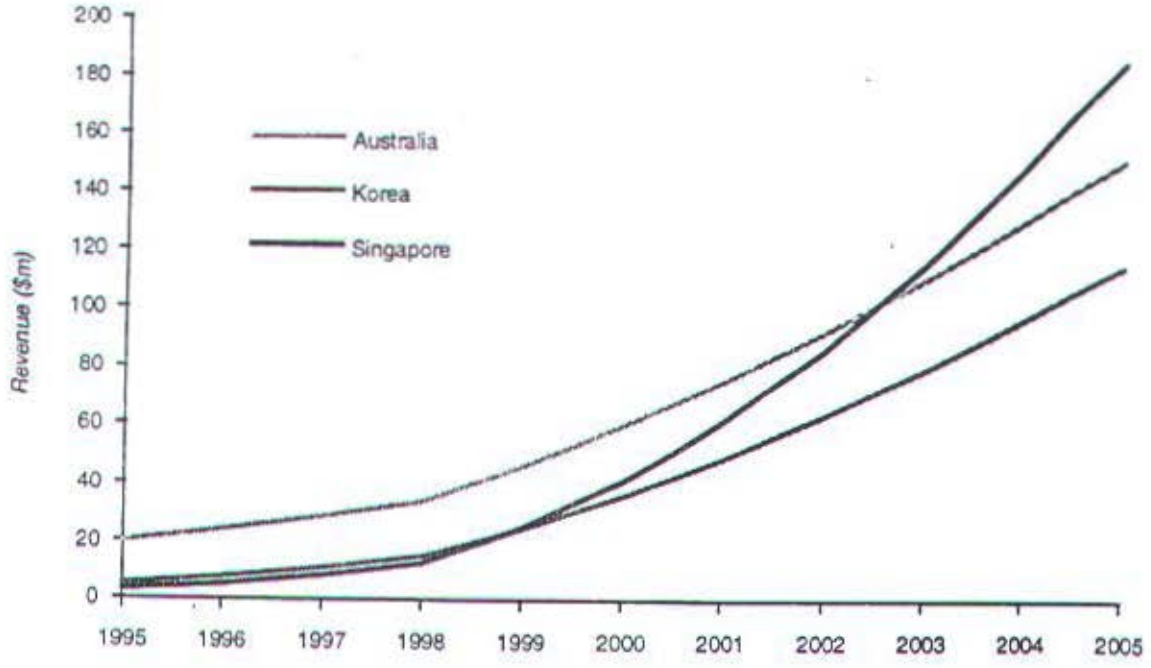


Figure G1.7 International VPN revenue – Asia-Pacific



It is often assumed that Spain would have a large amount of international traffic, particularly to Central and South America where Telefónica International holds a share in the local PTTs. There is, however, a weak traffic association between these Spanish-speaking countries: over 60% of Spain's international traffic goes to Europe. The US is the dominant economic pull for Central and South America and consequently the US receives a much higher proportion of the region's traffic than Spain.

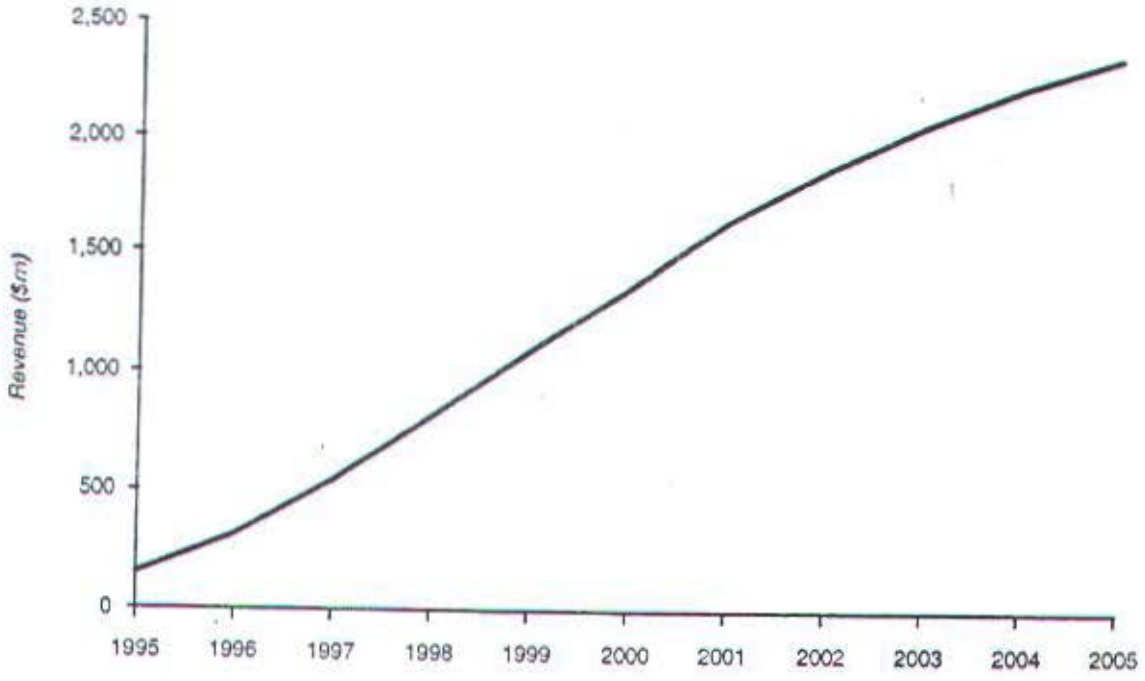
In the Asia-Pacific region, Singapore will overtake Australia as the larger market for international VPN services. Singapore Telecom is still developing its international VPN service; once the service is widely adopted by businesses located in Singapore, the island's proximity to and relations with the emerging Malaysian and Indonesian economies will propel revenues forward, as shown in Figure G1.7.

The comparative sizes of the markets in the final year are broadly consistent with ITU statistics for international traffic and revenues.

Global VPN service revenues

Global VPN services will grow from $150 million in 1995 to $2.3 billion in 2005. By 2000, 60% of multinationals will have adopted VPN services. As companies complete trials and more services and locations become available, expenditure per company will increase from an average of $3 million per year in 1995 to an average of $4.5 million by 2000. Average expenditure per company will increase to $5 million per year by 2005, as shown in Figure G1.8.

Figure G1.8 **Global VPN revenue**



18 APR 1995

FAKULTAS TEKNOLOGI INDUSTRI
JURUSAN TEKNIK ELEKTRO - ITS

EL 1799 TUGAS AKHIR (6 SKS)

Nama Mahasiswa	: Boedi Pratoto
Nomor Pokok	: 290 220 1474
Bidang Studi	: Teknik Telekomunikasi
Tugas Diberikan	: April 1995
Tugas Diselesaikan	: September 1995
Dosen Pembimbing	: DR. Ir. M. Salehudin, M. Eng. Sc.
Judul Tugas Akhir	:

STUDI TENTANG VIRTUAL PRIVATE NETWORK SEBAGAI APLIKASI JARINGAN PINTAR DAN PENERAPANNYA DI INDONESIA

Uraian Tugas Akhir

Virtual Private Network (VPN) adalah salah satu aplikasi dari teknologi intelligent network atau jaringan pintar yang akan mempunyai peranan penting dalam suatu perkembangan industri untuk masa sekarang dan masa yang akan datang. Penting sekali mengembangkan suatu mekanisme implementasi yang tidak tergantung pada jasa dan konfigurasi jaringan individu serta mengembangkan suatu mekanisme untuk merealisasikan jasa-jasa yang dibutuhkan dalam menanggapi permintaan pelanggan individu dan bebas mengkombinasikan dengan komponen jasa yang telah tersedia di jaringan yang telah terpasang. Dalam tugas akhir ini akan dibahas tentang dibangunnya jaringan private dengan menggunakan sarana jaringan publik serta kemungkinan penerapannya pada sistem komunikasi nasional.

Surabaya, 17 April 1995

Menyetujui
Bidang Studi Teknik Telekomunikasi
Koordinator,

Ir. M. Aries Purnomo
NIP. 130 532 040
18/4 95

Dosen Pembimbing,

DR. Ir. M. Salehudin, M. Eng. Sc.
NIP. 130 532 026
17/4 95

Mengetahui
Jurusan Teknik Elektro FTI - ITS
Ketua,

DR. Ir. M. Salehudin, M. Eng. Sc.

Usulan Tugas Akhir

1. Judul Tugas Akhir : **STUDI TENTANG VIRTUAL PRIVATE NETWORK SEBAGAI APLIKASI JARINGAN PINTAR DAN PENERAPANNYA DI INDONESIA**

2. Ruang Lingkup : - Telefoni Digital
- Komunikasi Data
- Teknik Jaringan Telekomunikasi

3. Latar Belakang : Dalam waktu yang tidak lama lagi komunikasi akan mempunyai bentuk yang berbeda dengan apa yang kita nikmati saat ini. Perkembangan jumlah kebutuhan masyarakat akan jasa telekomunikasi, khususnya di kota-kota besar semakin meningkat. Meningkatnya jumlah pelanggan menyebabkan jaringan telekomunikasi semakin kompleks dan rumit.

Penerapan teknologi Virtual Private Network (VPN) yang merupakan salah satu aplikasi dari jaringan pintar akan memberikan pelayanan yang dapat memenuhi kebutuhan komunikasi yang meningkat tersebut dengan tingkat keamanan jaringan telekomunikasi yang tinggi.

4. Penelaahan Studi : Dalam tugas akhir ini akan dibahas mengenai kemungkinan penerapan jaringan private di Indonesia dengan menggunakan sarana jaringan publik yang sudah ada tanpa harus menggunakan komponen jaringan secara khusus. Seperti diketahui bahwa jaringan publik sekarang ini memiliki sentral-sentral dengan karakteristik yang berbeda-beda, maka untuk itu diperlukan suatu jaringan private yang dapat diimplementasikan ke dalam sentral-sentral jaringan publik tadi tanpa harus menggunakan komponen jaringan secara khusus. Teknologi VPN pada dasarnya memiliki karakteristik yang meliputi penyediaan sebuah perencanaan penomoran pribadi, pembebanan panggilan berdasarkan waktu penggunaan dan penggunaan untuk komunikasi suara dan data atau keduanya. Sehinga dengan penerapan teknologi VPN ini akan memberikan suatu kompatibilitas antar perangkat dari pembuat yang berbeda dan mempertnggi fleksibilitas serta juga menurunkan biaya/harga jangkauan pelayanan.

5. Tujuan : Mengkaji kelayakan penerapan VPN pada jaringan publik di JAPATI dan seluruh Indonesia.

6. Langkah-langkah :
1. Studi literatur
2. Pengumpulan data
3. Analisa data
4. Penulisan buku

7. Relevansi : Dari tugas akhir ini diharapkan dapat digunakan sebagai acuan untuk penerapan VPN yang dikaitkan dengan perkembangan teknologi telekomunikasi di Indonesia.

8. Jadwal Kegiatan :

KEGITAN	BULAN					
	I	II	III	IV	V	VI
1. Studi Literatur						
2. Pengumpulan data						
3. Pembahasan Masalah						
4. Penulisan Tugas Akhir						

RIWAYAT HIDUP

A. IDENTITAS PENULIS

Nama : Boedi Pratoto

Tempat Lahir : Surabaya

Tanggal Lahir : 24 Juni 1971

Agama : Islam

Nama Ayah : R. Soemarto

Nama Ibu : Widawati Djanas

Alamat : Ngagel Jaya Tengah I no. 4 Surabaya

Penyusun adalah putra tunggal.

B. RIWAYAT PENDIDIKAN :

1. SDN Kertajaya XIII Surabaya, lulus tahun 1984
2. SMPN 6 Surabaya, lulus tahun 1987
3. SMAN 5 Surabaya, lulus tahun 1990
4. Diterima di Jurusan Teknik Elektro FTI - ITS pada tahun 1990, dan saat ini sedang menyelesaikan Tugas Akhir.

C. PENGALAMAN KEMAHASISWAAN :

1. Asisten Praktikum Dasar Sistem Komunikasi tahun 1994.
2. Asisten Praktikum Sistem Komunikasi Lanjut I, tahun 1995.
3. Asisten Praktikum Sistem Komunikasi Lanjut II, tahun 1995.
4. Kerja Praktek di PT. INDOSAT Jakarta dan di Stasiun Bumi Besar Surabaya.
5. Koordinator Sie Dana MPS tahun 1992.
6. Koordinator Sie Dokumentasi Kejuaraan Tenis Tingkat Nasional tahun 1992.
7. Koordinator Sie Acara Apresiasi Seni Kampus 19994.