BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

- - - - - - - - - - - - - - - - - -

LUẬN VĂN THẠC SĨ KHOA HỌC

CÔNG NGHỆ MẠNG RIÊNG ẢO DI ĐỘNG VÀ KHẢ NĂNG ỨNG DỤNG CHO MẠNG DI ĐỘNG GSM VÀ CDMA

NGÀNH: CÔNG NGHỆ THÔNG TIN
MÃ SỐ:

NGUYỄN NGỌC THÀNH

Người hướng dẫn khoa học: GS.TS. NGUYỄN THÚC HẢI

HÀ NỘI 2006

Mục lục

Thuật ngữ và chữ viết tắt

3GPP	3rd Generation Partnership Project	Đề án các đối tác thế hệ ba
AAA	Authentication, Authorization and Accounting	Xác thực, Ủy quyền và Kế toán
ANSI	American National Standard Institute	Viện Tiêu chuẩn quốc gia Mỹ
ASP	Application Service Provider	Nhà cung cấp dịch vụ ứng dụng
ATM	Asynchronous Transfer Mode	Chế độ truyền dị bộ
BGP	Border Gateway Protocole	Giao thức cổng biên
BSC	Base Station Controller	Bộ điều khiển trạm gốc.
BSS	Base Station System	Hệ thống trạm gốc.
BTS	Base Transceiver Station	Trạm thu phát gốc.
CAMEL	Customized Application for Mobile Network Enhanced Logic	Ứng dụng khách hàng hóa cho logic được mạng di động tăng cường
CDMA	Code Division Multiple Access	Đa truy nhập phân chia theo mã
CDR	Charging Data Record	Bản ghi số liệu tính cước
CHAP	Challenge Handshake Authentication Protocol	Giao thức xác thực bắt tay
CS	Circuit Switch	Chuyển mạch kênh
DLCI	Data Link Connection Identifier	Nhận dạng kết nối liên kết số liệu
DTM	Dual Transfert Mode	Chế độ truyền kép
EAP	Extensible Authentication Protocol	Giao thức xác thực mở rộng
ESP	Encapsulating Security Payload	Tải tin đóng gói an ninh
ETSI	European Telecommunications Standard Institute	Viện Tiêu chuẩn viễn thông châu Âu
FA	Foreign Agent	Tác tử ngoài
GGSN	Gateway GPRS Support Node	Node hỗ trợ GPRS cổng
GPRS	General Packet Radio Service	Dịch vụ vô tuyến gói chung
GRE	Generic Routing Encapsulation	Đóng gói định tuyến chung
GSM	Global System For Mobile Telecommunications	Hệ thống thông tin di động toàn cầu

GTP	GPRS Tunneling Protocol	Giao thức truyền tunnel GPRS
HA	Home Agent	Tác tử nhà
HLR	Home Location Register	Bộ ghi định vị nhà
IBGP	Internet Border Gateway Protocol	Giao thức cổng biên internet
IMSI	International Mobile Station Identifier	Nhận dạng thuê bao di động toàn cầu
IPCP	IP Configuration Protocol	Giao thức lập cấu hình IP
IPIP	IP in IP	Giao thức IP trong IP
IPSec	IP Security	An ninh IP
ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
IWF	Interworking Function	Chức năng tương tác
L2TP	Layer 2 Tunneling Protocol	Giao thức truyền tunnel lớp 2
LAC	L2TP Access Concentrator	Bộ tập trung truy nhập L2TP
LCP	Link Control Protocol	Giao thức điều khiển liên kết
LLC	Logical Link Control	Điều khiển liên kết logic
LNS	L2TP Network Server	Máy chủ mạng L2TP
MIP	Mobile IP	IP di động
MPLS	Multi-Protocol Label Switching	Chuyển mạch nhãn đa giao thức
MSC	Mobile Services Switched Center	Trung tâm chuyển mạch các dịch vụ di động
MT	Mobile Termination	Kết cuối di động
MVPN	Mobile Virtual Private Network	Mạng riêng ảo di động
NAI	Network Access Identifier	Nhận dạng truy nhập mạng
NAS	Network Access Server	Máy chủ truy nhập mạng
NAT	Network Address Translation	Biên dịch địa chỉ mạng
NAT-T	NAT Traversal	NAT cải tiến
PAP	Password Authentication Protocol	Giao thức nhận thực mật khẩu
PAT	Port Address Translation	Biên dịch địa chỉ cổng
PCF	Packet Control Function	Chức năng điều khiển gói
PCO	Protocol Configuration Options	Các tùy chọn cấu hình

PDP	Packet Data Protocol	Giao thức số liệu gói
PDSN	Packet Data Serving Node	Node phục vụ số liệu gói
PDU	Protocol Data Unit	Đơn vị số liệu giao thức
PIN	Personal Identitification Number	Số nhận dạng cá nhân
PKI	Public Key Infrastructure	Cơ sở hạ tầng khoá công cộng
PLMN	Public Land Mobile Network	Mạng di động mặt đất công cộng
PS	Packet Switch(ed)	Chuyển mạch gói
QoS	Quality of Service	Chất lượng dịch vụ
RADIUS	Remote Authentication Dial-in User Service	Dịch vụ xác thực người dùng quay số từ xa
RAN	Radio Access Network	Mạng truy nhập vô tuyến
RAS	Remote Access Server	Máy chủ truy nhập từ xa
RIL3	Radio Interface Layer 3	Lớp 3 giao diện vô tuyến
RLC	Radio Link Control	Điều khiển liên kết vô tuyến
RLP	Radio Link Protocol	Giao thức liên kết vô tuyến
RNC	Radio Network Controller	Bộ điều khiển mạng vô tuyến
R-P	Radio-Packet	Vô tuyến-gói
SGSN	Serving GPRS Support Node	Nút hỗ trợ GPRS phục vụ
SIM	Subscriber Identity Module	Thẻ nhận dạng thuê bao
SLA	Service Level Agreement	Thoả thuận mức dịch vụ
TDMA	Time Division Multiple Access	Đa truy nhập phân chia theo thời gian
TE	Terminal Equipment	Thiết bị đầu cuối
TIA	Telecommunication Industry Association	Hiệp hội công nghiệp viễn thông (Mỹ)
TLS	Transport Layer Security	An ninh lớp giao vận
UMTS	Universal Mobile Telecommunications System	Hệ thống thông tin di động toàn cầu
VCI	Virtual Channel Identifier	Nhận dạng kênh ảo
VLR	Visitor Location Register	Bộ ghi định vị tạm trú
VPI	Virtual Path Identifier	Nhận dạng tuyến ảo
WAP	Wireless Application Protocol	Giao thức ứng dụng vô tuyến

Lời nói đầu

VPN đã được sử dụng rộng rãi trong công nghệ nối mạng ở các dạng khác nhau trong nhiều năm. Ứng dụng mới nhất của VPN là MVPN, tuy hãy còn non trẻ và còn nhiều vấn đề chưa được giải quyết, cả về kỹ thuật lẫn kinh doanh. Nhưng chương trình khung đã được định nghĩa rộng rãi và cũng đã có các triển khai ở nhiều dạng khác nhau.

Để đảm bảo tăng trưởng lợi nhuận, các nhà cung cấp dịch vụ di động tìm kiếm các công nghệ và phương thức mới để đầu tư. Trong những năm gần đây họ lưu tâm rất nhiều đến các dịch vụ Internet có tiềm năng sinh ra những lợi nhuận đáng kể. Đây chính là lý do của những đầu tư tần phổ đắt tiền vào các công nghệ truy nhập vô tuyến thế hệ tiếp theo có tiềm năng hỗ trợ tốc độ số liệu cao cho các dịch vụ Internet: đó là hệ thống thông tin di động thế hệ 3 (3G) GPRS, UMTS, và CDMA2000. Sự pha trộn khả năng thoại di động truyền thống với các dịch vụ truyền bản tin và dựa trên vị trí là các dịch vụ hứa hẹn nhất. Các hệ thống này phải cung cấp cho người sử dụng khả năng truy nhập cá nhân an ninh đến các mạng số liệu riêng, các cộng đồng cùng công việc hoặc sở thích cả về kinh doanh lẫn giải trí.

Yêu cầu cao đối với dịch vụ này dẫn đến nhu cầu cung cấp kết nối mạng riêng ảo di động (MVPN) của các nhà cung cấp dịch vụ. MVPN được coi là chìa khóa trao đổi thông tin kinh doanh giữa người sử dụng di động và mạng số liệu riêng an ninh thông qua môi trường Internet. MVPN có thể định nghĩa như là sự mô phỏng của mạng số liệu di động an ninh riêng dựa trên các phương tiện vô tuyến và di động an ninh dùng chung.

Từ các phân tích nêu trên, luận văn " **CÔNG NGHỆ MẠNG RIÊNG ẢO DI ĐỘNG VÀ KHẢ NĂNG ỨNG DỤNG CHO MẠNG DI ĐỘNG GSM VÀ CDMA**" nghiên cứu các giải pháp kỹ thuật, công nghệ MVPN cho hệ thống thông tin di động và khả năng ứng dụng trong sản xuất và kinh doanh.

Luận văn chia thành 5 chương. Chương 1 và 2 nghiên cứu tổng quan các hệ thống thông tin di động và cơ sở nền tảng MVPN. Chương 3 và 4 nghiên cứu các

giải pháp MVPN cho thông tin di động (GSM/GPRS, UMTS và CDMA2000). Chương thứ 5 nghiên cứu thị trường, các khả năng triển khai và mô hình đề xuất với Việt Nam.

Do nội dung của đề tài liên quan đến rất nhiều công nghệ và đề cập nhiều vấn đề nên mỗi mục được trình bày một cách tóm lược các đặc điểm chính và có chú thích các tiêu chuẩn kiến nghị liên quan. Đồng thời nội dung nghiên cứu đề tài tương đối rộng nên chắc chắn không tránh khỏi hạn chế và thiếu sót. Rất mong được sự đóng góp ý kiến của thầy cô và các bạn.

Tôi xin gửi lời cảm ơn chân thành tới GS TS Nguyễn Thúc Hải đã định hướng nghiên cứu và giúp đỡ tôi rất nhiều trong quá trình thực hiện luận văn này.

Hà Nội Tháng 11 năm 2006

Chương 1 Tổng quan các hệ thống thông tin di động

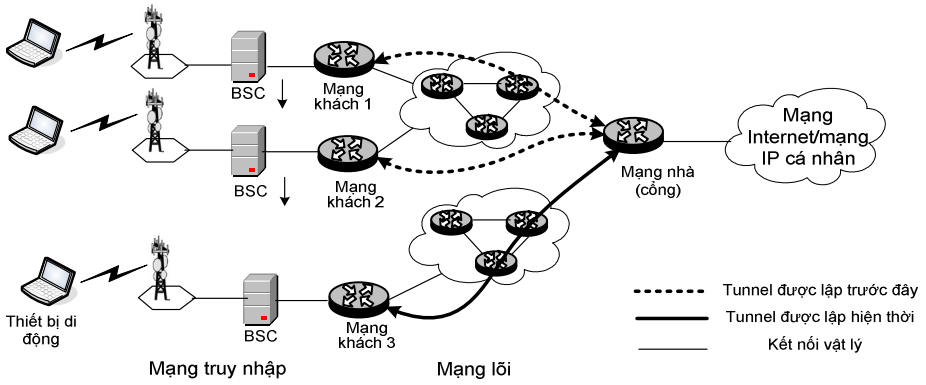
Các hệ thống thông tin di động (còn gọi là công nghệ tế bào) cung cấp dịch vụ số liệu dưới hai phương thức chuyển mạch kênh và chuyển mạch gói.

Trong mạng số liệu chuyển mạch kênh vô tuyến (CS), các kênh dành riêng được ấn định cho các thuê bao dù họ có sử dụng hay không. Dịch vụ số liệu được cung cấp thông qua mô hình quay số vô tuyến (giống truy nhập từ xa quay số hữu tuyến). Người sử dụng quay số điện thoại liên kết tới một NAS (Network Access Server) dùng cho dịch vụ số liệu vô tuyến đặc thù. Khi kết nối vật lý (kênh) được thiết lập giữa MS (Mobile Station) và NAS, PPP (Point-to-Point Protocol) cung cấp dịch vụ liên kết đầu cuối-đầu cuối. Có thể dễ dàng kết cuối phiên PPP người sử dụng, bằng các kỹ thuật quay số đơn giản dựa trên ngân hàng modem hay RAS (Remote Access Server) có bổ sung thêm chức năng IWF (InterWorking Function) với nâng cấp phần mềm phù hợp với môi trường vô tuyến. IWF kết cuối các giao thức truy nhập vô tuyến RLP (Radio Link Protocol) và tương tác với PSTN (Public Switched Service Telephone Network) khi cần. Triển khai VPN dựa trên CS không phải là hướng chính trong tương lai, do vậy sẽ không được đề cập đến trong luận văn này.

Các công nghệ mạng số liệu chuyển mạch gói vô tuyến (PS) dựa trên hỗ trợ mạng truy nhập vô tuyến để ghép kênh thống kê các phiên người sử dụng. Nó hỗ trợ truyền dẫn *số liệu dạng cụm (*19,2kbps ; 38,4kbps ; 76,8kbps ; 153,6kbps), và các tài nguyên mạng chỉ được sử dụng trong thời gian truyền số liệu và không sử dụng trong thời gian rỗi. Do đó giúp cho hệ thống hoạt động hiệu quả hơn. Điều đó cũng có nghĩa là người sử dụng trong các mạng đa phương tiện dùng chung phải tranh chấp băng thông khả dụng, nên đôi khi dẫn đến nghẽn, trễ và hiệu suất thông lượng trên một người sử dụng thấp hơn.

Tranh chấp truy nhập các tài nguyên dùng chung là vấn đề điển hình trong các hệ thống thông tin di động (TTDĐ) chuyển mạch gói. Để sử dụng hiệu quả các tài nguyên, các kênh truy nhập vô tuyến chỉ được cấp phát tạm thời cho người sử dụng. Sau một khoảng thời gian không tích cực, MS chuyển vào chế độ rỗi (trong GPRS)

hay chế độ ngủ (trong CDMA2000). Chế độ này cho phép MS luôn được kết nối bằng cách gửi báo hiệu và số liệu đến địa chỉ lớp mạng của nó thông qua các thủ tục cập nhật vị trí và tìm gọi, và không tài nguyên dành riêng nào cho phép MS gửi và nhận số liệu lúc này. Khi cần nhận số liệu, MS được tìm gọi, nó "tỉnh giấc" và phát đi yêu cầu thiết lập kênh mang vô tuyến (radio bearer) để được phép thu số liệu. MS phát đi yêu cầu giống như vậy khi nó cần phát số liệu và khi không có kênh mang vô tuyến sẵn sàng thiết lập.



Hình 1.1 Cơ chế truyền tunnel số liệu gói vô tuyến

Trong các hệ thống thông tin di động, về khái niệm, công nghệ hỗ trợ nối mạng di động số liệu PS người sử dụng là giống nhau. Nó dựa trên các cơ chế truyền tunnel khác nhau như MIP (trong CDMA2000) và GTP (trong GSM và UMTS). Các tunnel được thiết lập động giữa điểm nhập mạng vô tuyến tức thời của MS và một "điểm neo" tunnel hay mạng nhà, đồng thời đóng vai trò như một cổng cho mạng số liệu di động mà từ đó người sử dụng nhận được dịch vụ truy nhập. Vì các MS thay đổi động vị trí trong mạng (di chuyển từ một MSC (Mobile Switching Center) này đến một MSC khác hay đang ở biên MSC), nên các tunnel được thiết lập động giữa mạng nhà của MS và mạng truy nhập vô tuyến khách.

Với công nghệ mạng số liệu PS, do thiếu sản xuất đầu cuối hàng loạt và thử nghiệm tốn kém nên thời gian tiếp nhận dịch vụ chậm hơn dự tính. Người sử dụng cũng có thể kết nối *thường xuyên* hay *theo yêu cầu* đến mạng Internet hay mạng số liệu riêng. Tuy nhiên nó đòi hỏi có các quy định trước giữa mạng số liệu riêng và nhà khai thác.

Công nghệ thông tin di động, hiện nay đã trải qua ba thế hệ:

GENERATIONS	1G	2G	2.5 G	3G
Systems	NMT, TACS, AMPS	TDMA IS-136, GSM, CDMA IS-95, HSCSD, CDPD	GPRS, CDMA2000-1X, EDGE	CDMA2000-3X, CDMA2000-1X EV-DO UMTS, Enhanced EDGE
Voice/data technology	Circuit voice, circuit dial-up data	Circuit voice, circuit dial-up data	Circuit voice, circuit/packet data (Internet, IP services)	Circuit/packet voice, circuit data and highspeed packet data (multimedia, all IP option)
Theoretical data rate.	2.4–9.6 Kbps	9.6 -19.2 Kbps 28.8 Kbps	9.6 -144 Kbps; 70–473 Kbps	144Kbps-2Mbps; 144Kbps-2Mbps; 256Kbps-2.4Mbps
Expected average data throughput	2.0–9.0 Kbps	9.0–19.0 Kbps	9.0–300 Kbps	60–1000 Mbps;
Radio Access Technology	FDMA	TDMA, CDMA	TDMA, CDMA	TDMA, CDMA, W-CDMA, TD-SCDMA

Bảng 1 Các đặc tính của các hệ thống thông tin di động [4]

Thế hệ thứ nhất (1G) truyền tín hiệu thoại tương tự dựa trên FDMA (Frequency Division Multiple Access) với mạng lõi dựa trên TDM (time-division multiplexing). 1G được các nước Tây Âu sử dụng trong thời kỳ đầu.

Thế hệ thứ hai (2G) được thiết kế cho triển khai quốc tế (cung cấp khả năng chuyển vùng quốc gia) với các đặc tính mạnh như tính tương thích, khả năng chuyển mạng, và sử dụng truyền tải thoại đã được số hóa trên giao diện vô tuyến. Hệ thống 2G điển hình: GSM (Global System for Mobile Communications) và cdmaOne (tiêu chuẩn TIA [IS95]). Công nghệ mạng lõi của 2G có thể là số liệu chuyển mạch kênh hoặc chuyển mạch gói.

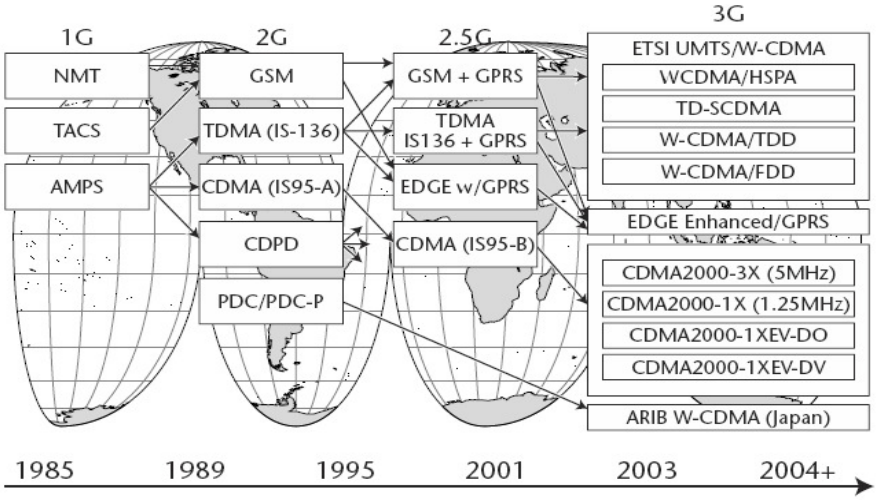
Hệ thống 2,5G là bước đệm tiến triển từ 2G lên 3G. Nó có công nghệ truyền dẫn vô tuyến của 2G và có tốc độ dữ liệu đến 144kbps của 3G. Điển hình là GPRS.

Một hệ thống TTDĐ thế hệ thứ ba (3G) phải đáp ứng các yêu cầu của ITU:

- Hoạt động tại một trong các dải tần số đã ấn định cho các dịch vụ 3G.

- Phải cung cấp dịch vụ số liệu mới cho người sử dụng, bao gồm multimedia, độc lập với công nghệ giao diện vô tuyến.
- Phải hỗ trợ truyền dẫn số liệu di động tại 144kbps cho người sử dụng di động tốc độ cao và đến 2Mbps (về lý thuyết) cho người di động tốc độ thấp.
- Phải cung cấp dịch vụ số liệu gói.
- Phải đảm bảo tính độc lập mạng lõi với giao diện truy nhập vô tuyến.

Hình 1.1 cho thấy con đường phát triển của các hệ thống thông tin di động.



Hình 1.1 Con đường phát triển của các hệ thống thông tin di động [4]

1.1 Số liệu chuyển mạch gói trong CDMA2000

Phần này sẽ trình bày kiến trúc số liệu gói liên kết với giao diện vô tuyến CDMA2000. Kiến trúc này được mô tả trong khuyến nghị 3GPP2 và các tiêu chuẩn TIA [IS835] và [TS115], cho phép các nhà cung cấp dịch vụ vô tuyến di động CDMA2000 đưa ra dịch vụ số liệu gói hai chiều sử dụng giao thức IP. Có hai phương pháp được sử dụng: Simple IP (*IP đơn giản*) và *MIP* (IP di động).

Trong IP đơn giản, nhà cung cấp phải ấn định cho người sử dụng một địa chỉ IP động. Địa chỉ này giữ nguyên không đổi khi người sử dụng duy trì kết nối với cùng một mạng trong miền nhà khai thác di động, nghĩa là người sử dụng vẫn trong vùng phủ của một PDSN (Packet Data Serving Node). Một địa chỉ IP mới phải nhận được khi người sử dụng nhập vào một mạng IP khác (vùng phủ của PDSN khác).

Uu điểm nổi trội của IP đơn giản (so với MIP) là không đòi hỏi cài đặt phần mềm đặc biệt trong MS. Tuy nhiên IP đơn giản chỉ hỗ trợ di động trong một vùng biên giới địa lý nhất định (vùng phủ của một PDSN).

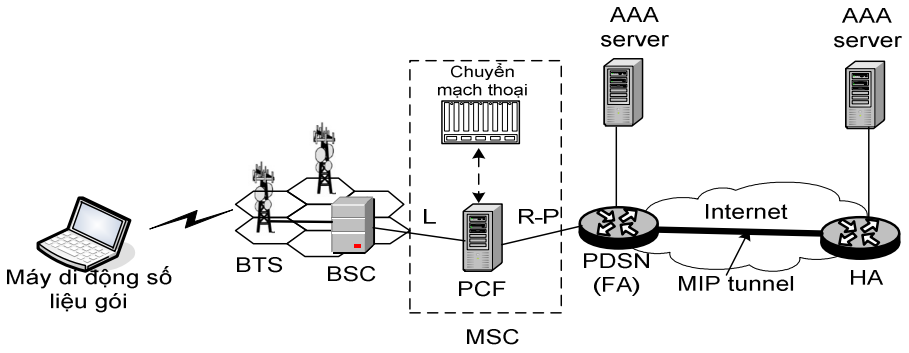
Phương pháp truy nhập MIP dựa trên [RFC3220]. Trước hết MS được nhập vào một PDSN phục vụ có hỗ trợ chức năng FA (Tác tử ngoài) và được ấn định địa chỉ IP theo HA (Tác tử nhà) của nó. MIP cho phép MS duy trì địa chỉ IP của mình trong thời gian phiên khi di chuyển trong mạng CDMA2000 hay sang mạng khác hỗ trợ MIP.

Các MS tương thích với tiêu chuẩn TIA/EIA [IS-2000] được kết nối vào mạng CDMA2000-1x, có thể thay đổi tốc độ số liệu khả dụng giữa tốc độ cơ bản 9,6kbps và tốc độ cụm. Tốc độ cụm này được ấn định bởi cơ sở hạ tầng, dựa trên nhu cầu người sử dụng và tính khả dụng của tài nguyên (cả băng thông vô tuyến lẫn các phần tử hạ tầng). Tùy thuộc vào tài nguyên và tình trạng di động được đánh giá tại một thời điểm, tốc độ cụm thích hợp sẽ được cấp cho một MS. Cấp phát cụm được thực hiện độc lập với đường lên và đường xuống dữ liệu của một MS.

1.1.1 Kiến trúc hệ thống số liệu gói CDMA2000

Kiến trúc hệ thống số liệu gói CDMA2000 mô tả ở hình 1.2, gồm các phần tử sau:

- MS có dạng máy cầm tay, PDA hay PCMCIA card trong máy tính xách tay/cầm tay hỗ trợ Simple IP hay MIP client hay cả hai.
- CDMA2000-1x RAN (Mạng truy nhập gói CDMA2000-1x).
- Chức năng điều khiển gói PCF (Packet Control Function).
- PDSN hỗ trợ chức năng tác tử ngoài FA (phương pháp truy nhập MIP).
- Tác tử nhà HA (phương pháp truy nhập MIP).



Hình 1.2 Kiến trúc số liệu gói CDMA2000

Khi MS kết nối đến trạm BTS, các bước thiết lập kết nối số liệu trong trường hợp MIP như sau:

1. MS thiết lập kết nối đến PDSN.
2. MS kết nối đến HA phục vụ (mạng nhà) qua một tunnel PDSN/FA và HA (tunnel MIP) do PDSN thiết lập.
3. Xác thực và ủy quyền được thực hiện tại PDSN và HA bằng cách yêu cầu hạ tầng AAA.
4. HA ấn định địa chỉ IP (động hoặc tĩnh) tại đầu mỗi phiên cho MS từ không gian địa chỉ IP của HA.

Khi MS kết nối đến trạm BTS, các bước thiết lập kết nối số liệu trong trường hợp IP đơn giản như sau:

1. MS thiết lập kết nối đến PDSN
2. PDSN xác thực MS.
3. PDSN ấn định địa chỉ IP cho MS
4. PDSN kết cuối liên kết PPP của người sử dụng và chuyển tiếp gói.
5. PDSN áp dụng các qui tắc lọc và chính sách khác khi cần.

Kết nối giữa MS và PDSN phục vụ đòi hỏi thiết lập một kết nối thứ hai cho thông tin IP. Kết nối này được đảm bảo bởi giao thức PPP và hỗ trợ IPCP, LCP, PAP và CHAP. PPP được khởi đầu bởi MS trong quá trình đàm phán kết nối và kết cuối bởi PDSN. Giữa mạng vô tuyến (MSC/PCF) và PDSN, lưu lượng PPP được đóng gói vào giao diện R-P (Radio-Packet).

PCF có các đặc điểm sau:

- Là phần tử mạng truy nhập vô tuyến (CDMA2000 RAN), có vai trò như một MSC và thực hiện như bộ điều khiển mạng RNC (Radio Network Controller).
- Chịu trách nhiệm thiết lập giao diện R-P và xử lý.
- Chuyển tiếp các khung PPP giữa MS và PDSN.
- Cho phép MS thay đổi PCF trong khi vẫn giữ MS gắn với cùng một PDSN và nhớ đệm số liệu của người sử dụng khi kết nối vô tuyến trạng thái "ngủ" được kết nối lại.

Vai trò của PDSN trong kiến trúc CDMA2000:

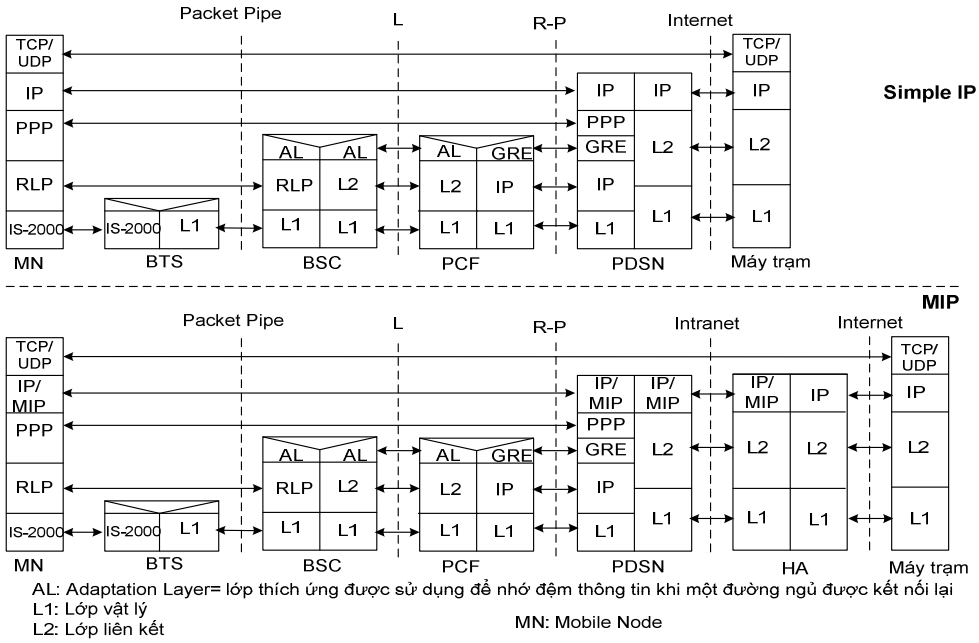
- Vai trò chính: kết cuối các phiên PPP khởi xướng từ MS và cung cấp chức năng FA (khi MIP yêu cầu) hay truyền các gói IP đến chặng tiếp theo (khi IP đơn giản được sử dụng).
- Xác thực người sử dụng và ủy quyền cho họ sử dụng các dịch vụ yêu cầu. Hỗ trợ tunnel ngược đến HA.
- Thiết lập, duy trì và kết cuối kết nối dựa trên PPP đến MS.
- Hỗ trợ AAA client để xác thực MS bởi AAA server địa phương.

Vai trò của giao diện R-P:

- Là một giao diện mở dựa trên giao thức truyền tunnel GRE (Generic Routing Encapsulation).
- Kết nối mạng vô tuyến và PDSN.
- Tách PDSN ra khỏi PCF, cho phép các hãng vô tuyến đưa ra các giải pháp PDSN đa nhà cung cấp vào mạng của họ.

Bằng các chuyển giao PCF trong khi vẫn giữ MS nối vào (neo vào) cùng một PDSN, các thiết bị di động dựa trên IP có thể đi qua các biên giới MSC mà không ảnh hưởng đến tính liên tục của phiên người sử dụng. Tức là người sử dụng chuyển dịch vào vùng phủ MSC mới, phiên người sử dụng không bị cắt, không buộc phải kết nối lại đến MSC mới và không nhận địa chỉ IP mới.

Hình 1.3 chỉ ra ngăn xếp giao thức tương ứng với mô hình kiến trúc số liệu gói hình 1.4.



Hình 1.3 Ngăn xếp giao thức dịch vụ gói CDMA2000

1.1.2 Thiết bị đầu cuối di động MS (Mobile station)

Trong CDMA2000, MS phải đảm bảo các yêu cầu sau:

- MS phải xác thực với HLR(Home Location Register) của nhà cung cấp dịch vụ cho truy nhập vô tuyến, và xác thực với PDSN và HA (sử dụng các truy nhập *IP đơn giản* hay *MIP)* cho truy nhập mạng số liệu.
- MS phải hỗ trợ giao thức nối mạng PPP, và khả năng xác thực dựa trên CHAP (với IP đơn giản), và hỗ trợ MIP client (với MIP)
- MS cũng phải hỗ trợ chuyển trạng thái ngủ/tích cực trên đường truyền vô tuyến

Trạng thái ngủ (các MS không có kết nối liên kết tích cực đến PCF)

- Cho phép MS hoặc MSC tạm ngưng kết nối đường truyền vô tuyến tích cực sau một khoảng thời gian không tích cực và giải phóng giao diện vô tuyến cùng với các tài nguyên BTS đang phục vụ.

- Nếu hoặc MS hoặc PCF liên kết có các gói cần phát trong khi ngủ, kết nối được tích cực lại và truyền dẫn lại tiếp tục.
- Tất cả các MS (tích cực hay ngủ) được đăng ký trong danh sách của PDSN và một ràng buộc với HA tương ứng.

Đối với chế độ MIP, PDSN/FA theo dõi thời gian còn lại của thời hạn hiệu lực đăng ký cho từng MS trong bảng định tuyến của nó và MS chịu trách nhiệm làm mới lại thời hạn của nó với HA. Nếu MS không đăng ký lại trước khi hết hạn đăng ký, PDSN sẽ chấm dứt liên kết với PCF đối với MS (PDSN/FA sẽ dừng định tuyến các gói đến MS) và kết thúc phiên. HA cũng làm tương tự nếu MS không đăng ký lại khi qua một PDSN khác.

Đối với các liên kết PPP mang lưu lượng tích cực, PDSN kết cuối phiên PPP với MS và chuyển tiếp lưu lượng IP được đóng gói đến MS từ HA hay đến HA từ MS qua truyền tunnel ngược. Đối với tất cả MS đã đăng ký, tồn tại một tunnel riêng duy nhất tới HA.

Các kiểu MS

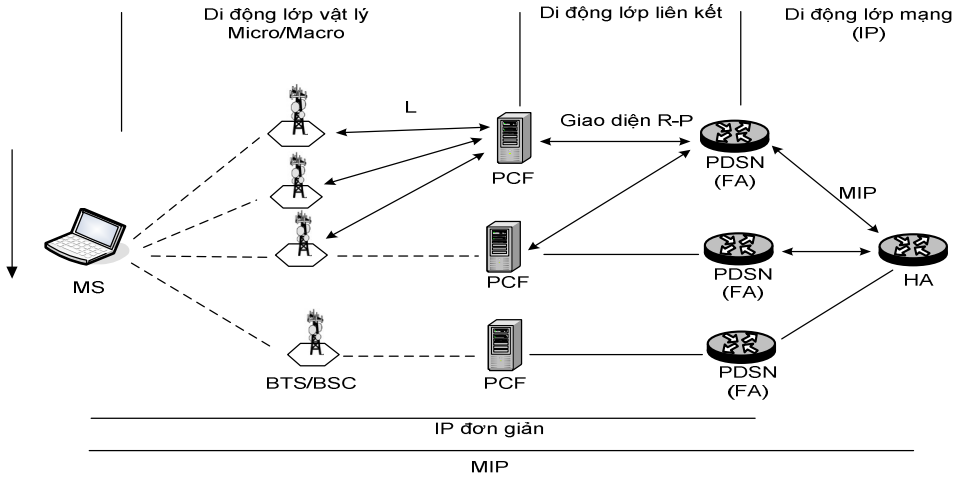
Tồn tại hai kiểu cấu hình MS cơ bản: Mô hình chuyển tiếp và mô hình mạng.

MS mô hình chuyển tiếp, đầu cuối di động được kết nối đến một đầu cuối số liệu cầm tay khác (như máy tính xách tay, thiết bị tính toán cầm tay ,..). Máy điện thoại mô hình chuyển tiếp không kết cuối bất kỳ lớp giao thức nào trừ lớp vật lý (giao diện vô tuyến) và lớp RLP. Còn các thiết bị đầu cuối số liệu đi kèm phải kết cuối tất cả các giao thức lớp cao hơn (PPP, IP, TCP/UDP…).

MS mô hình mạng, ngoài giao diện vô tuyến kết cuối tất cả các giao thức cần thiết, không cần bất cứ thiết bị đầu cuối bổ sung. Điển hình là PDA, PC Pocket,…

1.1.3 Các mức di động của CDMA2000

Kiến trúc số liệu gói CDMA2000 định nghĩa ba mức di động cho MS (Hình 1.4)



Hình 1.4. Phân cấp di động CDMA2000

Mức di động thứ nhất: tại lớp vật lý bởi chuyển giao mềm hay bán mềm giữa các BTS, trong khi MS neo giữ đến cùng một PCF, và trong suốt đối với PCF và PDSN.

Mức di động thứ hai: tại giao diện R-P trên lớp liên kết, mức này cho phép chuyển giao trong suốt từ PCF đến PCF trong khi vẫn duy trì phiên tại cùng một PDSN. Hai trạng thái sẽ xảy ra: Ngủ và tích cực. Trong trạng thái tích cực khi người sử dụng đi qua biên giới PCF, một chuyển giao xảy ra trong suốt đối với MS. MS tham gia vào chuyển giao bán mềm đến BSC (MSC) mới, trong khi phiên số liệu vẫn neo đến PCF gốc trong thời gian cuộc gọi và MS nằm trong trạng thái tích cực. Tức là khi MS trong trạng thái tích cực, không xảy ra thay đổi PCF phục vụ.

Khi MS trong trạng thái ngủ đi qua biên giới vùng phục vụ của một PCF, MS sẽ khởi động tích cực lại tại một BSC (MSC) mới để thiết lập một kết nối PCF. Điều này dẫn đến thay đổi PCF nhưng không nhất thiết thay đổi PDSN. PCF mới sẽ tìm cách ấn định MS cho PDSN đang phục vụ. Nếu PCF mới có kết nối đến PDSN này, thì MS và PDSN hoàn toàn không bị tác động.

Mức di động thứ ba (lớp mạng): là chuyển giao giữa các PDSN dựa trên sử dụng MIP. Giả sử MS đã đăng ký với HA và PDSN (MS đã được xác thực bởi hai phần tử này) để thiết lập IP tunnel cho lưu lượng cần truyền. Khi MS chuyển đến vị trí được phục vụ của một PCF kết nối đến PDSN mới, MS nhận được yêu cầu đăng ký

với PDSN mới này. Đăng ký này cập nhật các bảng ràng buộc tại HA, vì thế tất cả lưu lượng tiếp theo cho MS này sẽ định tuyến đến PDSN mới. Liên kết PPP của MS bị ảnh hưởng bởi sự thay đổi này trong khi địa chỉ IP không thay đổi, và tính di động vẫn giữ nguyên trong suốt đối với đối tác của MS.

Chế độ IP đơn giản chỉ thực hiện thông qua hai mức di động đầu. Còn chế độ MIP thực hiện cả ba mức trên.

1.1.4 AAA(Authentication, Authorization and Accounting) di động CDMA2000

Trước tiên ta xem xét một số khái niệm trong CDMA2000.

Mạng nhà:

- Một thuê bao có tài khoản (kế toán) được thiết lập với một nhà khai thác vô tuyến, nhà khai thác sẽ cung cấp dịch vụ thoại và số liệu cho người sử dụng và cung cấp mạng nhà cho thuê bao di động.
- Lưu lý lịch và thông tin xác thực người sử dụng.

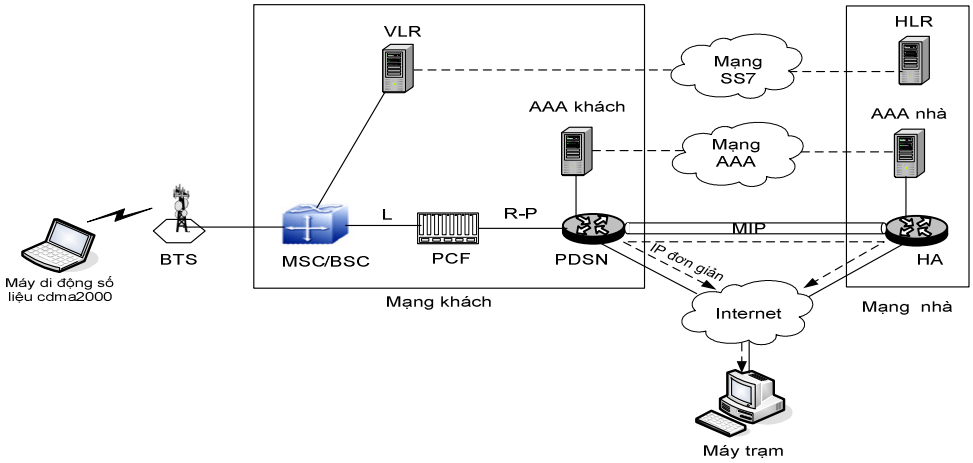
Mạng khách:

- Khi người sử dụng chuyển mạng vào vùng lãnh thổ của nhà khai thác khác
- Nhận thông tin xác thực và lý lịch dịch vụ từ mạng nhà của MS chuyển mạng.

Lý lịch dịch vụ: các tài nguyên vô tuyến người sử dụng được quyền sử dụng như: băng thông cực đại, mức ưu tiên truy nhập.

Trong CDMA2000 các lý lịch người sử dụng được lưu tại HLR mạng nhà và lưu tạm thời tại VLR mạng nhà.

Kiến trúc số liệu gói CDMA2000 được mô tả trên hình 1.5.



Hình 1.5 Mạng lõi CDMA2000 điển hình cùng với các hệ thống AAA

Khi một MS yêu cầu dịch vụ số liệu, đầu tiên MS vào trong giai đoạn đăng ký, nó sẽ bị xác thực hai lần: Trên lớp vật lý và trên lớp liên kết. *Xác thực lớp vật lý* (truy nhập mạng và thiết bị đầu cuối người sử dụng, chỉ xác thực MS) thực hiện bởi HLR và VLR, và dựa trên IMSI (International Mobile Station Identifier) [IS2000] của MS. *Xác thực lớp liên kết* (truy nhập mạng số liệu gói) thực hiện bởi các AAA server và các client. Quá trình này dựa trên số nhận dạng NAI (Network Access Identifier) [RFC2486] có dạng user@homedomain. Ngoài ra, NAI cho phép phân phát liên kết an ninh MIP đặc thù để hỗ trợ xác thực PDSN/HA trong thời gian đăng ký di động, ấn định HA và chuyển giao giữa các PDSN.

Sau khi hoàn thành giai đoạn đăng ký, người sử dụng muốn truy nhập đến mạng số liệu công cộng hay riêng, AAA mạng số liệu sẽ tiến hành xác thực người sử dụng

Hệ thống số liệu CDMA2000 đảm bảo hai cơ chế xác thực khi sử dụng phương pháp truy nhập IP đơn giản và MIP như định nghĩa trong [IS835] và [RFC3141].

- Đối với truy nhập IP đơn giản: xác thực dựa trên CHAP của giao thức PPP. Trong CHAP, PDSN hỏi (gửi challenge) MS bằng một giá trị ngẫu nhiên. MS trả lời (response) bằng một chữ ký MD-5, tên/mật khẩu người sử dụng. PDSN chuyển cặp challenge/response đến AAA server nhà để xác thực người sử dụng.

- Đối với truy nhập MIP: PDSN gửi challenge tới MS. MS trả lời response bằng một chữ ký và NAI (được kiểm tra bởi mạng nhà) cùng với yêu cầu đăng ký.

Cả hai cơ chế đều dựa trên *shared secrets* liên kết với NAI (lưu tại mạng nhà) và được hỗ trợ bởi cùng một hạ tầng AAA server. Trong cả hai trường hợp, số liệu kế toán được thu thập bởi PCF và PDSN được gửi đến AAA server địa phương. Trong đó PCF thu thập bản ghi kế toán truy nhập vô tuyến, và PDSN thu thập thống kê số liệu từng người sử dụng. Với MS chuyển mạng, AAA server địa phương chuyển một bản sao các bản tin kế toán RADIUS đến AAA server nhà.

Khi xảy ra chuyển giao giữa hai PDSN, PDSN được giải phóng gửi bản tin Accouting Stop (dừng kế toán) đến AAA server, và Accouting Start (bắt đầu kế toán) được gửi đến AAA server từ PDSN mới kết nối. Accounting Stop từ PDSN giải phóng đôi khi có thể đến sau Accounting Start từ PDSN mới (PDSN có thể không biết rằng MS đã rời đi, nhưng vẫn đợi thời hạn đăng ký hay tạm ngưng không tích cực PPP để kết thúc phiên). Điều này có nghĩa là server tính cước phải tiếp nhận nhiều chuỗi dừng/khởi tạo từ các PDSN khác nhau và xử lý chúng như một phiên duy nhất [IS 835]. Khi một bộ định thời không tích cực PPP hay thời hạn MIP đã hết hay MS kết thúc phiên, liên kết R-P được giải phóng và một Accounting Stop được gửi đến AAA server.

1.2 Số liệu chuyển mạch gói trong GSM và UMTS: GPRS và miền UMTS PS

Phần này xem xét hệ thống GPRS và miền UMTS PS, và các dịch vụ được cung cấp. Ta cũng xem xét các cách thức một MS truy nhập mạng liệu số gói, các giao thức được sử dụng và xác thực người sử dụng.

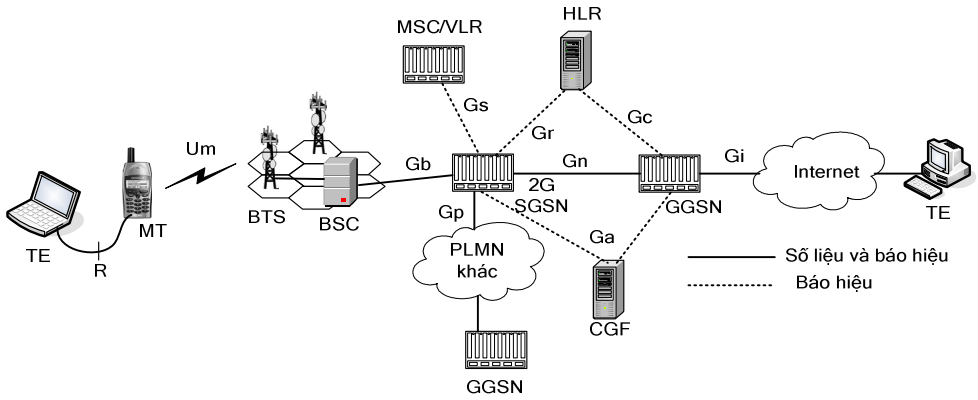
1.2.1 Các phần tử GPRS

Hệ thống GPRS mở rộng nối mạng số liệu gói của hệ thống GSM. GPRS hỗ trợ truyền dẫn số liệu gói trên giao diện vô tuyến và khả năng di động số liệu gói trong mạng lõi.

Để triển khai GPRS đòi hỏi cập nhật phần mềm BSS để

- ghép các dịch vụ số liệu lên các khe thời gian không bị các dịch vụ CS chiếm
- điều khiển dòng chảy và các cơ chế phát lại cần thiết để truyền số liệu gói trên công nghệ truyền dẫn vô tuyến GSM.

DNS và mạng thông minh (IN) là các phần tử bổ sung và là bộ phận của dịch vụ GPRS tiên tiến. Kiến trúc GPRS được ETSI định nghĩa và duy trì bởi 3GPP.



Hình 1.6 Kiến trúc GPRS

Hệ thống GPRS chủ yếu định nghĩa hai phần tử: BSS (Base Station System) và PLMN (Inter-PLMN Backbone Network). GPRS BSS và GSM BSS được tăng cường PCU (Packet Control Unit) để hỗ trợ các dịch vụ gói. Đường trục PLMN bao gồm hai nút mới: SGSN (Serving GPRS Support Node) và GGSN (Gateway GPRS Support Node). GGSN và SGSN được nối với nhau qua một mạng IP và tương tác với nhau qua giao diện Gn dựa trên giao thức GTP.

Đặc điểm chính của SGSN (còn gọi là 2G SGSN):

- Cung cấp các dịch vụ nén lớp mạng, chức năng phân đoạn và lắp ráp lại. Lập khung và ghép kênh lớp liên kết,
- Mật mã hóa cũng như xử lý báo hiệu MS và quản lý di động trong BSS, giữa các SGSN.
- Quản lý các GTP tunnel được thiết lập đến GGSN.
- Tương tác với HLR và IN, MSC và SMS-SC (SMS Service Center).
- Thu thập số liệu tính cước và truyền nó đến CGF trên giao diện Ga.

Đặc điểm chính của GGSN

- Neo giữ các phiên truyền số liệu.
- Cung cấp truy nhập đến các mạng số liệu gói bằng cách hỗ trợ kết cuối các GTP tunnel từ SGSN mà MS hiện thời đang nối đến.
- Cung cấp nền tảng và cổng đến các dịch vụ số liệu gói tiên tiến như Web, WAP, các mạng số liệu riêng ở xa.

Các phiên số liệu gói trong GPRS và UMTS PS được thiết lập bằng cách thiết lập và duy trì các GTP tunnel đến GGSN. Một GTP tunnel là quá trình đóng gói các gói giữa GGSN và SGSN trong GTP/UDP/IP.

Khi MS chuyển mạng, MS này nối đến một SGSN trong mạng khách và một GGSN mạng nhà hoặc mạng khách. Nếu GGSN mạng nhà, mạng IP được sử dụng để nối SGSN khách đến GGSN nhà và được gọi là mạng đường trục giữa các PLMN. Mạng đường trục giữa các PLMN thường được gọi là GRX (GPRS Roaming Exchange). Nét đặc biệt của GPRS liên quan đến GRX là SGSN mạng khách và GGSN mạng nhà tương tác với nhau trên mạng GRX qua giao diện Gp.

1.2.2 Các phần tử UMTS

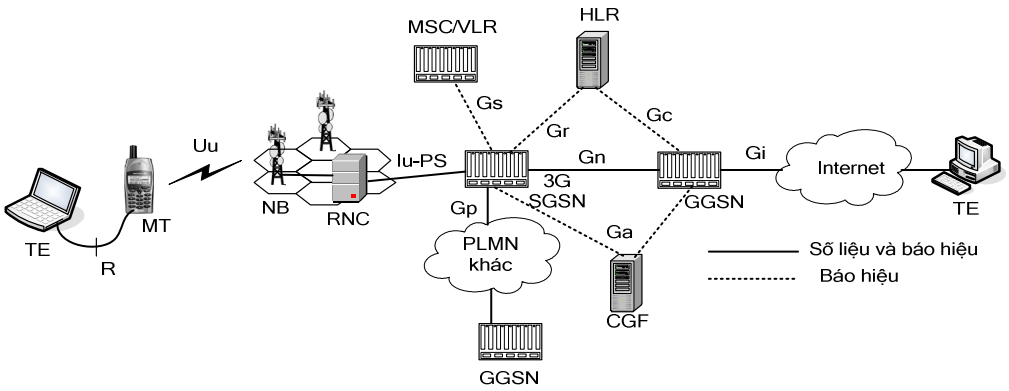
Với hệ thống UMTS, 3GPP định nghĩa miền CS cho dịch vụ chuyển mạch kênh và miền PS cho dịch vụ chuyển mạch gói. Vì tính di động, UTRAN (UMTS Terrestrial Radio Access Network) phải trong suốt đối với mạng lõi UMTS, nghĩa là mạng lõi không biết MS ở tại BTS nào.

Lõi miền UMTS PS giống lõi GPRS. Từ R99, cả hai đặc tả hệ thống không có các khác biệt kỹ thuật liên quan đến mạng lõi. Kiến trúc UMTS được cho trên hình 1.7 giống như kiến trúc GPRS.

Một số điểm khác biệt giữa UMTS PS và GPRS:

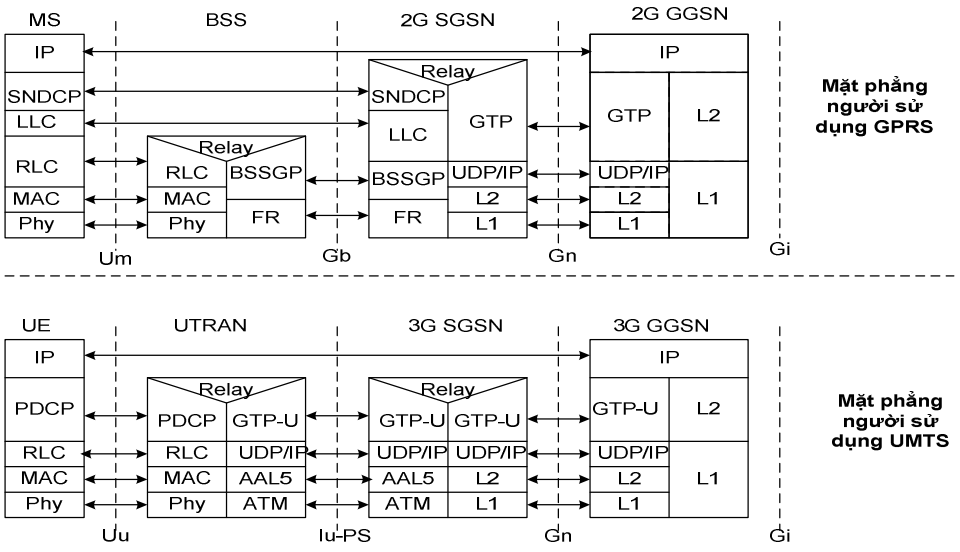
- UMTS PS sử dụng GTPv1 (GPRS sử dụng GTPv0).
- Hỗ trợ đa phương tiện
- SGSN (3G SGSN): không cung cấp nén lớp mạng hay mật mã hóa; chỉ chuyển tiếp các gói giữa GGSN và RNS trên GTP tunnel.

- RNC (Radio Network Controller):
  - Chức năng lớp liên kết được chuyển từ SGSN sang RNC (đảm bảo RAN trong suốt với mạng lõi).
  - Có vai trò như BSC trong GSM.
  - Quản lý tính di động của MS giữa các BTS.



Hình 1.7 Kiến trúc UMTS

Hình 1.8 trình bày ngăn xếp giao thức mặt phẳng người sử dụng hệ thống GPRS và UMTS.



Hình 1.8 Kiến trúc ngăn xếp giao thức mặt phẳng người sử dụng GPRS và UMTS.

1.2.3 Các khả năng dịch vụ của GPRS và miền UMTS PS

Các hệ thống GPRS và miền UMTS PS về nguyên tắc là đa giao thức và trung lập đối với lớp mạng hay các lớp liên kết của lưu lượng người sử dụng. Các giao thức người sử dụng còn được gọi là PDP (Packet Data Protocol).

GPRS đảm bảo hỗ trợ cho cả IPv4 và IPv6. Nó hỗ trợ PDP kiểu PPP từ R98, tuy nhiên các nhà cung cấp đầu cuối vẫn chưa hào hứng hỗ trợ kiểu PDP này. Hiện nay còn có rất nhiều tranh luận về PDP.

Các hệ thống GPRS và miền UMTS PS cung cấp kênh giao vận (transport) không tin cậy từ GGSN đến MS. Kênh này được đặc trưng bởi một số thông số QoS. Các thông số này khác nhau đối với các phiên bản trước R99 và sau R99. Sau R99 có thể phân biệt xử lý các gói thuộc cùng một phiên người sử dụng, bằng cách thiết lập các kênh mang *PDP contexts* cho các loại lưu lượng khác nhau và lý lịch QoS liên kết với cùng một phiên. Sau đó truyền gói trên kênh mang tương ứng dựa trên một số quy tắc phân loại được thiết lập tại GGSN và MS. Khả năng này đáp ứng yêu cầu cung cấp đa dịch vụ thông qua hệ thống UMTS. Trước R99, chỉ có một mức QoS và chỉ một PDP context liên kết với một phiên.

1.2.4 Đầu cuối cho GPRS và miền UMTS PS

Có ba loại GPRS MS khác nhau:

- **Loại A**: cho phép hỗ trợ đồng thời các dịch vụ GSM và GPRS.
- **Loại B**: MS giám sát các kênh tìm gọi GSM và GPRS, mỗi lần chỉ hỗ trợ một dịch vụ.
- **Loại C**: MS chỉ hỗ trợ dịch vụ GPRS.

Một đầu cuối di động có khả năng truy nhập UMTS PS hay GPRS đòi hỏi có hai thành phần logic: TE (Terminal Equipment) và MT (Mobile Termination). TE cung cấp khả năng tính toán, MT hỗ trợ các khả năng truy nhập số liệu vô tuyến. TE và MT thực hiện như các phần tử độc lập, chúng có thể được kết nối bởi nhiều công nghệ (nối tiếp, hồng ngoại, Bluetooth, …) với lớp liên kết dựa trên PPP hay một giao diện riêng khác. Hình 1.6 và 1.7 cho thấy hai phần tử MS phân cách nhau bởi

giao diện R, là giao diện bên trong giữa hai phần tử của một gói vật lý duy nhất chứ không phải các thực thể vật lý cách biệt.

Yêu cầu phổ biến hiện nay đối với thiết bị đầu cuối là khả năng song song hai chế độ GPRS/GSM và UMTS.

1.3 Kết luận

Trong chương này chúng ta đã đề cập đến mạng số liệu PS trong các hệ thống thông tin di động. Các khía cạnh đầu cuối và mạng lõi đã được đề cập. Các kiến thức của chương này sẽ là cơ sở để nghiên cứu MVPN trong các chương sau.

Chương 2 Cơ sở nền tảng MVPN

VPN đã được sử dụng rộng rãi trong công nghệ nối mạng. Ứng dụng mới nhất của VPN là MVPN, tuy hãy còn non trẻ và còn nhiều vấn đề chưa được giải quyết, cả về kỹ thuật lẫn kinh doanh. Nhưng chương trình khung cho MVPN đã được định nghĩa rộng rãi và đang có các triển khai ở nhiều dạng khác nhau.

Chương này đề cập đến MVPN, phân tích công nghệ của nó. Trước tiên sơ lược về công nghệ VPN số liệu truyền thống, sau đó bổ sung tính di động để nhận được bức tranh tổng thể về MVPN.

2.1 Định nghĩa VPN

VPN là sự kết hợp hai khái niệm: Nối mạng ảo và nối mạng số liệu riêng, là mô phỏng của các mạng số liệu riêng đảm bảo an ninh trên các phương tiện viễn thông công cộng chung không đảm bảo an ninh.

Thuộc tính VPN: gồm các cơ chế bảo vệ số liệu và thiết lập mối quan hệ tin cậy giữa các máy trạm trong mạng ảo. Đồng thời hợp nhất các phương thức khác nhau để áp đặt, duy trì các thỏa thuận dịch vụ (SLA), và chất lượng dịch vụ (QoS) cho các thực thể tạo lên mạng riêng ảo.

Mục đích chính của VPN: cho phép lựa chọn và truy nhập có đảm bảo an ninh đến tài nguyên nối mạng ở xa.

2.2 Các khối cơ bản của VPN

Các khối cơ bản của VPN bao gồm:

- Điều khiển truy nhập (Access Control)
- Xác thực (Authentication)
- An ninh (Security)
- Truyền tunnel
- Các thỏa thuận mức dịch vụ (Service Level Agreements)

Các khối này bao quát các kiểu VPN số liệu điển hình nhất, bao gồm cả MVPN.

Điều khiển truy nhập (AC)

- Là tập các chính sách và các kỹ thuật điều khiển truy nhập đến các tài nguyên nối mạng số liệu riêng cho các phía được ủy quyền.
- định nghĩa tài nguyên khả dụng cho người sử dụng sau khi đã được xác thực.
- Cơ chế AC hoạt động độc lập với xác thực và an ninh.

Xác thực (Authentication)

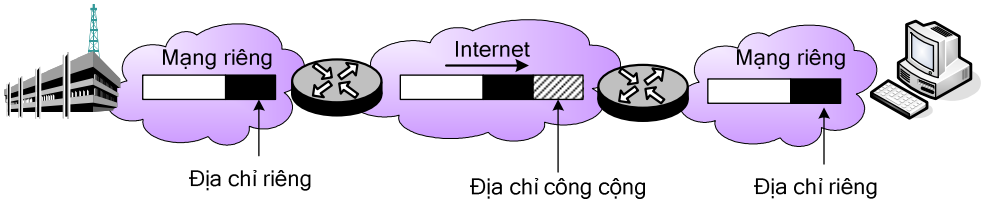
- Là chức năng quan trọng của VPN.
- Phương pháp xác thực phổ biến là PKI (Pubplic Key Infrastructure). PKI xác *thực dựa trên chứng nhận (certificate)*, các bên tham dự xác thực lẫn nhau thông qua trao đổi các chứng nhận của họ.
- Quá trình xác thực liên quan đến cung cấp thông tin xác thực dựa trên *Shared Secret* như: mật khẩu hay cặp challenge/response của CHAP cho người xác thực; NAS (Network Access Server) tra cứu file cục bộ hay truy vấn máy chủ RADIUS.
- Có hai kiểu xác thực trong VPN: xác thực client-cổng và cổng-cổng.
  Xác thực client-cổng: xác thực trong môi trường số liệu gói GPRS, là xác thực dựa trên RADIUS khi người sử dụng truy nhập GGSN. Chỉ khi thành công họ mới được sử dụng IPSec tunnel nối đến cổng IPSec mạng khách.
  Xác thực cổng-cổng: thường gặp khi kết nối site-site được thiết lập, hay khi các mạng quay số ảo được sử dụng, và khi đó xác thực thiết lập LTP2 tunnel được yêu cầu giữa LAC (L2TP Access Concentrator) và LNS (L2TP Network Server)..

An ninh (Security)

- VPN được xây dựng trên các phương tiện công cộng dùng chung không an toàn, vì thế tính toàn vẹn và mật mã hóa là yêu cầu tất yếu.
- Có thể đảm bảo an ninh cho VPN dựa trên phương pháp mật mã hóa đã có hay các cơ chế mật mã hóa kết hợp với các hệ thống phân bố khóa an ninh.
- An ninh không chỉ giới hạn ở mật mã hóa lưu lượng VPN, mà còn liên quan đến các thủ tục phức tạp của nhà khai thác và nhà cung cấp (chẳng hạn SIM card với các giải thuật và kiểm tra khóa bí mật).

Truyền tunnel

- Khái niệm truyền tunnel được áp dụng cho nối mạng riêng ảo. Là nền tảng của VPN.
- Truyền tunnel là công nghệ quan trọng xây dựng các IP VPN. Truyền tunnel bao gồm đóng gói (encapsulation) một số gói tin vào các gói khác theo một tập quy tắc được áp dụng cho cả hai đầu cuối của tunnel. Kết quả là nội dung được đóng gói trong tunnel không thể nhìn thấy đối với mạng công cộng không an ninh nơi các gói tin được truyền qua.
- Có thể định nghĩa tunnel bởi: các điểm cuối, các thực thể mạng nơi mở gói (decapsulation), và giao thức đóng gói được sử dụng. Các kỹ thuật truyền tunnel hỗ trợ VPN như L2TP hay PPTP được sử dụng để đóng gói các khung số liệu lớp liên kết (PPP). Tương tự các kỹ thuật truyền tunnel như IP trong IP và các chế độ IPSec được sử dụng để đóng gói các gói tin lớp mạng.
- Truyền tunnel thực hiện ba nhiệm vụ chính sau:
  - Đóng gói (Encapsulation).
  - Tính trong suốt đánh địa chỉ riêng: cho phép sử dụng địa chỉ IP riêng trên hạ tầng địa chỉ IP công cộng.
  - Bảo vệ tính toàn vẹn số liệu đầu cuối-đầu cuối và tính bí mật: đảm bảo rằng một người không được phép không thể thay đổi các gói truyền tunnel và do vậy nội dung gói được bảo vệ chống truy nhập trái phép.



Hình 2.1 Che đậy địa chỉ IP riêng bằng tunnel

- Khi áp dụng truyền tunnel để tạo lập một MVPN, ba chức năng (đóng gói, trong suốt đánh địa chỉ riêng, toàn vẹn số liệu đầu cuối-đầu cuối và bảo mật) phải đi kèm với một tập các cơ chế đảm bảo chuyển mạch tunnel động hay thiết lập lại nhằm hỗ trợ tính di động của người sử dụng VPN.

- Các tunnel di động dựa trên các hệ thống số liệu gói GPRS/UMTS và CDMA2000 móc nối với tunnel tĩnh tại biên mạng vô tuyến sẽ cho các kiến trúc MVPN khác nhau.

Các thỏa thuận mức dịch vụ SLA (Service Level Agreements)

- Các thực thể tham dự vào nối mạng ảo (các hãng vô tuyến, ISP, doanh nghiệp và người sử dụng từ xa) bị ràng buộc bởi các thỏa thuận để đạt được các mức dịch vụ yêu cầu cũng như các lợi nhuận mong muốn đối với các dịch vụ được cung cấp. Các thỏa thuận này được dự thảo giữa các bên quan tâm và các đối tác của họ để định nghĩa các mức cho phép định lượng và đánh giá dịch vụ được gọi là các SLA. Các SLA sử dụng ở nhiều dạng, và đặc biệt quan trọng đối với MVPN dựa trên hạ tầng dùng chung hay nhiều hạ tầng dùng chung.
- Các mạng số liệu di động sử dụng các quan hệ đồng cấp, cần nhiều SLA để hỗ trợ tất cả các dịch vụ và thực thể liên quan đến phía nhà cung cấp hoặc khách hàng.
- Các vấn đề liên quan đến SLA trong môi trường di động (MVPN SLA):
    - MVPN SLA đặc biệt phức tạp vì bao gồm cả phần vô tuyến và hữu tuyến.
    - Các yếu tố chính tác động đến chất lượng dịch vụ đầu cuối-đầu cuối:
        - Không thể đảm bảo được hiệu năng phần vô tuyến phù hợp (vì bản chất không dự đoán được của giao diện vô tuyến).
        - Người sử dụng có thể chuyển đến một mạng bên ngoài miền quản lý của nhà cung cấp dịch vụ mạng nhà
    - Các vấn đề cần xem xét khi soạn thảo một MVPN SLA điển hình là:
        - Tunnel cố định: tính khả dụng, đảm bảo băng thông, độ trễ.
        - Tốc độ tế bào/gói đỉnh và chấp nhận được; Tỷ lệ gói tin mất.
        - Các đảm bảo liên tục phiên (giới hạn về thời gian kỳ vọng mà phiên có thể bị mất trong một số vùng phủ và trong một số điều kiện di động của vùng phủ có độ rộng giới hạn.

- Các thời gian tạm ngưng của các phiên rỗi (có thể khác với thời gian tạm ngưng thường buộc thi hành bởi server truy nhập mạng, do nhu cầu tiết kiệm tài nguyên phía mạng vô tuyến).
- Các vùng được phép chuyển mạng và hiệu năng khi chuyển mạng.

2.3 Phân loại công nghệ VPN

Có hai cách tiếp cận để phân loại công nghệ VPN:

- ***Phân loại theo kiến trúc***: Xét đến cách triển khai kiến trúc.
- ***Phân loại theo truyền tunnel***: Xét đến thực thi các kỹ thuật truyền tunnel.

Về mặt lịch sử, phân loại theo kiến trúc được sử dụng nhiều hơn trong các tài liệu nối mạng VPN số liệu hữu tuyến, còn phân loại theo truyền tunnel được sử dụng trong các tài liệu về các hệ thống thông tin di động. Phần này chỉ đề cập đến *Phân loại theo truyền tunnel.*

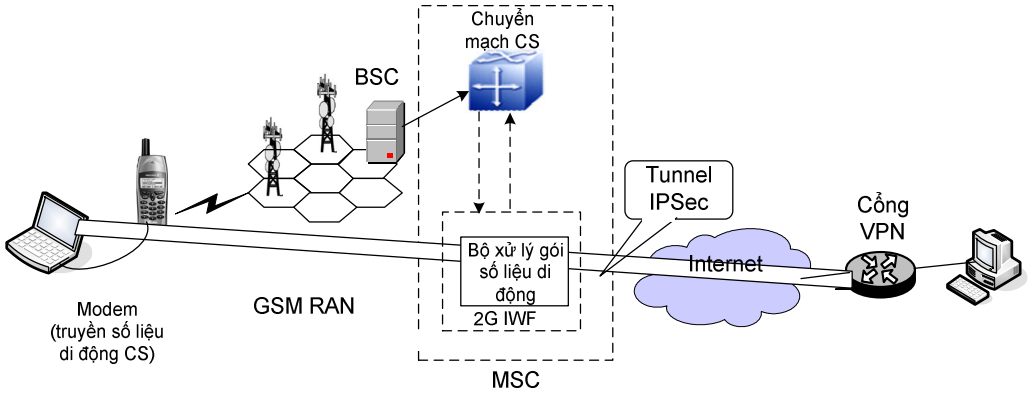
Đối với các VPN dựa trên truyền tunnel ta có thể phân loại chúng như sau:

- Đầu cuối - đầu cuối, hay *tự ý* (voluntary).
- Dựa trên mạng, hay *bắt buộc* (compulsory).
- Các tunnel móc nối hay trung gian (Chained or mediated tunnels).

VPN tự ý

- Cho phép người sử dụng ở xa tạo lập tunnel từ các thiết bị đầu cuối của mình (như máy điện thoại di động, PDA,…) đến một điểm kết cuối tunnel (như một cổng VPN đặt trong mạng số liệu riêng). PDA người sử dụng có thể thiết lập một IPSec tunnel có ESP đến mạng doanh nghiệp bằng cách sử dụng khoá phân tán dựa trên PKI (phương pháp khóa không đối xứng) hay khóa *shared secret* phân tán trước (phương pháp khóa đối xứng).
- Người sử dụng ở xa mở "tự ý" kênh thông tin đến mạng số liệu riêng khi cần.
- Truyền tunnel chỉ tồn tại trong thời gian của phiên và bị ngắt kết nối khi người sử dụng từ xa không còn yêu cầu truy nhập mạng số liệu riêng hoặc người sử dụng từ xa bị ngắt kết nối khi gặp một tập các sự kiện định nghĩa trước (như khoảng thời gian phiên, các giới hạn quyền truy nhập).

- Các VPN tự ý yêu cầu ấn định các địa chỉ IP công cộng đúng theo cấu hình topo cho thiết bị người sử dụng ở xa.
- Do số lượng IPv4 khả dụng với các nhà khai thác TTDĐ có hạn (vì phải cung cấp nối mạng IP "thường xuyên" cho khách hàng), nên để tiết kiệm không gian địa chỉ IP, nhiều kỹ thuật đã được kết hợp với nhau: sơ đồ đánh địa chỉ riêng (private), subnet, NAT, ...
- Một số ưu điểm của *VPN tự ý*:
    - Là cách đơn giản nhất để thiết lập kết nối truy nhập VPN từ xa.
    - Nhà quản lý mạng số liệu riêng chỉ cần cung cấp cổng VPN kết nối đến mạng Internet (hay mạng IP), có khả năng kết cuối truyền tunnel, thiết lập một tập các chính sách, và các thủ tục an ninh.
    - Không đòi hỏi mọi quan hệ được thiết lập trước giữa các doanh nghiệp (mạng số liệu riêng) và nhà cung cấp dịch vụ. Vì thế sẽ không có các SLA và các thỏa thuận quy định về bảo mật số liệu.
- Nhược điểm của *VPN tự ý*:
    - Chất lượng dịch vụ thấp và thất thường (do không có các SLA).
    - Khi các MVPN thực hiện trong môi trường TTDĐ, truyền tunnel tự ý sẽ thêm một tầng đóng gói trên đường truyền vô tuyến chặng cuối cùng, làm tiêu tốn hơn các tài nguyên vô tuyến đắt tiền và quí hiếm.
    - Mật mã hóa và các giải thuật an ninh phức tạp không phù hợp cho các thiết bị vô tuyến nhỏ do khả năng xử lý và nguồn acqui có hạn.
    - Các điều kiện vô tuyến dễ thay đổi, môi trường vô tuyến gây tổn hao không thuận lợi cho việc thiết lập và duy trì các IPSec tunnel. Điều này làm cho thời gian thiết lập tunnel dài, dẫn đến sự cố hoàn toàn và đòi hỏi phải chuyển đến vùng phủ sóng tốt hơn.



Hình 2.3 VPN tự ý trên mạng TTDĐ 2G

Vì các lý do trên, dù truyền *tunnel tự ý* đảm bảo giải pháp đầu cuối-đầu cuối an ninh và trong suốt truy nhập đến mạng số liệu riêng, nhưng hiệu suất VPN và các dịch vụ lại chỉ có thể đạt được khi có sự tham ra của các nhà cung cấp dịch vụ.

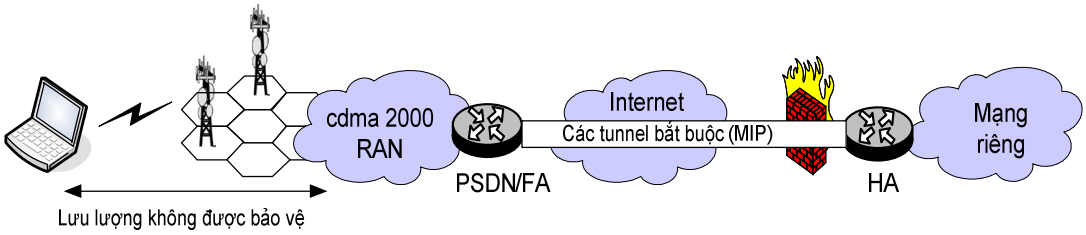
VPN bắt buộc

- Dịch vụ *VPN bắt buộc* cung cấp bằng cách móc nối nhiều tunnel, hay cung cấp một tunnel duy nhất cho từng đoạn đường đi số liệu giữa hai điểm cuối tham dự.
- Người sử dụng ở xa không cần tham dự vào quá trình thiết lập VPN. Họ bị "buộc" sử dụng dịch vụ được cung cấp mỗi khi cần truy nhập mạng.
- Yêu cầu cơ sở hạ tầng mạng nhà khai thác có tính năng thông minh và các chức năng cần thiết để hỗ trợ các dịch vụ VPN dựa trên một tunnel (hay tập các tunnel) được cung cấp giữa mạng số liệu riêng và mạng của nhà cung cấp dịch vụ (hơn là tác động đến người sử dụng đầu cuối).
- Doanh nghiệp (mạng số liệu riêng) phải thiết lập SLA với nhà cung cấp dịch vụ VPN, phải tin tưởng nhà cung cấp dịch vụ trong việc xử lý số liệu với trách nhiệm và bí mật cần thiết.
- Nhà cung cấp dịch vụ VPN tham dự vào điều khiển truy nhập mạng, thực thi chính sách truy nhập mạng số liệu riêng do nhà quản lý mạng số liệu riêng đưa ra.
- Các ưu điểm:
    - *VPN bắt buộc* sử dụng tốt hơn giao diện vô tuyến do không cần chi phí đóng gói trên giao diện vô tuyến.

- Thiết bị đầu cuối không phải hỗ trợ bất kỳ một VPN client nào (các VPN client đòi hỏi CPU xử lý mạnh và tiêu thụ nguồn nhiều).
- Người sử dụng không tham gia vào việc tạo lập VPN, chỉ cần yêu cầu dịch vụ khi truy nhập mạng của nhà cung cấp dịch vụ.
- Nhà cung cấp dịch vụ không tham dự vào quá trình cung cấp, thậm chí cũng không biết về sự tồn tại lưu lượng được đóng gói và được mật mã hóa.
- Các nhà cung cấp dịch vụ kiểm soát người sử dụng nhiều hơn: tham dự vào quá trình xác thực và gán địa chỉ IP. Các địa chỉ IP được ấn định đến người sử dụng ở xa từ không gian địa chỉ riêng mạng (private) khách hàng, vì thế tiết kiệm được các địa chỉ IP định tuyến công cộng từ phía nhà cung cấp.

- Nhược điểm: Có một đoạn tuyến số liệu riêng không được bảo vệ (giữa MS và RAN, lưu lượng được phát trên kênh vô tuyến khó đảm bảo an ninh). Phải tin vào nhà cung cấp dịch vụ. Thiết lập các SLA và các thỏa thuận bảo mật số liệu phức tạp.

Hình 2.4 cho thấy kịch bản áp dụng VPN bắt buộc, số liệu người sử dụng đóng gói vào MIP tunnel giữa PDSN nhà cung cấp dịch vụ và HA mạng số liệu riêng.

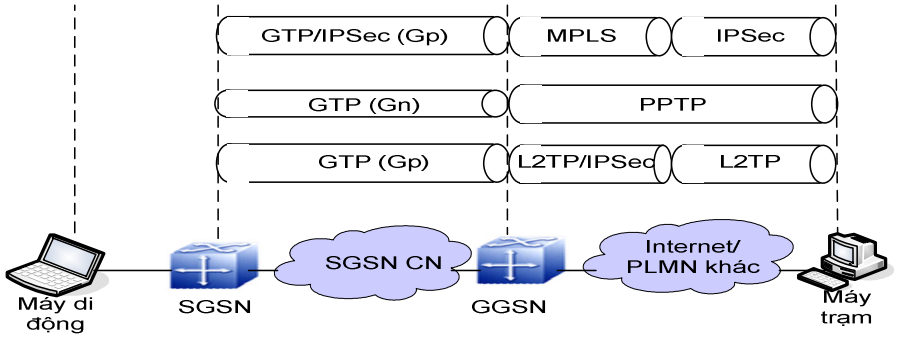


Hình 2.4 VPN bắt buộc trong CDMA2000

VPN tunnel móc nối (Chained Tunnel VPN)

- VPN này bao gồm một tập các tunnel móc nối kéo dài toàn bộ đường truyền đến thiết bị đầu cuối. VPN tunnel móc nối có nhiều dạng, và nhiều cách móc nối tunnel trong mạng GPRS.
- VPN tunnel móc nối đảm bảo bảo vệ số liệu đầu cuối-đầu cuối người sử dụng và người sử dụng tham gia vào khởi đầu tunnel (Giống VPN tự ý).

- Nhà cung cấp dịch vụ tham dự vào cung cấp và cấu trúc VPN tunnel móc nối, dễ dàng áp dụng QoS, và tạo dạng lưu lượng tại các điểm móc nối tunnel (giống VPN bắt buộc). Sự tham gia này không cần SLA và các thỏa thuận xử lý số liệu.



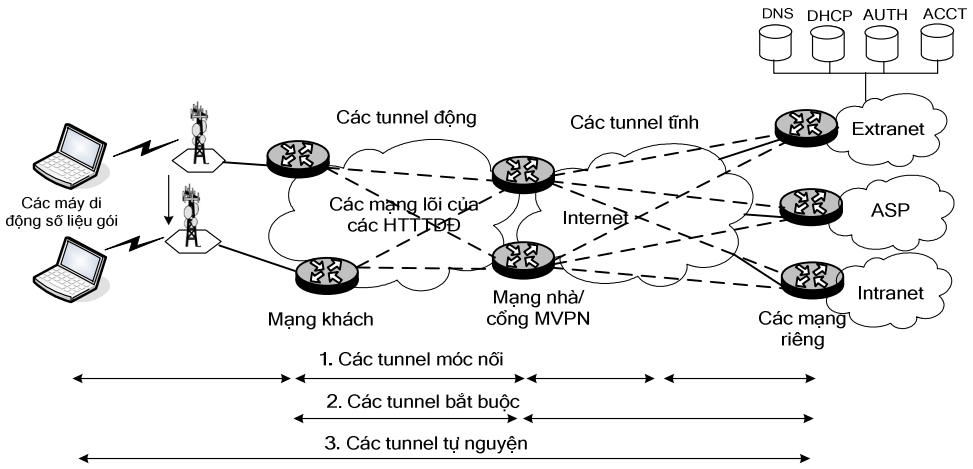
Hình 2.5 Một số tùy chọn VPN tunnel móc nối trong môi trường GPRS.

Tất cả các dạng VPN nói trên đều có các ưu và nhược điểm của riêng mình.Các nhà cung cấp dịch vụ có thể chào hàng chúng tùy thuộc vào công nghệ khả dụng, khả năng phù hợp với từng nhiệm vụ và môi trường kinh doanh.

2.4 VPN trong môi trường số liệu gói vô tuyến di động

Phần này đề cập đến hỗ trợ VPN trong mạng số liệu gói vô tuyến 2,5G và 3G.

Công nghệ số liệu gói TTDĐ dựa trên khái niệm truyền tunnel động, trong đó các tunnel liên tiếp được tạo lập và rỡ bỏ giữa các mạng ngoài và mạng nhà. Tính phức tạp khi cung cấp dịch vụ VPN trong môi trường này là ở cách kết hợp kỹ thuật này với cấu hình tunnel cố định hay "tựa cố định" cần thiết ở phía mạng hữu tuyến để cho phép người sử dụng di động có thể truy nhập mạng số liệu riêng an ninh. Nhiệm vụ này đặc biệt phức tạp khi cần dịch vụ VPN bắt buộc. Nhà khai thác phải có thiết bị có khả năng không chỉ hỗ trợ truyền tunnel động mà cả chuyển mạch tunnel động giữa các phần cố định và động trong hạ tầng của họ. Hình 2.6 cho thấy kiến trúc minh họa yêu cầu này. Trong trường hợp VPN tự ý, nhiệm vụ này đơn giản hơn, vì địa chỉ IP của điểm cuối giữ cố định. Các sơ đồ di động số liệu sử dụng trong GPRS và CDMA2000 phải giải quyết yêu cầu này.



Hình 2.6. VPN trong các môi trường vô tuyến

Hỗ trợ MVPN đòi hỏi các nút mạng có khả năng chuyển mạch các tunnel phức tạp và các thiết bị di động. Trong số liệu gói vô tuyến, các cơ chế lớp mạng cho phép các MS thay đổi vị trí và điểm nối mạng của chúng trong khi vẫn duy trì kết nối đến mạng nhà. Khi MS di chuyển đến một mạng khác thuộc một nhà khai thác khác với nhà khai thác ban đầu, MS vẫn giữ kết nối đến mạng nhà thông qua sử dụng các sơ đồ truyền tunnel hỗ trợ di động như GTP (trong GSM và UMTS) hay MIP (trong CDMA2000). Trong các môi trường này, không thể thiết lập mọi kết nối kênh cố định kiểu quay số giữa MS và mạng số liệu riêng. Vì nó sẽ làm hỏng mục đích chuyển từ môi trường chuyển mạch kênh sang chuyển mạch gói.

Công nghệ tốt nhất cho truy nhập mạng số liệu riêng trong môi trường này là MVPN, hoặc bắt buộc hoặc tự ý dựa trên các giao thức truyền tunnel di động phù hợp, ít nhất là trên một đoạn của tuyến số liệu đầu cuối-đầu cuối. Vì thế MVPN trong các hệ thống số liệu gói không chỉ đơn giản là một tùy chọn truy nhập (so với các kiểu truy nhập khác như quay số trực tiếp, các đường thuê riêng, ATM và Frame Relay trong nối mạng hữu tuyến) mà là cần thiết. Sau khi đã xem xét tầm quan trọng của các MVPN, bây giờ ta xét chi tiết hơn các kiểu MVPN chính.

MVPN tự ý

MVPN dựa trên truyền tunnel tự ý áp dụng gần giống như VPN hữu tuyến. Cũng như với VPN hữu tuyến, cần xét xem nhà cung cấp dịch vụ sử dụng sơ đồ đánh địa chỉ IP riêng hay công cộng và NAT nào (nếu cần) được sử dụng. Một cách

xem xét khác riêng cho môi trường vô tuyến là tính ổn định của địa chỉ IP được ấn định cho thiết bị di động. Tổng quát, các giao thức truyền tunnel hỗ trợ di động trong các hệ thống số liệu gói tiên tiến cho phép giữ nguyên các địa chỉ IP ấn định cho MS. Một số thậm chí còn cho phép cung cấp trước các địa chỉ IP cố định, đây là điều kiện tốt để các tunnel đầu cuối-đầu cuối ổn định tạo thành nền tảng cho VPN tự ý ổn định.

Tuy nhiên trong một số hệ thống vô tuyến, một số chế độ truy nhập chỉ cung cấp di động IP hạn chế. Thí dụ trong CDMA2000, chế độ truy nhập IP đơn giản chỉ đảm bảo di động trong biên giới của một PDSN/FA. Ở đây không thể duy trì các tunnel đầu cuối-đầu cuối khi thay đổi PDSN phục vụ, vì kênh mang số liệu gói cần được thiết lập lại đến PDSN mới và MS phải nhận được địa chỉ IP mới. Đòi hỏi MS client phải khởi động lại phiên với địa chỉ IP mới. Điều này có thể không phải là vấn đề quan trọng khi cho rằng một PDSN điển hình có thể phủ với diện tính lớn, nhưng đối với người sử dụng di chuyển dọc biên giới thì đây sẽ là một thách thức. Sử dụng VPN bắt buộc với chế độ truy nhập IP đơn giản sẽ không cải thiện tình trạng này, vì kết nối đầu cuối-đầu cuối bị mất và cần phải thiết lập lại truy nhập mạng từ xa mỗi khi MS chuyển vào PDSN mới. Điều này sẽ thay đổi nếu sử dụng chế độ truy nhập MIP theo hai cách: Cung cấp truy nhập trực tiếp đến mạng mà người sử dung cần truy nhập nhưng vẫn đảm bảo di động; Hoặc nhà khai thác có thể cung cấp truy nhập không gián đoạn, và người sử dụng chọn thiết lập tự ý một tunnel đầu cuối-đầu cuối bằng cách sử dụng VPN client chung.

Một đặc điểm đáng quan tâm khác của tính truy nhập MVPN tự ý: do đặc tính truy nhập MVPN tự ý dễ dàng cho MS, nên lợi nhuận trên một thuê bao từ khách hàng truy nhập mạng số liệu riêng sử dụng VPN client lớn hơn rất nhiều so với truy nhập người tiêu dùng thông thường.

MVPN bắt buộc

MVPN bắt buộc dựa trên các nguyên tắc giống như VPN hữu tuyến. Tuy nhiên VPN hữu tuyến dựa trên một tunnel cố định duy nhất (hay một ít các tunnel móc nối cố định), thì MVPN áp dụng trong môi trường di động dựa trên tổ hợp các tunnel

động hỗ trợ di động và các tunnel cố định ở phía hữu tuyến, gọi là *chuyển mạch truyền tunnel động*. Đòi hỏi các nhà khai thác vô tuyến phải triển khai các phần tử hạ tầng thông minh có khả năng hỗ trợ nhiều loại kỹ thuật truyền tunnel.

Chuyển mạch tunnel là một khái niệm khá mới, đầu tiên được các nhà cung cấp thông tin số liệu hữu tuyến đưa ra để cạnh tranh trong thị trường các dịch vụ IP. Các thiết bị hỗ trợ khả năng chuyển mạch tunnel phải định tuyến số liệu đi qua các tập tunnel bằng cách kết cuối các tunnel mang số liệu và khởi đầu các tunnel đóng gói số liệu ra. Điều này thường được xây dựng trên một tập các chính sách được cung cấp trong mạng hay trong các thiết bị đơn lẻ bởi các nhà khai thác vô tuyến đại diện cho các khách hàng kinh doanh.

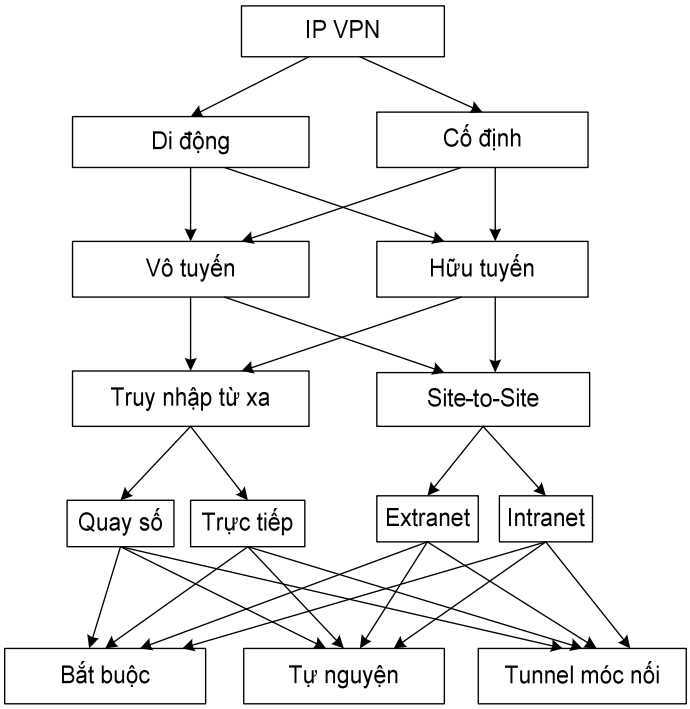
MVPN bắt buộc có thể áp dụng theo các cách khác nhau, phụ thuộc vào mô hình di động triển khai. Chẳng hạn, khi di chuyển của người sử dụng bị hạn chế, có thể xây dựng một dịch vụ bắt buộc trong chế độ truy nhập IP đơn giản của CDMA2000. Đây là trường hợp thường xảy ra đối với các doanh nhân khi truy nhập mạng riêng từ các điểm nóng (như nhà chờ sân bay hay khách sạn). Dịch vụ này đòi hỏi thiết lập động một L2TP tunnel giữa PDSN phục vụ và mạng khách hàng. Thực chất, không thể phân bổ một PDSN cụ thể, nơi có thể định nghĩa một tunnel bắt buộc cố định giữa doanh nghiệp và nhà khai thác vô tuyến, vì thuê bao có thể sử dụng mọi PDSN làm mạng truy nhập vô tuyến nơi nó di chuyển đến.

Về mặt kiến trúc, có thể áp dụng dịch vụ bắt buộc trong các hệ thống CDMA2000 hay GPRS bằng cách cho phép thiết bị là điểm cuối của các giao thức hỗ trợ di động (như PDSN hay HA hay GGSN) cũng là điểm khởi đầu trao đổi lưu lượng với các mạng khách hàng thông qua một tập các tunnel cố định.

Thị trường và nhu cầu khách hàng sẽ quyết định lựa chọn nào trong các lựa chọn MVPN đề cập đến ở trên.

2.5 Kết luận

Chương này nghiên cứu công nghệ VPN nói chung, phân loại các thuật ngữ và sau đó bổ sung tính di động để giới thiệu MVPN. Hình 2.7 tạo lên một phân cấp VPN rõ ràng. Phân cấp này sẽ là nền tảng tốt cho các nghiên cứu trong các chương sau đối với MVPN.



Hình 2.7. Cây phả hệ VPN

Chương 3 Giải pháp VPN trên CDMA2000

Chương này phân tích các kiểu dịch vụ VPN chính mà hệ thống CDMA2000 có thể cung cấp. Đầu chương phân tích các thủ tục và truyền an ninh giữa PDSN (Packet Data Serving Node) và các mạng số liệu riêng khi các phương pháp MIP và *IP đơn giản* được sử dụng. Sau đó xét đến các chiến lược triển khai HA khác nhau khi chuyển sang ấn định địa chỉ IP cho CDMA2000 và các vấn đề AAA. Cuối cùng trình bày thí dụ về triển khai thực tế dịch vụ số liệu.

Hầu hết chương này tập trung vào phương pháp VPN bắt buộc của CDMA2000 được xây dựng trên cơ sở truyền tunnel đầu cuối-đầu cuối và độc lập với các công nghệ cơ sở mức thấp hơn. Các VPN này không thay đổi quá nhiều giữa các hệ thống thông tin khác nhau, và CDMA2000 không phải là ngoài lệ khi cung cấp địa chỉ IP công cộng cho thiết bị người sử dụng, hoặc sử dụng địa chỉ IP riêng kết hợp với cơ chế truyền IPSec NAT-T. Phần "quản lý địa chỉ IP" sẽ chi tiết hơn vấn đề này.

3.1 Truy nhập mạng số liệu riêng CDMA2000

Hệ thống nối mạng số liệu của mạng lõi CDMA2000 được xây dựng trên cở sở các dịch vụ của lớp liên kết, cung cấp bởi PPP kết hợp với sơ đồ di động đa lớp phức tạp bao gồm cả MIP. Dịch vụ VPN cung cấp trong hệ thống này dựa trên đóng gói PPP kết hợp với L2TP, cho phép xác thực người sử dụng và lập cấu hình đầu cuối bằng cách tự mình kết cuối các phiên PPP và LNS. Thêm vào đó, giao thức MIP cũng được sử dụng và lớp liên kết PPP được kết cuối tại mạng của nhà khai thác. Trong cấu hình này, các tính năng tiên tiến của MIP như xác thực và lập cấu hình địa chỉ IP động, được cộng đồng CDMA2000 sử dụng để chuyển mạng người sử dụng. Tính năng này đặc biệt quan trọng trong hỗ trợ MVPN, và được phần tử hạ tầng PDSN của CDMA2000 hỗ trợ. PDSN xử lý các phiên PPP được khởi xướng bởi MS và đóng gói lưu lượng người sử dụng để truyền qua mạng lõi của nhà khai thác hay qua mạng IP công cộng như Internet. PDSN kết cuối tunnel được khởi xướng trong các mạng số liệu riêng và hướng các gói đến MS.

Mặc dù mức độ an ninh cho lưu lượng số liệu trong CDMA2000 được cho là đủ, nhưng việc truyền tunnel bắt buộc không thể bảo vệ an ninh đầu cuối-đầu cuối như các phương pháp tự ý. Lúc này để đảm bảo an ninh đầu cuối-đầu cuối, các nhà khai thác mạng phải bảo vệ an ninh cho đoạn truyền số liệu không được bảo vệ (phần giao diện vô tuyến và các đoạn truyền bên trong mạng nhà khai thác) bằng tunnel bắt buộc an ninh. Thông thường nhà khai thác vô tuyến cung cấp cho khách hàng mức độ đảm bảo cao về an ninh trong mạng của họ, coi như điều kiện kiên quyết để thiết lập quan hệ tin cậy cần thiết cho thực thi dịch vụ VPN bắt buộc. Đối với MS chuyển mạng, các đối tác chuyển mạng (mạng khách) phải đảm bảo mức an ninh tương đương khi cung cấp dịch vụ chuyển mạng.

Trong CDMA2000, VPN dựa trên IP đơn giản và MIP cũng không thể tránh được sự cần thiết phải có quan hệ tin cậy trong dịch vụ VPN bắt buộc. Mặc dù các tiêu chuẩn cố gắng tránh cho nhà khai thác tham gia vào liên kết an ninh giữa MS và mạng số liệu riêng, số liệu truyền qua mạng truy nhập vô tuyến vẫn luôn nhạy cảm với các truy nhập trái phép tại PDSN. PDSN trong mạng nhà khai thác vô tuyến là điểm kết cuối PPP cũng như điểm khởi tạo MIP hoặc L2TP, nên các gói IP dễ bị nghe trộm. Vì thế PDSN là một mắt xích yếu trong chuỗi các thiết bị tham gia vào truyền lưu lượng người sử dụng khi sử dụng chế độ VPN bắt buộc.

3.2 IP đơn giản

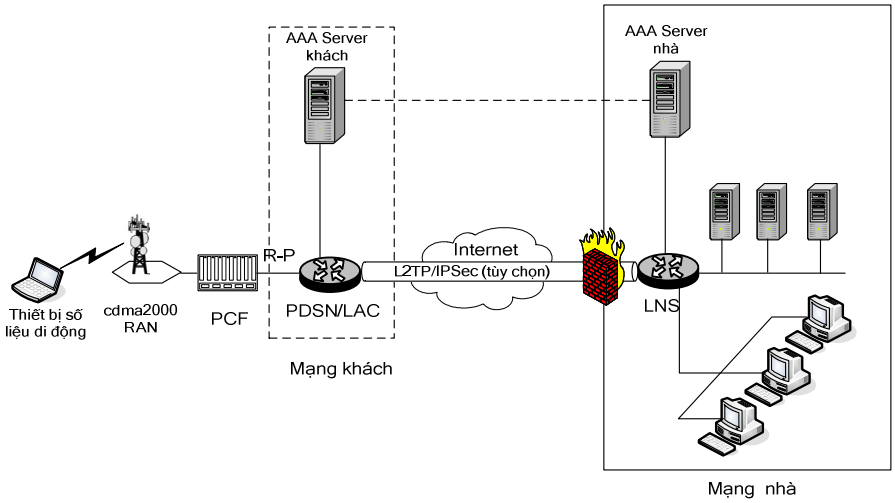
Như hình 1.4 ở chương một đề cập mô hình di động số liệu ba lớp CDMA2000. MIP cung cấp một trong ba mức di động, trong khi vẫn giữ nguyên địa chỉ IP của MS khi MS thay đổi PDSN phục vụ. Khi không có dịch vụ MIP (vì bất cứ một lý do nào), dịch vụ IP đơn giản đươc sử dụng. Trong IP đơn giản, các phiên PPP do MS khởi xướng được kết cuối tại PDSN theo cách giống như MIP. Tuy nhiên nếu MS thay đổi PDSN phục vụ, phiên PPP bị kết thúc và MS phải nhận địa chỉ IP mới khi vào vùng phục vụ PDSN mới.

Các nhà cung cấp thiết bị hạ tầng CDMA2000 đã rất cố gắng giải quyết vấn đề này trên các lớp vật lý và liên kết. Một giải pháp thông dụng (hình 3.1) là kết nối hài hòa các PCF (Packet Control Function) và PDSN. Giải pháp này đảm bảo MS

luôn neo tại một PDSN ngay cả khi PCF phục vụ nó thay đổi, vì kết nối PPP được thiết lập giữa MS và PDSN, và nếu mạng cơ sở giữ nguyên sự tồn tại kết nối này thì phiên PPP vẫn được bảo toàn. Bằng cách đó, địa chỉ IP của MS không đổi và thậm chí giữ nguyên khi chuyển qua biên giới MSC. Mặc dù phải tốn kém đường trục và các hạn chế ấn định địa chỉ IP, giải pháp này chỉ hoạt động trong thời gian phiên. Nói cách khác, sau khi mất phiên, cần phải có địa chỉ IP động mới và sau đó MS khôi phục lại. Điều này càng hay xảy ra khi vùng phủ sóng hẹp. Vì thế IP đơn giản không được coi là phương pháp truy nhập chủ yếu cung cấp cho khác hàng, khi họ đòi hỏi dịch vụ chất lượng cao trong yêu cầu sử dụng dịch vụ. Do các hạn chế này, các thuê bao sử dụng các máy di động làm việc ở chế độ IP đơn giản thường không thể nhận được dịch vụ MVPN thực sự. Trong nhiều trường hợp MS kết nối trong chế độ IP đơn giản không thể duy trì các kết nối bắt buộc lẫn tự nguyện, nếu PDSN phục vụ thay đổi. Đối với người sử dụng "không may mắn" này, có thể mô phỏng cảm giác MVPN bằng các ứng dụng được thiết kế đặc biệt hay các tăng cường hạ tầng đặc biệt, nhưng không bao giờ được hỗ trợ thực sự tại lớp mạng. Ngoài trở ngại trên, việc chuyển đến các mạng sử dụng các công nghệ khác cũng sẽ là các vấn đề lớn. Tóm lại, truy nhập IP đơn giản chỉ tối ưu cho truy nhập đến các mạng đòi hỏi di động hạn chế hoặc không di động.

3.2.1 Kiến trúc VPN dựa trên IP đơn giản

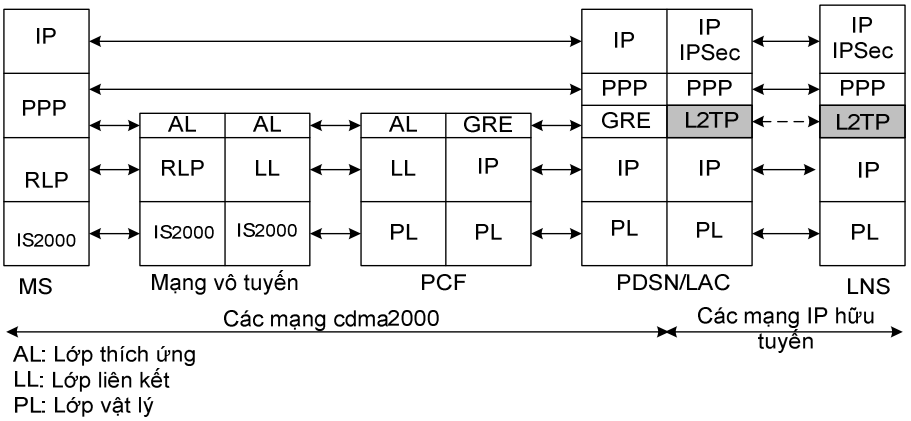
Ta đi xét mô hình kiến trúc IP đơn giản hình 3.1. Giống như các mạng truy nhập từ xa hữu tuyến, phiên PPP do MS khởi xướng được kết cuối bởi NAS (trong trường hợp này NAS được hỗ trợ bởi PDSN) và sau đó được chuyển tiếp qua tunnel đến điểm cuối tunnel phía xa nằm sau firewall trong mạng số liệu riêng. Giao thức truyền L2TP tunnel được khuyến nghị bởi IS 835. Chức năng LAC (L2TP Access Concentrator) do PDSN hỗ trợ sẽ đóng gói phiên PPP của MS và mang nó trên một mạng IP đến LNS (L2TP Network Server) phía xa. Đến lượt mình LNS kết cuối liên kết PPP trong mạng số liệu riêng.



Hình 3.1 Mô hình kiến trúc IP VPN đơn giản

VPN vô tuyến dựa trên IP đơn giản với L2TP khởi đầu từ PDSN được coi là loại truyền tunnel bắt buộc. Liên kết PPP của người sử dụng di động được chuyển tiếp qua một L2TP tunnel đến một LNS ở xa nơi kết cuối liên kết PPP. LNS kết hợp với AAA Server nhà đảm bảo các chức năng xác thực sơ cấp và ấn định địa chỉ, cho phép người quản lý mạng số liệu riêng điều khiển xác thực và ấn định địa chỉ IP cho MS (vì thế nhà khai thác cung cấp dịch vụ mà không cần lo đến các công việc này). PDSN và AAA Server khác liên kết với nó chỉ cần hoàn thiện các đàm phán CHAP để phát hiện địa chỉ của LNS riêng. Khác với MIP, phương pháp truy nhập IP đơn giản không yêu cầu HA (Home Agent) nhưng vẫn dựa trên hạ tầng AAA phân bố dựa trên bộ môi giới (Brocker) để truy nhập AAA Server ở xa liên kết với LNS trong các mạng số liệu riêng. Chi tiết về hệ thống con AAA và các tùy chọn ấn định địa chỉ IP sẽ được xét muộn hơn trong chương này. Nếu dịch vụ VPN không được yêu cầu trong giai đoạn đàm phán IP, PDSN trở thành một phần tử chịu trách nhiệm cho ấn định địa chỉ IP và xác thực người sử dụng.

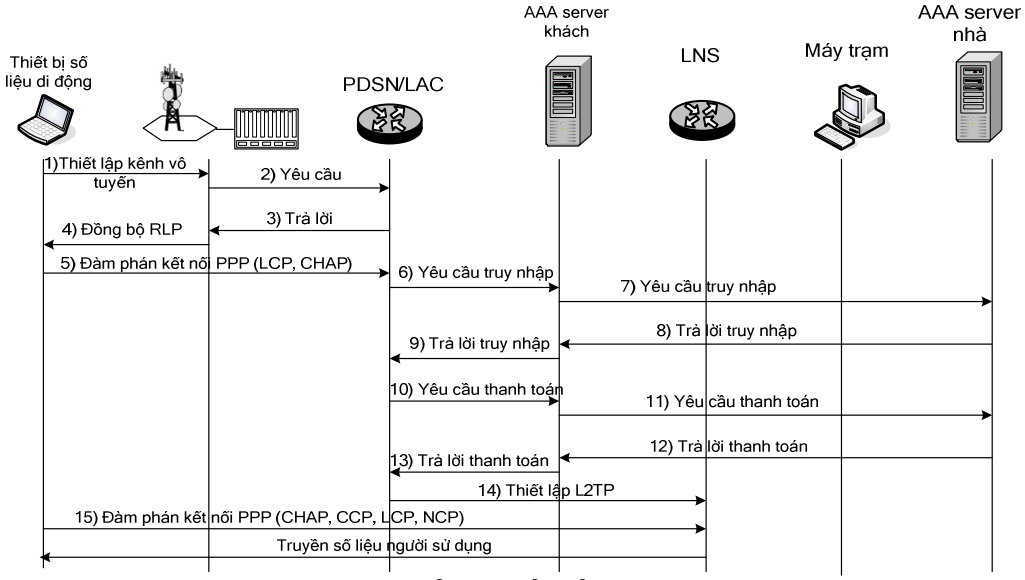
Mô hình giao thức IP VPN đơn giản được cho trên hình 3.2. Trên hình này, L2TP được tăng cường bởi IPSec tùy chọn. Các nhà khai thác vô tuyến thường ưa thích tùy chọn này. Truyền L2TP tunnel là phương thức mềm dẻo, được sử dụng để đảm bảo các dịch vụ đặc biệt như truy nhập từ xa bằng phương tiện của hãng khác, truy nhập IP diện rộng v.v.. đến các đối tác thứ ba: ISP và ASP.



Hình 3.2 Mô hình giao thức IP VPN đơn giản

3.2.2 Kịch bản VPN dựa trên IP đơn giản

Xét chuỗi thiết lập kết nối IP VPN đơn giản mô tả trên hình 3.3. Kịch bản này coi MS được nhập vào mạng nhà, nơi địa chỉ IP ban đầu được ấn định.



Hình 3.3 Thiết lập kết nối IP VPN đơn giản

Tồn tại hai giai đoạn thiết lập kết nối VPN: Giữa MS và PDSN phục vụ và thiết lập phiên L2TP đóng gói lưu lượng PPP giữa chức năng LAC và LNS trong mạng số liệu riêng. Do các nhà cung cấp thiết bị ngày càng có xu thế kết hợp các chức năng của PDSN và LAC trên cùng một nền tảng duy nhất và để đơn giản ta sẽ nói về kết hợp này ở dạng PDSN/LAC trong chương này.

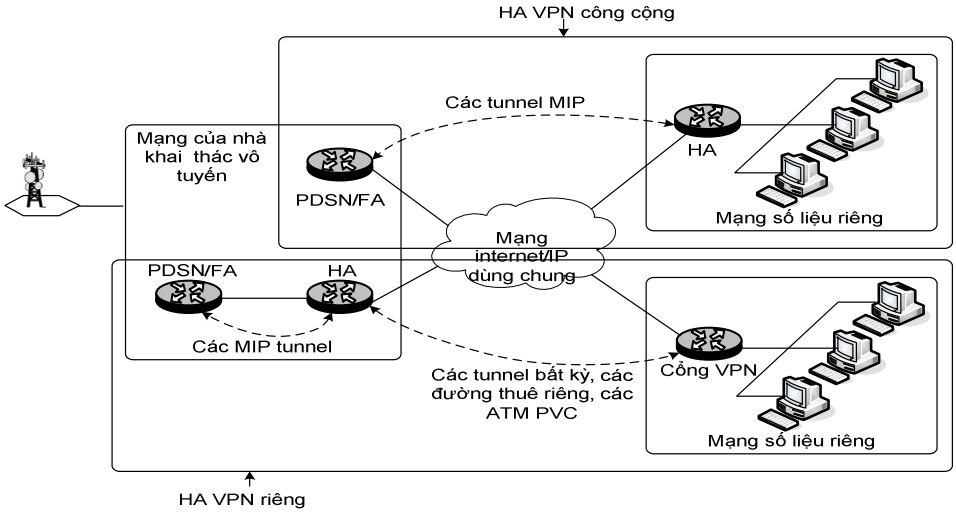
Giai đoạn đầu, đường truyền vô tuyến được thiết lập giữa MS và BSS và sau đó lớp liên kết được thiết lập giữa MS và PCF. Để xác thực người sử dụng, PDSN yêu cầu xác thực đến AAA Server địa phương. AAA Server gửi trả lời xác thực rằng yêu cầu có được tiếp nhận hay không. Bản tin từ AAA Server cũng chứa kiểu tunnel (L2TP) và địa chỉ IP nơi nhận của LNS trong mạng số liệu riêng. Nếu người sử dụng được xác thực đúng, truy nhập mạng số liệu riêng được phép và liên kết PPP được thiết lập.

Trong giai đoạn sau, PDSN/LAC tạo lập một tunel L2TP đến LNS trong mạng số liệu riêng (nếu trước khi sự kiện này xảy ra nó chưa có) để tạo ra một phiên duy nhất cho lưu lượng của người sử dụng. Sau khi đàm phán bằng LCP bổ sung và xác thực, LNS ấn định địa chỉ IP cho MS từ không gian địa chỉ mạng số liệu riêng thông qua RADIUS và DCHP hay các cơ chế ấn định địa chỉ động khác tại giai đoạn thiết lập NCP. Tiếp theo, LNS tách ra các hearder và định tuyến gói tin IP đến máy trạm nơi nhận trong mạng số liệu riêng của nó. Tại hướng ngược lại các gói IP từ máy trạm cần gửi đến MS sẽ đến LNS. Ở đây chúng được đóng gói vào các khung PPP và được gửi đến PDSN/LAC, nơi neo giữ MS thông qua L2TP tunnel. PDSN/LAC loại bỏ hearder của L2TP và chuyển các khung PPP đến MS. IPSec tăng cường bảo vệ an ninh cho các L2TP tunnel bằng ESP. Nếu MS thay đổi vị trí và đến một PDSN khác, cần phải làm lại tòan bộ thủ tục nói trên và các địa chỉ IP mới được ấn định, điều này gây bất tiện cho thuê bao sử dụng dịch vụ MVPN.

3.3 VPN dựa trên MIP

Dịch vụ MIP VPN được tiêu chuẩn hóa bởi TIA/EIA, 3GPP2 và IETF. Nó giải quyết nhiều nhược điểm của giải pháp VPN dựa trên IP đơn giản. Nó duy trì địa chỉ MIP không đổi khi MS di chuyển trong vùng được phục vụ bởi nhiều PDSN. MIP VPN được coi là dịch vụ thực sự di động. Trong các hệ thống CDMA2000, MIP VPN thực hiện theo hai cách: Cách thứ nhất (*HA VPN công cộng từ xa*) coi HA được đặt trong mạng số liệu riêng khác với mạng nhà khai thác và được kết nối với một PDSN đặt trong mạng miền của nhà khai thác thông qua một MIP tunnel thông minh; Cách thứ hai (*HA VPN riêng địa phương*) coi HA được đặt trong cùng

intranet như PDSN và thuộc sở hữu cũng như được bảo trì bởi nhà khai thác vô tuyến. Các dịch vụ VPN trong trường hợp này sẽ được hỗ trợ bởi kết hợp của các MIP tunnel và các tùy chọn (chẳng hạn chuỗi các tunnel khác nhau, các đường thuê riêng hay các ATM PVC). Trong phần tiếp theo ta sẽ xét cả hai phương pháp này.



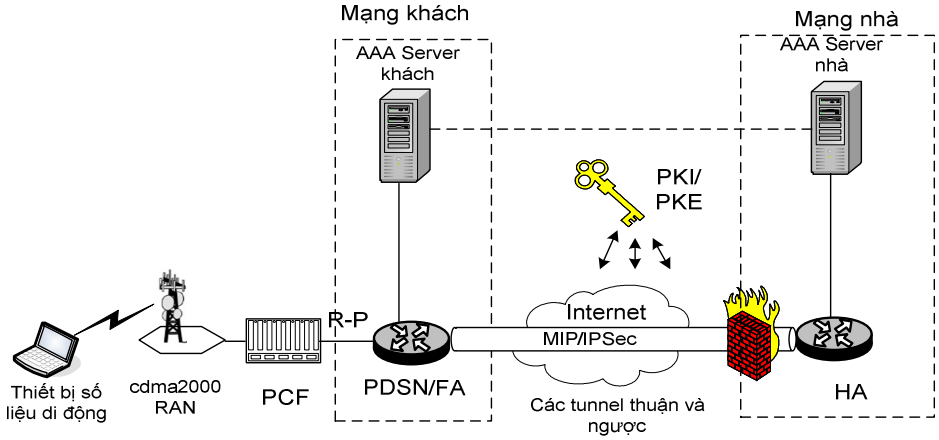
Hình 3.4 Các phương pháp MIP VPN

3.3.1 Phương pháp HA VPN công cộng

Trong phương pháp này tất cả các lưu lượng đường xuống (đến MS) khởi đầu trong mạng số liệu riêng sẽ truyền tunnel đến HA đặt trong mạng số liệu riêng, sau đó đến PDSN nằm trong mạng nhà khai thác vô tuyến. Lưu lượng đường lên (khởi xướng từ MS) được truyền tunnel đến PDSN trong mạng nhà khai thác vô tuyến, sau đó đến HA trong mạng khách hàng. Để như vậy, PDSN thiết lập tunnel ngược tùy chọn [RFC3220]. Cả tunnel thuận và ngược đều dựa trên các giao thức IP trong IP hay GRE và kết hợp với tùy chọn IPSec.

Địa chỉ IP của MS được ấn định từ không gian địa chỉ mạng số liệu riêng, dựa trên sơ đồ đánh địa chỉ IP công cộng hoặc riêng để giảm nhẹ công việc quản lý địa chỉ IP của nhà cung cấp dịch vụ truy nhập vô tuyến (giống VPN dựa trên IP đơn giản). Theo IS835, địa chỉ HA trong mạng số liệu riêng được phát hiện bằng cách sử dụng NAI trong RRQ khi HA được ấn định tĩnh (ấn định HA động sẽ được xét cuối chương này). Trong trường hợp đó, MS phải đăng ký với cả AAA server khách

và nhà và trải qua một thủ tục AAA với sự tham gia của các AAA client trong cả PDSN và HA.



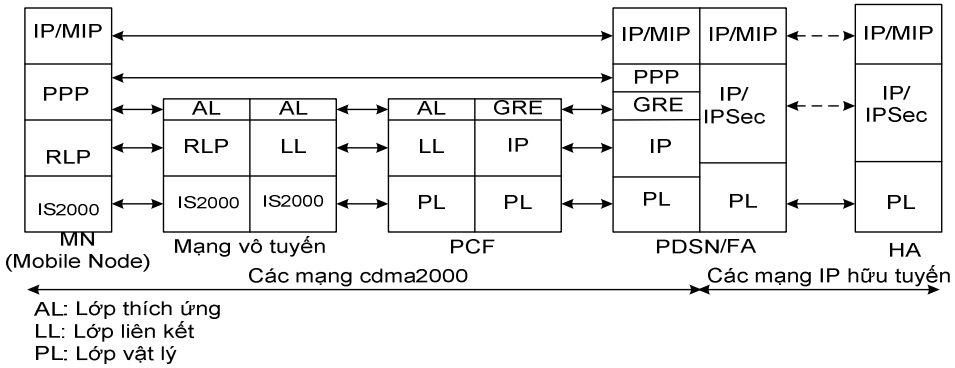
Hình 3.5 Kiến trúc HA VPN công cộng

An ninh VPN của HA công cộng

Các MIP tunnel đến và từ các mạng số liệu riêng (được thiết lập thông qua các mạng IP như Internet) thường không an ninh và đòi hỏi bảo vệ an ninh giống như trường hợp đối với các L2TP tunnel trong trường hợp IP đơn giản. Có thể cung cấp bảo vệ an ninh này bằng IPSec cùng với một cơ chế phân phối các khóa như IKE (Internet Key Exchange). Hình 3.6 cho thấy mô hình tham khảo giao thức cho phương pháp VPN này. HA cần phải kiểm tra nhận dạng PDSN nhà khai thác vô tuyến vì chúng sẽ truy nhập đến số liệu người sử dụng không được bảo vệ trong thời gian phiên. PDSN cũng cần phải kiểm tra nhận dạng của HA để lưu lượng người sử dụng không bị chuyển sai đến một vị trí không an toàn chưa biết trước. Trong trường hợp HA VPN công cộng, HA thuộc sở hữu và được khai thác bởi mạng số liệu riêng, và HA sẽ quản lý cả an ninh và di động của người sử dụng bằng cách tạo ra các liên kết an ninh động với các PDSN phục vụ thay đổi.

Thông thường các nhà khai thác vô tuyến triển khai an ninh IP để truyền thông liên vùng và để bảo vệ báo hiệu MIP. PDSN có thể quyết định áp dụng chính sách nào dựa trên tham số của RADIUS về mức an ninh [IS825]. Trong quá trình thiết lập tunnel an ninh giữa PDSN và HA, IKE được sử dụng kiểm tra nhận dạng của PDSN và HA. Khóa liên kết an ninh có thể là:

- Một số bí mật được lập cấu hình tĩnh cho mở rộng xác thực MIP HA-FA.
- Một số secret shared IKE được lập cấu hình động.
- Một số secret shared IKE động được AAA nhà phân phối.
- PKI với các chứng chỉ.



Hình 3.6 Ngăn xếp giao thức HA VPN công cộng

Theo thứ tự ưu tiên đầu tiên là mở rộng xác thực MIP HA-FA, sau đó là số bí mật IKE tĩnh, rồi đến số *secret shared* được phân phối động và cuối cùng là chứng chỉ PKI. Tiêu chuẩn [IS835] hiện nay chi phối hầu hết các yêu cầu hạ tầng lõi CDMA2000 đòi hỏi cung cấp trước khoá dùng chung MN-HA. Thông tin lập khóa được phân phối trong quá trình đăng ký AAA phải được bảo vệ chống nghe trộm. Bảo vệ này được cung cấp trên từng chặng, chẳng hạn sử dụng IPSec giữa các AAA server khách với phần còn lại của hạ tầng AAA.

Khi sử dụng liên kết khóa *secret shared*, trao đổi giai đoạn đầu được xác thực bằng các mã xác thực bản tin. Sử dụng các *secret shared* đơn giản khi khai thác, tránh được cần thiết xử lý và xác nhận chứng chỉ. Tuy nhiên các liên kết này có thể đưa vào tải bổ sung vì phải thiết lập chúng trong các cặp PDSN-HA. Vì thế, IS835 cung cấp cơ chế cho phân phối *secret shared* động thông qua hạ tầng AAA trong quá trình đăng ký MS. Trong khi AAA mạng nhà xử lý và xác nhận cặp *challenge/response*, nó tạo ra *secret shared* và phân phối bằng trả lời của AAA đến PDSN. PDSN sử dụng bí mật này cùng với một nhận dạng được cấu trúc từ trả lời để thực hiện đàm phán với HA. Điều này cho phép thiết lập IPSec giữa PDSN và HA với cấu hình tự động cho các khóa giữa tất cả các cặp có thể có.

Nếu tunnel ngược được hỗ trợ bởi HA theo chỉ thị của AAA Server trong tham số của RADIUS ở đặc tả tunnel ngược [IS835], IPSec được sử dụng với số liệu truyền tunnel. Các tunnel ngược được thiết lập khi MS thiết lập bit "T" trong yêu cầu đăng ký của nó, các gói gửi đi từ MS được đóng gói và chuyển đến HA bởi PDSN. Các tunnel này cho phép MS sử dụng các địa chỉ riêng không duy nhất, và tùy theo yêu cầu miền nhà các tunnel ngược (cũng như các tunnel thuận) sẽ được bảo vệ bởi IPSec.

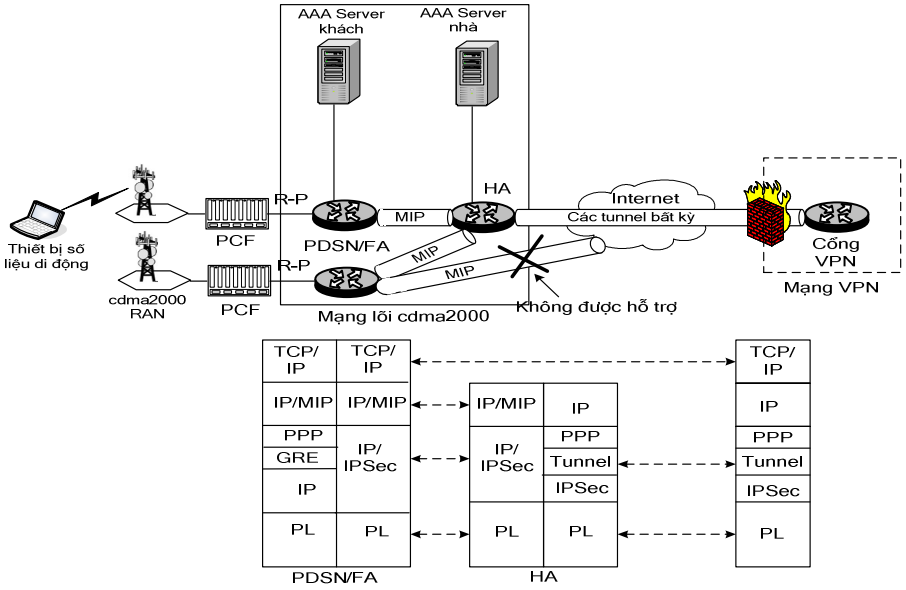
3.3.2 HA VPN riêng

Các nhà khai thác không muốn mở rộng ý tưởng chia sẻ hạ tầng số liệu với phần còn lại của thế giới như mô hình HA VPN công cộng. Điều này có thể đặc biệt gây lúng túng khi một số phần tử hạ tầng như HA thuộc sở hữu phía thứ ba được nối đến mạng lõi của họ qua mạng IP công cộng. Ngoài ra các nhà khai thác không muốn từ bỏ kiểm soát quản lý thuê bao của mình và do dự trở thành chỉ là nhà cung cấp truy nhập số liệu vô tuyến. Các nhà khai thác CDMA2000 đang triển khai tùy chọn HA VPN riêng cũng sở hữu PDSN và các phần tử hạ tầng HA.

Trong khi cần đảm bảo khối lượng lớn dung lượng HA trong mạng nhà khai thác vô tuyến cho công việc không phải VPN, thì việc sử dụng HA của nhà khai thác cho các dịch vụ VPN vẫn chưa được các tiêu chuẩn đề cập và vì thế cần phân tích một cách kỹ lưỡng. Đường truyền số liệu thuê bao CDMA2000 gồm cả PDSN và HA. Lưu lượng số liệu đường xuống phải đi qua HA trong mạng nhà của MS và PDSN phục vụ. Lưu lượng đường lên (từ MS) phải đi qua PDSN chỉ khi MS yêu cầu truy nhập Internet thông thường và qua cặp PDSN/HA được kết nối bởi MIP tunnel ngược nếu MS yêu cầu truy nhập mạng số liệu riêng. Để thỏa mãn các yêu cầu này, các nhà khai thác vô tuyến phải triển khai đủ dung lượng HA để hỗ trợ các MS sử dụng MIP mỗi khi chúng yêu cầu truy nhập mạng số liệu riêng hay chỉ yêu cầu truy nhập Internet thông thường.

Chỉ khi đã có cơ sở hạ tầng HA đủ lớn như vậy, các nhà khai thác vô tuyến muốn điều khiển tối đa việc hỗ trợ thuê bao mới có thể hoàn toàn cấm truy nhập đến các HA trong các mạng số liệu riêng, bằng cách buộc tất cả lưu lượng đến và từ các

mạng số liệu riêng đi qua các HA của mình sau đó chuyển chúng giữa các mạng số liệu riêng thông qua công nghệ khác như hình 3.7. Trong trường hợp này, các mạng số liệu riêng không cần duy trì HA và kết cuối các MIP tunnel. Thay vào đó, nhà khai thác vô tuyến và mạng số liệu riêng phải dựa trên một tập các tunnel (hay các công nghệ khác) móc nối nhau tại HA thuộc sở hữu của mình, kết hợp với các thỏa thuận đồng cấp riêng và các SLA để cung cấp VPN an ninh.



Hình 3.7 Kiến trúc HA VPN riêng và ngăn xếp

Các quy tắc triển khai HA VPN riêng hoàn toàn khác với các quy tắc HA VPN công cộng và dẫn đến một số hệ quả đối với nhà khai thác. HA VPN riêng có thể đơn giản việc ấn định địa chỉ IP cho MS bởi chỉ có một thực thể (nhà khai thác vô tuyến) thực hiện điều khiển thủ tục này. Ngoài ra (ít nhất về mặt lý thuyết) các nhà khai thác này có thể kết hợp quá trình ấn định địa chỉ vào một vị trí: Một tổ hợp HA giả định kết hợp với kho địa chỉ IP và DHCP và AAA server siêu cỡ. Các nhà khai thác vô tuyến vẫn được quyền điều khiển cung cấp cho người sử dụng và cả an ninh lưu lượng báo hiệu lẫn tải tin, vì thế giảm thiểu các nguy hiểm vi phạm an ninh mạng lõi của họ.

Trách nhiệm ấn định địa chỉ IP đặt nhà khai thác CDMA2000 vào tình thế khó xử. Các nhà khai thác phải quyết định có cung cấp cho thuê bao của họ địa chỉ IP công cộng hoặc riêng "không đúng theo cấu hình topo" hay cả hai. Cả hai trường

hợp đều có các vấn đề như nhau. Các địa chỉ IPv4 công cộng quý và số lượng hạn chế. Đánh địa chỉ riêng là cách giải quyết dễ hơn, nhưng cách này sẽ ngăn chặn các thuê bao di động truy nhập các mạng số liệu riêng sử dụng VPN tự nguyên dựa trên truyền tunnel đầu cuối-đầu cuối, vì nó đòi hỏi các địa chỉ IP định tuyến công cộng (trừ khi sử dụng các sơ đồ NAT-T phức tạp và chưa được định nghĩa thích hợp). Trong mọi trường hợp, khách hàng sẽ có cảm giác buộc phải sử dụng HA VPN riêng và kéo theo các thỏa thuận bắt buộc giữa khách hàng và nhà khai thác rằng đây chỉ là tùy chọn cho truy nhập intranet riêng.

Một thách thức quan trọng khác liên quan đến HA VPN riêng là cần tạo lập hạ tầng chuyển mạch tunnel xung quanh HA. Tình trạng này không được đề cập trong các tiêu chuẩn và sẽ đòi hỏi một khung kiến trúc mới liên quan đến các nhà khai thác vô tuyến lẫn khách hàng của họ. Việc tạo khung như vậy không phải là một công việc dễ vì nó liên quan đến các SLA mới, tính cước, các yêu cầu mới đối với các nền tảng HA để hỗ trợ chuyển mạch tunnel, và các công nghệ WAN trên phạm vi nhà khai thác cùng với các nhiệm vụ khác.

Kiến trúc mẫu trên hình 3.7 được triển khai trong chế độ tunnel. Trong kịch bản này, các MIP tunnel đến và đi từ các PDSN phân bố theo lãnh thổ phải kết cuối tại HA riêng trong mạng nhà khai thác và sau đó móc nối với IPSec tunnel được tạo lập cho hãng với giả thiết đã có các quan hệ quy định trước với nhà khai thác. Kịch bản này coi rằng không chỉ ấn định địa chỉ IP mà cả xác thực các MS đều được thực hiện trong mạng nhà khai thác.

3.4 Cấp phát HA trong mạng CDMA2000

Trong phần này ta sẽ xét các phương pháp triển khai HA trong nối mạng lõi CDMA2000 cũng như ảnh hưởng của nó đến kiến trúc và cung cấp MVPN.

3.4.1 Mối quan hệ giữa cấp phát HA và PDSN

Như đã đề cập, PDSN phủ một vùng địa lý nhất định, và PDSN phân biệt rõ phục vụ người sử dụng tại mạng nhà hay chuyển mạng. Trong khi đó HA đại diện cho mạng nhà của MS và phục vụ như một điểm neo cho các phiên số liệu. HA luôn phục vụ một tập người sử dụng được cung cấp dịch vụ không phụ thuộc vào họ

được nối đến mạng nhà hay chuyển mạng. Về mặt này, có hai kịch bản cấp phát HA chính: HA đồng vị trí và HA tập trung.

HA đồng vị trí

Trong kịch bản HA đồng vị trí, sẽ có nhiều vị trí HA trong mạng. Vì lưu lượng người sử dụng MIP (ít nhất trên đường lên) phải đi qua cặp PDSN/HA, các cửa PDSN và HA trong các hệ thống phải rất gần nhau đặc biệt là khi phương pháp HA VPN riêng được thực hiện. Thông thường các chức năng này được hỗ trợ trong cùng một nền tảng, vì thế đặt chúng chung (thành cụm) tại một vị trí địa lý để tiêt kiệm không gian.

Ưu điểm chính của phương pháp này là khả năng thay đổi động các cụm PDSN/HA nếu tỷ lệ khách hàng chuyển mạng và mạng nhà thay đổi. Chẳng hạn trong thời gian triển lãm thương mại lớn tập trung nhiều nhóm lớn người sử dụng di động được ấn định đến các HA phục vụ các vị trí địa lý khác, các PDSN địa phương phải phục vụ nhiều người sử dụng di động hơn thường lệ, nên chúng phải truyền tunnel lưu lượng đến các HA trên toàn thế giới. Để giải quyết tình trạng này, các nhà khai thác triển khai các HA đồng vị trí để dễ dàng thay đổi các cụm PDSN/HA địa phương cho dung lượng PDSN cao hơn. Sau khi sự kiện kết thúc, các cụm thay đổi trở về tỷ lệ thông thường.

Một ưu điểm khác của phương pháp này là đối với các nhà khai thác dự định phục vụ số lượng lớn người sử dụng cố định tại các địa phương khác nhau. Nếu di động trong các mạng này không cao do người sử dụng thường ở lại trong các vùng được phục vụ bởi các HA địa phương, nên các nhà khai thác có thể giảm thiểu mạng đường trục của họ. Các mức tối ưu đường trục cũng đạt được đối với các mạng với chủ yếu là người sử dụng chuyển mạng khi có cấp phát HA động.

Cuối cùng, khi HA đồng vị trí được sử dụng, mỗi cụm PDSN/HA sử dụng hiệu quả hơn khả năng quản lý địa chỉ của mình nhờ việc cấp phát các địa chỉ IP đến các MS từ các kho địa chỉ IP có tại chỗ (trong khi các kho địa chỉ cách biệt có thể dẫn đến kém hiệu suất). Kích cỡ các các PDSN/HA phải đủ để đảm bảo sử dụng tốt cho

trường hợp trung bình. Các địa chỉ riêng và NAT hỗ trợ giải quyết các vấn đề liên quan đến không gian địa chỉ.

HA tập trung

Trong kịch bản này, các HA phục vụ tất cả người sử dụng MIP trong mạng được đặt tại một trung tâm duy nhất. Giải pháp này có một số ưu điểm (khi không có cấp phát HA động), nhất là đối với các nhà khai thác phục vụ người sử dụng mà phần lớn trong số họ thường xuyên di động và thay đổi PDSN và vì thế phải kết cuối trở lại HA gốc của mình. Các trung tâm số liệu HA cho phép dễ dàng quản lý hơn như cung cấp dịch vụ, bảo dưỡng và nâng cấp đối với các nhà khai thác. Ngoài ra vì các tài nguyên dự phòng và các bản lưu làm cho việc khôi phục lại sau thảm họa cũng dễ dàng hơn so với trường hợp HA đồng vị trí. Một ưu điểm khác là khả năng cân bằng tải HA bao gồm toàn bộ dung lượng của các HA trong mạng so với cân bằng tải phạm vi nhỏ trong cụm HA địa phương ở HA đồng vị trí.

Phương pháp HA tập trung dành cho các nhà khai thác muốn tại một vị trí trung tâm quản lý kho địa chỉ IP để gán địa chỉ cho người sử dụng di động trên toàn mạng một cách hiệu quả hơn.

Độ tin cậy HA

Độ tin cậy HA trở lên đặc biệt quan trọng trong mô hình HA tập trung. Một MS được phục vụ bởi một PDSN địa phương bất kỳ. Trong trường hợp sự cố PDSN, MS phản ứng lại biến cố này bằng cách thiết lập lại PDSN với việc phát đi các quảng cáo mời chào cho đến khi một PDSN dự phòng đi vào phục vụ. Cả tunnel tự ý và bắt buộc đều không bị ảnh hưởng của biến cố này, nếu bộ định thời không tích cực và các thông số khác của MS được lập cấu hình đúng. Vì thế sự cố PDSN không phải là một biến cố thảm họa và được giải quyết êm đẹp nhờ các tính chất của MIP.

Các ảnh hưởng của sự cố HA lên MS (cả trong trường hợp HA VPN riêng và công cộng) lớn hơn và có thể gây các hậu quả nghiêm trọng đối với kết nối số liệu của MS. Trong CDMA2000, mỗi MIP MS được lập trình để truy nhập đến một HA đặc thù. Điều này có nghĩa rằng nếu HA chứa địa chỉ IP của một nhóm MS nào đó

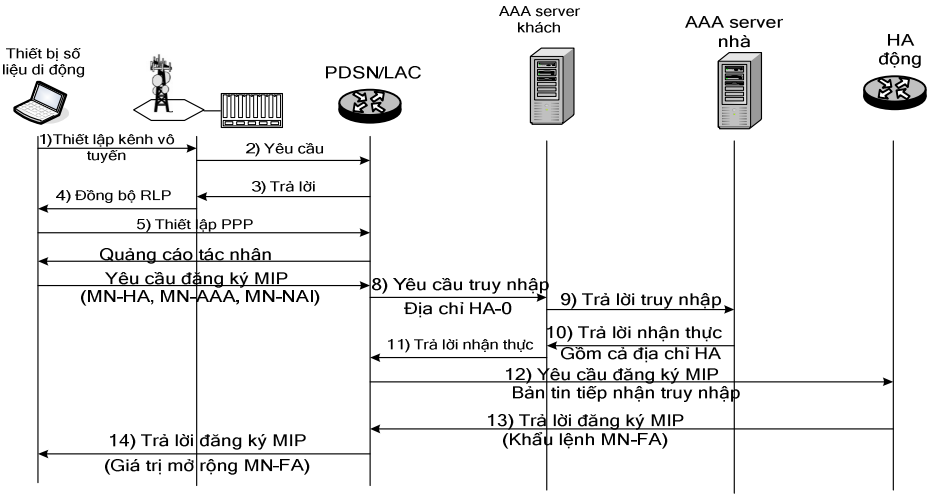
bị sự cố, tất cả các MS liên kết với HA này sẽ không thể nhận được dịch vụ số liệu gói. Để giải quyết tình trạng này, nền tảng HA phải có các tùy chọn giải quyết nhanh sự cố nội bộ, chẳng hạn tự động liên kết các địa chỉ gắn với HA bị sự cố đến phần tử phần cứng khác trong cụm HA tại chỗ.

Các mô hình triển khai HA riêng trong thực tế bao gồm cả hai mô hình cấp phát trên, các nhà khai thác CDMA2000 sẽ có nhiều lựa chọn để cấp phát tài nguyên mạng lõi một cách linh hoạt và động khi các điều kiện kinh doanh thay đổi.

3.4.2 Cấp phát HA động

Các phần trên dựa trên giả thiết rằng HA trong mạng lõi CDMA2000 chỉ có thể được cấp phát tĩnh. Sở dĩ như vậy vì cho đến nay việc tiêu chuẩn hóa cấp phát HA động vẫn chưa hoàn thành. Các nhóm tiêu chuẩn như IETF, 3GPP2 và TIA hiện đang nghiên cứu mở rộng các tiêu chuẩn mạng lõi CDMA2000 bổ sung cho các IETF RFC hiện có bằng cách bổ sung hỗ trợ cấu hình động địa chỉ nhà MS hay bản thân HA.

Trong kiến trúc hiện thời, MS được mã hóa cứng với một địa chỉ của một HA, địa chỉ này có trong yêu cầu đăng ký của nó trong thủ tục đăng ký PDSN. Một HA tĩnh chỉ đơn giản hỗ trợ, vì địa chỉ IP của HA đã được lập cấu hình trong MS và secret shared có thể được sử dụng để mở rộng xác thực MN-HA. Tuy nhiên HA ấn định động đặt cùng PDSN có thể tối ưu hóa khai thác tốt hơn, do tính khả dụng dịch vụ cao hơn và nhiều tuyến tối ưu hơn khi MS di chuyển khá xa mạng nhà dẫn đến chi phí đường trục cao. Chẳng hạn số liệu từ một PDSN tại Hà Nội không cần chuyển đến và đi từ một HA tại TP Hồ Chí Minh mỗi khi người sử dụng muốn đọc một email từ một mail server đặt tại Hải Phòng, nếu có thể ấn định động HA cho một tác tử nhà ở gần. Các tính năng này đòi hỏi tổ chức an ninh phức tạp vì thế quá trình tiêu chuẩn hoá tùy chọn này đòi hỏi thời gian. Điều gì cần có khi hỗ trợ cấp phát HA động an ninh trong mạng lõi CDMA2000. Hình 3.8 (theo dự thảo các tiêu chuẩn hiện nay) cho thấy các bước cần thiết để cấp phát động một HA.



Hình 3.8 Thiết lập HA động

Thiết lập HA động đòi hỏi nghiên cứu khóa secret shared giữa MS và HA để các đăng ký di động tiếp theo được xác thực khi MS thay đổi các PDSN khác. Trong trường hợp cấp phát HA động, địa chỉ HA được xác định bởi một AAA chứ không phải MIP RRQ (Registration Request) như với ấn định HA tĩnh. Một AAA server nhà cấp phát động một HA trong mạng nhà cung cấp dịch vụ hay mạng số liệu riêng ở xa, và trả lời địa chỉ của nó đến AAA server khác và PDSN. Cùng với secret shared, MN-HA được phân bố động cho cả MS và HA để xác thực muộn hơn. Các bí mật này được bảo vệ bằng mật mã hóa bởi mạng AAA quá giang. PDSN sau đó trả lời các giá trị này cho MS và MS bắt đầu sử dụng địa chỉ nhà mới của nó.

Để hỗ trợ cấp phát động một địa chỉ nhà, MS phải cung cấp NAI trong yêu cầu đăng ký MIP của mình. Đây là một tên duy nhất có dạng *user@domain* để nhận dạng người sử dụng yêu cầu dịch vụ từ mạng. Tên này hoạt động như một nhận dạng và không liên kết với địa chỉ IP của thiết bị. NAI cho phép mạng phục vụ tìm kiếm mạng nhà (có thể được đặt trong mạng số liệu riêng) thông qua một hạ tầng AAA, bằng cách sử dụng các mở rộng MIP *Challenge/Response*, "giấy ủy nhiệm" của người sử dụng được xác thực bởi miền nhà. Sau khi người sử dụng được xác thực và được ủy quyền để nhận được dịch vụ trên mạng khách, MS đăng ký với HA (NAI chứ không phải địa chỉ IP nhà xuất hiện trong yêu cầu đăng ký), sau đó HA cấp phát địa chỉ nhà cho MS và gửi trả lời nó trong trả lời đăng ký nhà.

Phiên bản hệ thống tiếp theo sẽ gồm cả tính năng ấn định HA động với phân bố các khóa động từ AAA server nhà đến HA. Phiên bản này giả thiết rằng các HA luôn được cấp phát trong mạng nhà và có liên kết an ninh với AAA server nhà. [IS835] C3 cũng định nghĩa một cơ chế dựa trên RADIUS mới cho HA để yêu cầu RADIUS AAA server nhà cung cấp khóa, sau khi đã cấp phát HA và sau khi nó nhận được yêu cầu đăng ký từ MS. Đối với hoạt động bình thường, MS sẽ hủy đăng ký với HA khi nó chuẩn bị rời mạng số liệu gói CDMA2000. Nếu MS chỉ tạm thời rời và lại xuất hiện tại một PDSN khác, thì MS sẽ buộc phải đàm phán lại PPP và đăng ký lại với HA cũ. Nếu không xảy ra đăng ký lại, thì ràng buộc MIP sẽ tồn tại trên HA cho đến khi hết hạn MIP và các tài nguyên của HA được giải phóng.

3.5 Quản lý địa chỉ IP trong CDMA2000

Phần này xem xét quản lý địa chỉ IP từ cả phía nhà khai thác vô tuyến lẫn mạng số liệu riêng. Khi một MS kết nối đến mạng số liệu riêng trong chế độ IP đơn giản hoặc MIP, nó được ấn định địa chỉ IP riêng từ không gian địa chỉ mạng số liệu riêng. Vì không thể ấn định toàn cầu các địa chỉ như vậy, nên các địa chỉ này không thể định tuyến toàn cầu hay thậm chí duy nhất, và chúng sẽ không gây ra trở ngại đáng kể đối với hãng (mạng số liệu riêng) hay nhà khai thác vô tuyến. Khi đó PDSN phải có khả năng định tuyến các gói đến và đi từ HA ngay cả khi chúng có các địa chỉ riêng chồng lấn. Để thực hiện điều này, PDSN sử dụng địa chỉ HA trong hearder của IP các gói được truyền tunnel và thông tin nhận dạng lớp liên kết ở phía mạng truy nhập (giao diện R-P) của PDSN để giải quyết các xung đột tiềm ẩn trong các địa chỉ được ấn định cho các MS khác nhau.

Trong khi các địa chỉ riêng có thể tiếp nhận được hoàn hảo trong môi trường VPN của CDMA2000, thì các địa chỉ công cộng dành cho MVPN tự nguyện đem lại các lợi ích bổ sung cho các thuê bao sử dụng dịch vụ CDMA2000. Chẳng hạn, bổ sung các mức an ninh khác nhau được cung cấp bởi nhà khai thác vô tuyến cho các khách hàng khác nhau, có yêu cầu đảm bảo an ninh đầu cuối-đầu cuối để bảo vệ các số liệu quan trọng như thông tin mật.

Một cách khác, với các nhà khai thác vô tuyến sử dụng địa chỉ IP riêng trong mạng lõi, NAT là cách cho hiệu quả cao khi các địa chỉ IP công cộng khan hiếm. MVPN tự ý cũng được hỗ trợ (với mức độ khó khăn hơn) khi một trong số các cơ chế NAT-T được thực hiện bởi nhà khai thác.

3.5.1 Ấn định địa chỉ VPN của IP đơn giản

Trong CDMA2000, ấn định địa chỉ IP đơn giản được thực hiện bởi PDSN nếu dịch vụ VPN không được yêu cầu. Khác với MIP, phương pháp truy nhập IP đơn giản không cho phép cung cấp trước địa chỉ IP tĩnh cho MS. Trái lại, địa chỉ IP phải được ấn định động cho MS thông qua một trong các cơ chế ấn định địa chỉ khả dụng, trong thời gian khởi đầu PPP khi MS đầu tiên đăng ký với PDSN và gửi đi một địa chỉ IP 0.0.0.0 trong giai đoạn IPCP để yêu cầu địa chỉ IP động. Lưu ý rằng địa chỉ được ấn định cho MS có thể là một địa chỉ IP riêng hay địa chỉ công cộng.

Các tùy chọn ấn định địa chỉ IP đối với IP đơn giản:

- Ấn định từ kho địa chỉ được lập cấu hình trong PDSN hay trong một cụm PDSN. Không gian này có thể liên kết tĩnh với người sử dụng thông qua bảng chuyển đổi có trong từng PDSN, hay tên của không gian địa chỉ có thể được gửi ngược lại PDSN trong bản tin chấp nhận truy nhập RADIUS (RADIUS Access Accept) bởi AAA server.
- Ấn định thông qua sử dụng AAA server như RADIUS hay DIAMETER khi thực hiện xác thực MS. Giống như trường hợp kho địa chỉ địa phương, địa chỉ từ AAA server được truyền đến client trong quá trình đàm phán PPP.
- Ấn định qua DHCP đòi hỏi hỗ trợ DHCP client trong PDSN.

Khi yêu cầu dịch vụ VPN bắt buộc trong chế độ IP đơn giản, trách nhiệm ấn định địa chỉ IP cho di động được chuyển giao cho mạng số liệu riêng. Trong trường hợp này liên kết PPP được kết cuối và sau đó được đóng gói vào L2TP tunnel và được chuyển đến LNS trong mạng số liệu riêng nơi mà sau đó ấn định địa chỉ được thực hiện.

3.5.2 Ấn định địa chỉ VPN của MIP

Giống như IP đơn giản, quá trình ấn định địa chỉ cho dịch vụ MIP có thể thực hiện bằng nhiều cách. Không giống như IP đơn giản, các MS yêu cầu dịch vụ MIP ấn định địa chỉ IP cố định cho MS, địa chỉ này sẽ được đưa đến PDSN trong quá trình đàm phán PPP (ấn định địa chỉ IP cho dịch vụ MIP nói chung luôn được thực hiện bởi HA). Điều này làm HA (trong cả công cộng lẫn riêng) trở thành phần tử quan trọng nhất trong quá trình ấn định địa chỉ trong MIP VPN.

Sau khi MS được xác thực với PDSN, nó có thể yêu cầu địa chỉ IP tĩnh hoặc động từ HA của nó. HA trả lời địa chỉ IP sẽ được MS sử dụng trong bản tin trả lời đăng ký MIP (MIP Registration Reply) được PDSN chuyển đến MS. Như đã nói ở trên địa chỉ này có thể là định tuyến công cộng hoặc được cung cấp từ không gian địa chỉ riêng theo quyết định của nhà khai thác vô tuyến (trường hợp tùy chọn HA VPN riêng) hay một mạng số liệu riêng (trường hợp tùy chọn HA VPN công). Tiêu chuẩn TIA [IS835] PDSN hỗ trợ nhiều địa chỉ riêng chồng lấn, miễn là các địa chỉ từ các HA đơn lẻ là duy nhất và không chồng lấn. Một tùy chọn hữu ích khác để phân biệt các khả năng ấn định địa chỉ MIP so với IP đơn giản là khả năng hỗ trợ nhiều địa chỉ trong MS để hỗ trợ nhiều phiên thông tin giữa MS và mạng số liệu riêng của nó.

Nếu MS yêu cầu truy nhập đến một địa chỉ nhà riêng, nó phải đàm phán truyền tunnel ngược [RFC2344]. Kết quả PDSN tạo ra một liên kết logic chứa nhận dạng phiên R-P (R-P Session ID), địa chỉ nhà của MS và địa chỉ HA. Khi PDSN nhận được một gói từ HA cho MS đã đăng ký, PDSN chuyển địa chỉ HA của MS và địa chỉ nhà thành một liên kết và truyền gói này đến kết nối R-P được chỉ ra bởi nhận dạng phiên R-P của liên kết.

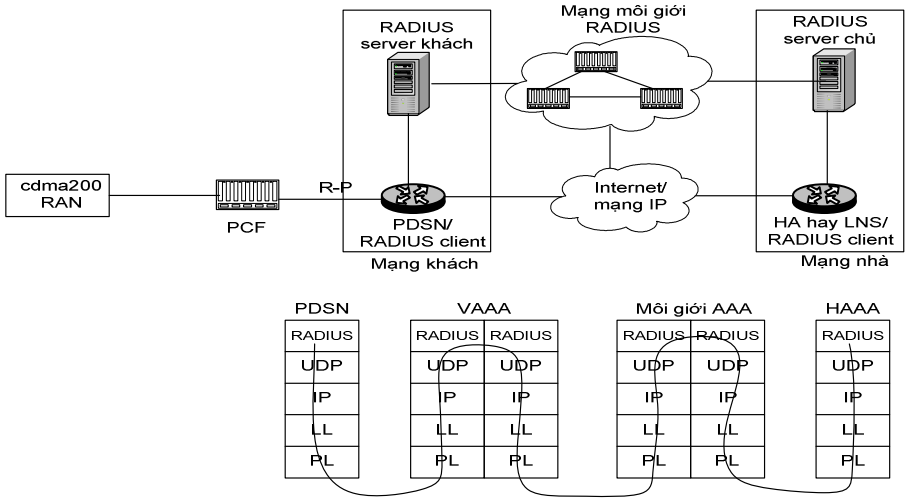
3.6 Xác thực, ủy quyền và kế toán cho dịch vụ MVPN

Cả MIP lẫn L2TP tự mình đều không cung cấp các cơ chế có khả năng thay đổi kích cỡ để điều khiển truy nhập hay kế toán. MIP cơ sở không đặc tả các mở rộng có thể sử dụng để xác thực MS với FA hay FA với HA, nhưng các mở rộng này không bắt buộc và chúng coi rằng đã có các *secret shared* được lập cấu hình trước

giữa các thực thể này. Đây là vấn đề, vì mạng CDMA2000 công cộng toàn cầu sẽ bao gồm nhiều mạng con hay các miền thuộc sở hữu của nhiều hãng, nhà khai thác, ISP hữu tuyến và ASP. Các mạng của nhà khai thác vô tuyến khách hỗ trợ các PDSN sẽ trả tiền cho các dịch vụ số liệu vô tuyến từ MS hay miền nhà của người sử dụng. Để được sự đảm bảo trả tiền, kiến trúc mạng lõi CDMA2000 phải hỗ trợ mạng AAA khả năng định cỡ bao gồm các AAA server cung cấp nhiều dịch vụ được kết nối với nhau chứ không phải một nhóm các AAA server không kết nối cũng như liên lạc với nhau.

3.6.1 Kiến trúc AAA trong CDMA2000

AAA trong môi trường CDMA2000 dựa rất nhiều vào việc sử dụng RADIUS và các giao thức khác như PAP và CHAP. Trong phần này ta sẽ phân tích chi tiết hơn kiến trúc AAA và ảnh hưởng của nó lên MVPN. Để đảm bảo hoạt động AAA bền vững cho truy nhập mạng số liệu riêng, cần mở rộng thêm một bước khái niệm hạ tầng AAA khách-nhà phân bố. Để thỏa mãn tốt hơn yêu cầu đối với các phương pháp truy nhập mạng số liệu riêng khác nhau và giảm nhẹ trao đổi đồng cấp mà không cần thiết lập trước các thỏa thuận, cần phát triển kiến trúc ở dạng kiến trúc AAA khách-môi giới-nhà như thấy ở hình 3.9, giảm nhẹ kiến trúc mạng được chia sẻ bởi nhiều thực thể riêng đồng cấp như ISP, ASP, các mạng hãng và các nhà khai thác di động.



Hình 3.9 Kiến trúc AAA trên CDMA2000 RADIUS và mô hình tham khảo giao thức

MS truy nhập mạng số liệu riêng qua mạng truy nhập do một đối tác thứ ba cung cấp cần được xác thực bởi cả hai mạng. MS sẽ được nhận dạng đối với mạng truy nhập bởi ID của mình (IMSI chẳng hạn), và đối với mạng số liệu riêng bởi NAI. Như hình 3.9, nhận dạng này đòi hỏi chức năng AAA tại cả mạng khách lẫn mạng nhà. Trong CDMA2000, chức năng này được thực hiện bởi RADIUS AAA client (được đặt trong PDSN) và server mạng khách, và RADIUS AAA client (được đặt trong HA đối với MIP và LNS đối với IP VPN đơn giản) và server mạng nhà.

Ngoài xác thực và trao quyền MS trong CDMA2000 khi cần truy nhập mạng số liệu riêng, các yêu cầu xác thực được gửi đi từ AAA server khách liên kết với PDSN đến AAA server nhà liên kết với HA và trả lời ủy quyền được gửi theo phía ngược lại. Thông tin kế toán khi này cũng được lưu trong AAA server khách và tùy chọn được gửi đến AAA nhà bằng cách sử dụng giao thức AAA tin cậy và sau đó được gửi đến hệ thống tính cước. Đối với dịch vụ VPN, thông tin kế toán có thể gồm các thông số: NAI, QoS, nhận dạng phiên đối với dịch vụ IP đơn giản và địa chỉ nơi nhận. Thông tin AAA nhà-khách (được xây dựng trên một cơ chế giao vận tin cậy) có thể được tùy chọn bảo vệ bởi IPSec và có khả năng phân phối secret shared cho IKE.

Mô hình này căn bản như nhau đối với cả IP VPN đơn giản lẫn MIP VPN và có thể bao gồm cả các phần tử tùy chọn như server đại diện RADIUS và các bộ môi giới AAA. Đối với cả hai kiểu VPN này, truyền thông cơ sở giữa các RADIUS client và các server tuân theo [RFC2865] và [RFC2866]. Tùy chọn, truyền thông tin này cũng được đảm bảo an ninh bởi IPSec để cung cấp một liên kết an ninh giữa MS, PDSN và HA (hay LNS trong trường hợp IP đơn giản) và hỗ trợ phân phối khóa động sử dụng IKE.

3.6.2 Môi giới AAA trong CDMA2000

Hạ tầng AAA nhà/khách vừa được trình bày được thiết kế để phục vụ mạng nhà và mạng khách với quan hệ được thiết lập trước qua SLA. Trong các trường hợp các quan hệ này không được thiết lập, nhưng MS khách yêu cầu dịchvụ số liệu, cần sử dụng môi giới AAA. Ta sẽ xét kỹ hơn về môi giới này. Các server nhà và khách có

thể có quan hệ hai chiều trực tiếp. Tuy nhiên kiến trúc TTDĐ có mặt trong hàng nghìn miền với rất nhiều mạng số liệu riêng thuộc sở hữu của các công ty, hãng yêu cầu dịch vụ số liệu vô tuyến cho MS của họ. Nếu số miền nhỏ, các mạng đang phục vụ và mạng nhà có các quan hệ trước (được đảm bảo an ninh qua các liên kết an ninh IP). Tuy nhiên đây không phải là một giải pháp khả thi, nó sẽ đòi hỏi quá nhiều các quan hệ hai chiều được thiết lập trước từng đôi một.

Các bộ môi giới AAA cho phép các yêu cầu AAA được định tuyến dựa trên NAI đến các mạng nhà hay các bộ môi giới khác biết được vị trí của mạng nhà. Các môi giới có vai trò tài chính trong việc thiết lập kế toán giữa các miền và xử lý các bản tin kế toán cho các yêu cầu truy nhập mạng mà chúng cho phép. Do mạng khách sẽ không cung cấp dịch vụ nếu nó không nhận được xác thực từ mạng nhà của người sử dụng di động hay từ một bộ môi giới nhận trách nhiệm tài chính, kiến trúc AAA phải là kiến trúc tin cậy. Điều này có nghĩa là các server phải phát lại các yêu cầu và chuyển mạch sang các server dự phòng khi xảy ra sự cố của khối sơ cấp.

Theo [TSB115], mạng AAA phải hỗ trợ ba chế độ hoạt động của bộ môi giới:

- *Chế độ không trong suốt* (không đại diện): khi bộ môi giới kết cuối các yêu cầu đến và đi từ AAA server khách và nhà, và khởi xướng các yêu cầu mới thay mặt cho chúng. Trong chế độ này, bộ môi giới được phép thay đổi nội dung và các thông số của các bản tin, được sử dụng khi bộ môi giới được phép hoạt động tài chính thay mặt cho các mạng khách.
- *Chế độ trong suốt*: bộ môi giới không được ủy quyền thay đổi bản tin AAA và chỉ được phép chuyển hướng chúng đến các điểm tương ứng nơi nhận.
- *Chế độ chuyển hướng*: trong đó các AAA server giới thiệu nhà cung cấp dịch vụ đến một AAA server khác.

Một nhiệm vụ quan trọng khác của bộ môi giới AAA là giảm nhẹ các dịch vụ chuyển mạng.

3.6.3 Nhìn từ phía MIP VPN

Trong trường hợp MIP VPN, khi MS truy nhập HA trong mạng số liệu riêng, nhà cung cấp truy nhập vô tuyến (người sở hữu PDSN) không được tham gia vào

liên kết an ninh giữa MS và mạng nhà của nó. Đây là yêu cầu mà kiến trúc AAA phải tuân thủ. Bằng thông số mức an ninh TIA trong bản tin tiếp nhận truy nhập, AAA server nhà ủy quyền PDSN trên cơ sở từng người sử dụng để tùy chọn sử dụng IPSec trên các bản tin đăng ký và số liệu truyền tunnel.

Nếu AAA server nhà chỉ ra rằng cần sử dụng liên kết IP an ninh giữa PDSN và HA, PDSN sẽ cung cấp các dịch vụ IPSec theo [IS835] dựa trên mức an ninh được định nghĩa bởi 3GPP2. Nếu không có liên kết an ninh nào, PDSN sẽ tìm cách thiết lập liên kết an ninh bằng cách sử dụng chứng chỉ HA X.509. Nếu không tồn tại chứng chỉ X.509, nhưng chứng chỉ gốc tồn tại, PDSN tìm cách thiết lập liên kết an ninh mà nó nhận được trong giai đoạn một IKE, PDSN tìm cách sử dụng secret shared phân bố động nhận được trong bản tin chấp nhận truy nhập. Nếu không *secret shared* nào được gửi, PDSN tìm cách sử dụng *secret shared* thiết lập trước được lập cấu hình tĩnh, nếu có. Nếu PDSN không nhận được thông số mức an ninh 3GPP2 từ RADIUS server nhà, nó tiếp tục sử dụng liên kết an ninh cũ. Nếu không tồn tại liên kết an ninh, PDSN sẽ tuân theo chính sách an ninh được lập cấu hình tại chỗ.

3.6.4 Nhìn từ phía VPN IP đơn giản

Đối với chế độ truy nhập IP VPN đơn giản, kiến trúc AAA không chứa HA. Trái lại hoạt động của nó được hỗ trợ bởi LNS, như đã trình bày trước đây. AAA server phải định vị được LNS cung cấp truy nhập đến mạng nhà người sử dụng. Vì thế các AAA server đại diện trong các mạng nhà cung cấp dịch vụ liên quan phải được thiết lập để định vị LNS. Sau khi LNS được xác định vị trí, L2TP tunnel được thiết lập giữa LNS và PDSN (nơi mà MS yêu cầu dịch vụ). Địa chỉ IP của MS được ấn định bởi LNS sau khi tunnel được thiết lập. Vì MS không tham gia vào các quyết định định tuyến giữa các điểm cuối tunnel, các địa chỉ có đăng ký lẫn không đăng ký đều có thể được ấn định cho MS. AAA server khách ghi lại bản ghi kế toán và gửi bản tin yêu cầu kế toán đến AAA server nhà nếu xảy ra chuyển mạng.

Chuỗi các sự kiện AAA xảy ra khi khởi đầu mạng số liệu riêng IP đơn giản: Khi một MS (sử dụng phương pháp IP đơn giản) khởi đầu kết nối đến PDSN, PDSN tạo

ra một bản tin yêu cầu truy nhập và gửi nó đến AAA server nhà để xác thực. Yêu cầu được xác thực thành công và bản tin chấp thuận truy nhập chứa kiểu truyền tunnel "L2TP" được gửi ngược trở lại đến AAA server khách. PDSN khởi đầu L2TP tunnel nếu nó chưa được thiết lập và gửi bản tin yêu cầu kế toán (Accounting Request) cho mục đích tính cước để ghi lại thời điểm bắt đầu dịch vụ. Khi dịch vụ không còn được yêu cầu nữa, phiên người sử dụng L2TP và tunnel kết thúc. Cuối cùng PDSN gửi bản tin yêu cầu kế toán khác để ghi lại thời gian dừng dịch vụ.

3.7 Kịch bản triển khai

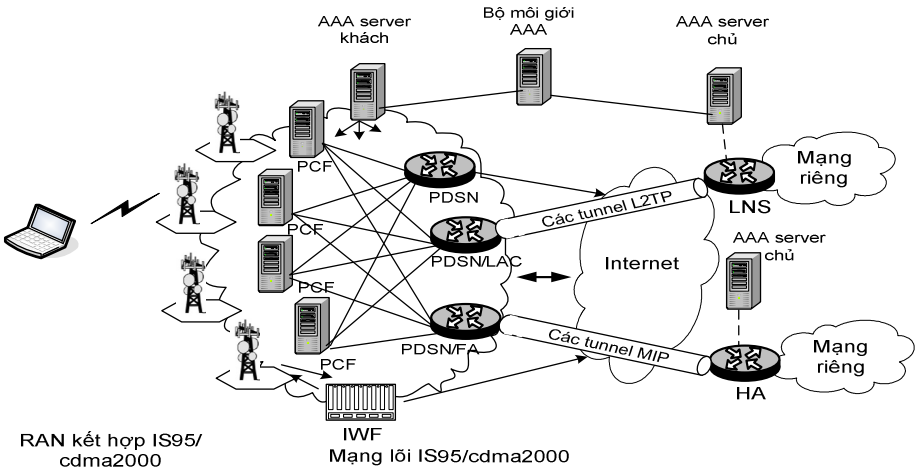
Về mặt lịch sử, CDMA phát triển theo các quy tắc khác với GSM và CDMA2000 có mức độ khác biệt lớn hơn đối với UMTS mặc dù các giao diện vô tuyến của chúng liên quan mật thiết với nhau. Vùng phủ CDMA2000 vẫn tập trung ở Bắc Mỹ và Đông **Á**. Cho đến nay, CDMA chủ yếu thống trị bởi một số ít các hãng khai thác rất lớn cùng với một số các hãng nhỏ tập trung lên các thị trường nhỏ và các vùng nông thôn. Trong phần này ta sẽ phân tích một mạng CDMA2000 (kết hợp với mạng IS-95) được thành lập tại Mỹ bởi một hãng lớn, gọi là hãng USA.

Nhà khai thác này được cung cấp tài chính tốt và cố gắng cung cấp cho các khách hàng Bắc Mỹ nhiều dịch vụ giống như hoặc thậm chí vượt trội các dịch vụ được đồng nghiệp của mình cung cấp tại châu Âu. Chẳng hạn hiệu suất tần số của giao diện vô tuyến CDMA2000 có thể cao hơn GSM GPRS và băng thông đủ lớn đảm bảo cung cấp cho người sử dụng số liệu các dịch vụ tiên tiến hơn. Trong khi các nhà khai thác GPRS, đặc biệt là ở các trung tâm thành phố như London, phải vật lộn để cung cấp cho các khách hàng nhiều khe thời gian thì vấn đề này được giải quyết dễ dàng hơn với mạng vô tuyến trải phổ hiệu suất cao CDMA2000.

Hãng USA đã cung cấp dịch vụ số liệu kênh một số năm. Mạng số liệu lõi của nó dựa trên các IWF tập trung tại sáu trung tâm số liệu và phủ đồng đều địa lý nước Mỹ, các trung tâm này chứa các server ứng dụng và thiết bị khác. Mặc dù mạng đã triển khai toàn quốc ngay từ đầu, nhưng tốc độ không đáp ứng mong đợi dẫn đến lợi nhuận thấp, bảo dưỡng nối mạng số liệu kém và chi phí hỗ trợ cũng như giảm tốc độ mở rộng được quy hoạch ban đầu. Vì thế tất cả các IWF được tập trung trong

một vị trí để giảm các chi phí bảo dưỡng. Một trong số các tính năng mới là "Quick VPN" nhằm vào các người sử dụng kinh doanh dựa trên kiến trúc Quick Net Connect được đề nghị bởi nhà sản xuất IWF cho phép truy nhập nhanh mạng số liệu riêng bằng cách sử dụng truyền tunnel L2TP đến mạng số liệu riêng thay cho thủ tục quay số modem truyền thống.

Hãng USA gần đây quyết định nâng cấp mạng lên CDMA2000 với triển khai lúc đầu dịch vụ gói thí điểm toàn quốc. Theo kế hoạch này, các trung tâm số liệu hiện có sẽ được sử dụng để chứa các PDSN và HA cho dịch vụ internet thông thường (hình 3.10). Để nâng cấp thành công thiết bị vô tuyến cần nâng cấp cả phần mềm lẫn phần cứng. Các MSC phải được tăng cường các PCF được thực hiện trên một nền tảng cách biệt và phải lắp đặt các PDSN và HA. Các cán bộ kỹ thuật và tiếp thị của hãng USA thực hiện đánh giá toàn diện IP đơn giản so với MIP và kết luận rằng trước hết nên triển khai IP đơn giản cùng với chiến dịch tiếp thị tập trung lên MIP vì dịch vụ này sẽ được đưa vào sau một thời gian ngắn. Lý do là vì chưa có các máy cầm tay có khả năng MIP và chưa chín muồi các MIP client cho cả hệ điều hành Windows lẫn Linux. Phân tích cũng cho thấy rằng mạng truy nhập IP đơn giản được thiết kế và cung cấp bởi nhà cung cấp thiết bị được chọn gần giống như MIP.



Hình 3.10 Mạng lõi kết hợp IS95/CDMA2000 của ACME USA

Giải pháp được nhà cung cấp đưa ra để giải quyết các hạn chế của IP đơn giản bao gồm một mạng hỗn hợp các PCF và các PDSN, mạng này sẽ cho phép các thuê bao IP đơn giản giữ nguyên kết nối đến cùng một PDSN ngay cả khi các PCF phục

vụ thay đổi. Điều này sẽ đảm bảo rằng các địa chỉ ấn định cho các máy di động giữ nguyên không đổi trong thời gian phiên để cho phép truyền tunnel tự ý và các ứng dụng nhậy cảm địa chỉ IP khác. Cùng với mạng số liệu gói, nhà khai thác triển khai một mạng AAA phân bố và quyết định đặt dịch vụ môi giới AAA ở một trong các trung tâm số liệu của mình. Nhà khai thác cũng dự định khởi đầu tiếp thị dịch vụ môi giới đến các nhà khai thác khác đồng thời với việc triển khai dịch vụ MIP.

Hãng USA quyết định hỗ trợ một sơ đồ đánh địa chỉ IP công cộng và riêng kết hợp để giảm nhẹ việc đa dạng hóa cung cấp các dịch vụ IP tiên tiến bao gồm cả dịch vụ MIP VPN sắp tới.

Nhận thức được tính phức tạp và sự chưa chín muồi của thị trường MIP VPN, hãng USA quyết định thử nghiệm thị trường với nhiều tùy chọn VPN gồm cả các dịch vụ tự ý và bắt buộc. Đề nghị dịch vụ của hãng USA cho người sử dụng VPN bắt buộc bao gồm cả địa chỉ IP định tuyến công cộng kết hợp với các đảm bảo mức dịch vụ, các tùy chọn quản lý băng thông và các mức an ninh khác nhau. Dịch vụ IPSec tùy chọn cũng sẵn sàng và được tiếp thị cho các khách hàng kinh doanh ở dạng một bộ phận của dịch vụ tạo nguồn truy nhập vô tuyến ở xa. Chương trình CPE (Customer Premise Equipment) cho các khách hàng VPN tự ý bao gồm IPSec và các client phần mềm PPTP kết hợp với hỗ trợ và các dịch vụ định vị.

Dịch vụ VPN bắt buộc cũng được đề nghị trong một gói hấp dẫn kết hợp các dịch vụ chủ và đại diện, ấn định địa chỉ bởi hãng khác và chương trình CPE mở rộng (các phần cứng và phần mềm) cho các xí nghiệp bao gồm các LNS, các cổng IPSec và thiết bị HA (cho dịch vụ MIP sẽ triển khai sắp tới). Một tùy chọn IPSec được cung cấp cùng với firewall và quản lý băng thông loại gói giá cao dành cho các hãng lớn và các cơ quan nhà nước. Cả hai dịch vụ IP đơn giản và MIP VPN đều được cung cấp trong dạng tiêu chuẩn và dựa trên truyền tunnel L2TP và MIP, môi giới RADIUS AAA và các SLA thử nghiệm với các khách hàng cao cấp.

Chương 4 Giải pháp VPN trên GSM/GPRS và UMTS

Cả hai hệ thống GSM/GPRS và UMTS cung cấp các khả năng số liệu gói. Hệ thống GSM trước đây được thiết kế và tối ưu hóa hỗ trợ dịch vụ thoại và số liệu kênh. GPRS được thiết kế nhằm mục đích tăng cường khả năng số liệu gói cho hệ thống GSM. Vì thế hệ thống GPRS không cung cấp truyền dẫn tối ưu hay các dịch vụ số liệu có hiệu năng và thông lượng cao. UMTS được thiết kế ngay từ đầu để hỗ trợ các dịch vụ gói số liệu thông qua miền gói PS của mình, nên có hiệu năng và tốc độ số liệu cao hơn GPRS. Chương trước đã trình bày các khả năng dịch vụ số liệu gói của GPRS và miền UMTS PS. Các khác biệt về dịch vụ VPN giữa hệ thống GPRS và UMTS hầu như không đáng kể với hầu hết các trường hợp. Một số ngoại lệ là:

- Một số tính năng mới được đưa vào các tiêu chuẩn 3GPP R99 không có trong các hệ thống GPRS R99, như: Nhiều mức QoS trên mỗi phiên số liệu.
- Chuyển tiếp DHCP tại GGSN và MIP FA được hỗ trợ tại GGSN.

Các tính năng này mở rộng đáng kể dải dịch vụ của các nhà cung cấp dịch vụ và chúng sẽ là chung cho cả hệ thống GPRS và UMTS từ R99 trở đi. Tuy nhiên sau các dịch vụ số liệu gói R99, các mạng sẽ không được tập trung quanh GSM/GPRS và vì thế các khả năng này sẽ phổ biến hơn ở các hệ thống UMTS (trừ việc triển khai EDGE). Vì các lý do trên, chương này sẽ chỉ nói về các VPN chung của GPRS và miền UMTS PS.

4.1 Các giải pháp công nghệ số liệu gói

Trước hết ta tập trung vào nút hỗ trợ GPRS phục vụ GGSN (Serving GPRS Support Node). GGSN được đặt giữa mạng vô tuyến và các mạng hữu tuyến giao tiếp với nó. GGSN là chung cho cả các hệ thống GPRS và UMTS, và là phần tử mạng quan trọng đảm bảo các dịch vụ số liệu tiên tiến như MVPN. HLR (Home Location Register), hệ thống AAA, các SGSN, lý lịch người sử dụng và các hệ thống con quản lý quan hệ khách hàng là các phần tử quan trọng trong cung cấp các dịch vụ IP. Nhưng "trí tuệ" của các dịch vụ IP được tập trung tại GGSN, và đây là điểm xử lý các gói của người sử dụng tại lớp mạng và ở các lớp cao hơn. GGSN là

phần tử mạng kết cuối các GTP tunnel. GTP tunnel được thiết lập từ SGSN. SGSN định vị người sử dụng khi họ di chuyển trong mạng truy nhập vô tuyến. GGSN cung cấp các điểm truy nhập đến các mạng số liệu gói. Mỗi điểm truy nhập được nhận dạng thông qua một tên logic hay APN (Access Point Name). Khuôn dạng của APN được đặc tả trong [3GPP TS23.003]. Tại thời điểm thiết lập phiên, SGSN phân giải APN thông qua DNS thành địa chỉ IP (hay một danh sách các địa chỉ IP) trực thuộc một hay nhiều GGSN để cung cấp điểm truy nhập mong muốn. Thực chất, để đảm bảo tính khả dụng dịch vụ, để có thể định cỡ hay chia sẻ tải, cần cho phép phân bố một điểm truy nhập dịch vụ trên nhiều GGSN. Điều này dẫn đến việc chọn lựa địa chỉ IP sử dụng để thiết lập GTP tunnel. Giải thuật chọn địa chỉ IP từ một danh sách địa chỉ IP phân giải bởi DNS do nhà cung cấp quyết định. Nó có thể đơn giản là quay tròn hay "chọn IP đầu tiên trong danh sách và duyệt danh sách thay cho việc cố gắng sử dụng lại địa chỉ khi không có trả lời từ GGSN".

Thiết lập GPRS tunnel là chìa khoá để cung cấp các dịch vụ VPN, dưới đây ta sẽ giải thích kỹ quá trình này. Bản tin đầu tiên được sử dụng để thiết lập GTP tunnel chứa các thông tin sau:

- Chứa nhận dạng người sử dụng nhận được từ IMSI và MSISDN ([3GPP TS23.003] định nghĩa IMSI và MSISDN).
- Mang hai thông tin quan trọng: nhận dạng mạng NI (Network Identifier) của APN và chế độ chọn (Selection Mode).

Có thể xác thực người sử dụng dựa trên IMSI hay MSISDN. Khi chuyển IMSI hay MSISDN và APN đến AAA server, AAA server sẽ kiểm tra thông tin nhận dạng đến từ môi trường vô tuyến này có đáng tin cậy hay không. Là một bộ phận của quá trình này, GGSN thu nhận thông tin lý lịch của người sử dụng trong các bản tin trả lời nhận được từ hệ thống con AAA. Sau đó thông tin này có thể được sử dụng tại GGSN để nhận các tham số và chính sách liên quan đến dịch vụ từ các cơ sở dữ liệu bên ngoài như các danh mục của LDAP và COPS, để có thể thực hiện các chính sách phù hợp với người sử dụng.

NI (Network Identifier) của APN được sử dụng tại GGSN để liên kết phiên với một mạng ngoài tương ứng và quyết định: phương pháp xác thực người sử dụng,

giao thức sẽ được sử dụng (IPv4, IPv6 hay PPP), và có cần thiết xử lý phiên PPP tại GGSN hay không, hay chỉ đơn giản chuyển tiếp đến một LNS qua một L2TP tunnel (GGSN sẽ hoạt động như một LAC). Cũng như vậy, cách thức xử lý gói, chính sách, địa chỉ IP của server bên ngoài, thông tin cấu hình máy trạm và các thông tin khác có thể được liên kết với APN. Vì thế một GGSN mạnh cho phép lập cấu hình một khối lượng thông tin đáng kể trên một APN để quyết định cách xử lý các phiên đến cho từng nhu cầu của APN. Có nhiều phương pháp chọn dịch vụ và lập cấu hình như lấy thông tin cấu hình từ miền mà đặc tả người sử dụng gộp cùng với tên của người sử dụng tại thời điểm đăng nhập. Ta sẽ xét các vấn đề này muộn hơn trong chương này.

Phần tử thông tin về chế độ chọn (Selection Mode) được mang trong yêu cầu tạo lập ngữ cảnh PDP (Create PDP Context) sẽ quyết định cách truyền phiên người sử dụng đến một điểm truy nhập đặc thù, nghĩa là mạng (SGSN) cho phép người sử dụng sử dụng APN theo tiêu chí nào. Thực ra, APN có thể do MS đặc tả hoặc mạng đặc tả (mặc định SGSN đặc tả APN), hay là một bộ phận của lý lịch đăng ký thuê bao và được tạo ra bởi MS hay bởi mạng.

Dựa trên thu nhận thông tin APN và tra cứu thông tin xử lý phiên được lập cấu hình cho APN, các dịch vụ truy nhập mạng khác nhau có thể được cung cấp tại GGSN. Các dịch vụ này có thể được phân loại thành:

- Kiểu IP PDP.
    - Simple IP (IP đơn giản).
    - IP với các tùy chọn cấu hình giao thức (IP PCO).
- Kiểu PPP PDP (bắt đầu có từ R98).
    - Chuyển tiếp PPP.
    - PPP kết cuối tại GGSN.

Trong các tiêu chuẩn, *truy nhập trong suốt* được định nghĩa khi GGSN không tham gia vào xác thực người sử dụng. GGSN không yêu cầu truy vấn đến server ngoài để xác thực người sử dụng, và xác thực người sử dụng cho truy nhập mạng chỉ đơn giản dựa trên xác thực mạng truy nhập vô tuyến. Xác thực mạng truy nhập

vô tuyến chỉ thực hiện khi người sử dụng đăng nhập PMM (Packet Mobility Management) tại SGSN, hay người sử dụng thay đổi SGSN khi di chuyển (dựa trên sự tin tưởng vào thông tin nhận được từ SGSN cũ hay dựa trên sự xác thực lại của MS tại SGSN mới). Phương pháp truy nhập này thuộc về chế độ IP đơn giản. Trong chế độ truy nhập IP đơn giản, các server ngoài có thể được sử dụng và GGSN vẫn có thể tham ra vào xác thực người sử dụng.

Chỉ có thẻ SIM (hay USIM) trong MS được xác thực chứ không phải người sử dụng SIM (PIN). PIN trên MS đảm bảo nhận dạng người sử dụng tại mức người sử dụng. Mạng ngoài (mạng khách) không thể xác thực người sử dụng thông qua sử dụng PIN xác thực truy nhập vô tuyến. Vì thế mạng ngoài cung cấp dịch vụ truy nhập trong suốt dựa trên quan hệ tin cậy với nhà khai thác di động.

Trong các tiêu chuẩn, *truy nhập không trong suốt* đề cập đến tất cả các phương pháp truy nhập khác khi GGSN tham gia vào xác thực người sử dụng. Tuy nhiên vẫn còn nhiều vấn đề không rõ ràng liên quan đến thế nào là trong suốt và không trong suốt. Thực chất, PPP Relay trên các L2TP tunnel có vẻ theo phân loại là truy nhập không trong suốt, tuy nhiên xác thực người sử dụng được thực hiện tại LNS không đặt tại GGSN. Vì thế, theo định nghĩa, đây là chế độ truy nhập trong suốt.

4.2 Dịch vụ truy cập mạng kiểu IP PDP

Kiểu IP PDP cho phép cung cấp các dịch vụ truy nhập mạng IP cho cả IPv4 và IPv6 bằng cách cung cấp kết nối lớp IP và các dịch vụ cho MS. Chương này chỉ duy nhất xét IPv4, vì trong một vài năm tới nó vẫn sẽ là xu thế cung cấp các dịch vụ truy nhập mạng doanh nghiệp và các dịch vụ IP tiên tiến.

Các giải pháp dựa trên loại PDP này bao gồm các cách khác nhau cho phép cấp địa chỉ IP, lập cấu hình máy trạm, và kết nối lớp thấp hơn đến mạng IP. Giá trị phần nhận dạng mạng của APN (NI) được gửi đến GGSN trong yêu cầu *Create PDP context* (tạo lập ngữ cảnh PDP) sẽ quyết định tổ hợp nào trong các khối cơ sở của dịch vụ nói trên cho các phiên dựa trên cấu hình của GGSN. Ngoài ra, có thể cung cấp thông tin khác tại GGSN trên cơ sở ANP-NI như chặng tiếp theo cho gói đường

lên, giúp định tuyến các gói đến các nơi nhận phù hợp trên cơ sở APN (trong trường hợp một ISP hay mạng khác liên kết với các APN khác nhau).

Kiểu IP đơn giản

Một APN được lập cấu hình cho chế độ truy nhập kiểu chế độ IP đơn giản đảm bảo các kiểu dịch vụ sau:

- Kết nối dựa trên lớp 2 (ATM, MPLS, Frame Relay, PPP,…) hay trên tunnel (chế độ IPSec tunnel, IP/IP, GRE,…) đến mạng ngoài.
- Khả năng giao tiếp với server AAA để thực hiện xác thực IMSI hay MSISDN hay ấn định địa chỉ IP dựa trên RADIUS.
- Sử dụng RADIUS accounting (kế toán Radius) để thông tin các sự kiện liên quan đến phiên cho các server kế toán hay các server ứng dụng.
- Ấn định địa chỉ IP tĩnh hoặc động.
- Tích cực PDP context khởi tạo bởi mạng

Khi PDP context khởi tạo bởi mạng được hỗ trợ, địa chỉ IP cần được liên kết cố định với IMSI của MS. Địa chỉ IP này được cấp từ các dải địa chỉ cục bộ tại GGSN hay RADIUS hay DHCP client, và sau đó địa chỉ này được thông báo cho MS trong IE địa chỉ người sử dụng đầu cuối của trả lời GTP Create PDP context và các bản tin chấp nhận kích hoạt PDP Context của RIL3 [3GPP TS24.008].

Hạn chế lớn nhất của chế độ truy nhập này là mô hình tin cậy của nó. Trong mô hình này mạng ngoài hoàn toàn dựa vào mạng vô tuyến để đảm bảo xác thực người sử dụng. Không có cả mật khẩu lẫn xác thực hai yếu tố (bí mật do con người đảm bảo cộng với mã do thẻ tạo ra tại một thời điểm) để ngăn chặn người nào đó biết được bí mật của đầu cuối (tình cờ hoặc dụng ý xấu), và rồi có thể truy nhập mạng liên kết với APN. Vì thế chế độ này thích hợp nhất để cung cấp truy nhập đến các ứng dụng và các dịch vụ không yêu cầu xác thực người sử dụng.

Mặt khác chế độ truy nhập này thích hợp nhất cho các dịch vụ đòi hỏi tương tác tối thiểu giữa người sử dụng và đầu cuối để thiết lập kết nối. Nếu kết hợp với sử dụng xác thực và kế toán RADIUS, chế độ này cũng có thể được sử dụng để đảm bảo ký giao kèo đơn lẻ bằng cách truyền thông tin liên quan đến phiên cho một lớp truy nhập các dịch vụ có nhiệm vụ phân phối nhận dạng người sử dụng và địa chỉ IP

được dùng để sắp đặt các ứng dụng. Thực chất, lớp truy nhập dịch vụ có thể "biết" cách chuyển đổi địa chỉ IP thành IMSI hay MSISDN thông qua ấn định địa chỉ IP dựa trên RADIUS hay quá trình báo cáo về chuyển đổi địa chỉ IP vào nhận dạng người sử dụng (IMSI hay MSISDN) thông qua các bản tin kế toán của RADIUS. Hiện nay quá trình chuyển đổi địa chỉ IP vào ID của người sử dụng chủ yếu được sử dụng trong các cổng WAP hay HTTP proxy để cung cấp các tính năng tính cước và quy định nội dung tiên tiến.

Bình thường, IP đơn giản sẽ được sử dụng cho các ứng dụng trình duyệt dựa trên Web hoặc WAP. Khả năng ứng dụng khác của chế độ truy nhập mạng này là VPN đầu cuối-đầu cuối, nghĩa là truy nhập mạng từ xa dựa trên client. Tuy nhiên nó đòi hỏi các địa chỉ IP công cộng. Mới đây, đề xuất IPSec NAT traversals (NAT-T) với IETF sử dụng các địa chỉ riêng cho hoạt động chế độ IPSec tunnel, nhờ vậy giảm bớt áp lực phải sử dụng các địa chỉ IP công cộng.

Trong IP đơn giản, nếu thuộc tính của chế độ chọn (Selection Mode) được thiết lập giá trị 0, phần tử thông tin IE (Information Element) của chế độ chọn trong yêu cầu Create PDP context sẽ cung cấp cho GGSN bằng chứng về quyền truy nhập APN của thuê bao. Điều này có nghĩa là "MS hay mạng đã được cung cấp APN, đăng ký đã được kiểm tra". Tất nhiên nếu sự tín nhiệm về thông tin này là nền tảng cơ bản cho hoạt động của dịch vụ, thì cần bảo vệ báo hiệu GTP bằng các biện pháp an ninh để bảo toàn tính toàn vẹn. Một cách khác, GGSN truy vấn AAA server bằng *RADIUS Access Accept,* loan báo MSISDN của người sử dụng hay IMSI RADIUS 3GPP VSA ([3GPP TS29.061]), để thực hiện xác thực người sử dụng dựa trên thông tin tin cậy IMSI hay MSISDN do mạng cung cấp. Trong trường hợp này, tên và mật khẩu người sử dụng trong *Access Request* phải được chứa trong một số giá trị giả. Ngoài ra cũng cần bảo vệ thông tin về IMSI hay MSISDN mang trong báo hiệu GTP, để có thể bảo toàn tính toàn vẹn của nó (nếu cần cả tính bảo mật của nó). Thông thường điều này đạt được bằng cách sử dụng GTP được bảo vệ bởi IPSec.

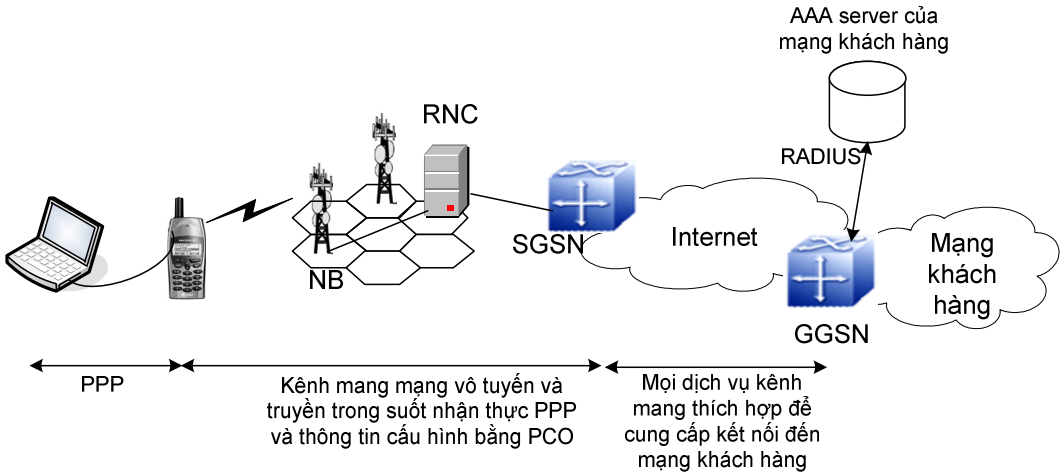
Với IP đơn giản, lập cấu hình host không mạnh như các giải pháp khác. Người sử dụng phải lập cấu hình bằng tay cho MS (hoặc bằng một số công cụ phần mềm

trang bị cùng với thuê bao trên CD-ROM) địa chỉ IP của các NetBIOS (Network Basic Input-Output System) server hay các server DNS.

Tóm lại chế độ truy nhập này phù hợp cho các đầu cuối đơn giản, truy nhập đến các ứng dụng có thể giải quyết vấn đề xác thực người sử dụng chặt chẽ theo cách thức độc lập với xác thực truy nhập mạng.

IP với các tùy chọn cấu hình giao thức (PCO)

Hình 4.1 mô tả kiến trúc IP với truy nhập PCO (Protocol Configuration Options).



Hình 4.1 Kiến trúc IP với chế độ truy nhập dựa trên PCO

Bản tin Create *PDP context* có thể chứa PCO IE (Information Element - phần tử thông tin). IE này chứa cấu hình máy trạm và thông tin xác thực trong suốt được trao đổi giữa các phần tử TE (Terminal Equipment) và MT (Mobile Terminal) của MS. TE có thể sẽ là máy tính để bàn hay một thiết bị khác giao tiếp với MT qua liên kết dựa trên PPP. Giai đoạn xác thực PPP dựa trên PAP (Password Authentication Protocol) hay CHAP (Challenge Handshake Authentication Protocol). MT luôn luôn xác thực thành công TE, thu thập tư liệu xác thực từ TE và chuyển vào giai đoạn IPCP (Internet Protocol Control Protocol). Tư liệu xác thực này và yêu cầu lập cấu hình IPCP sau đó được đặt vào PCO IE trong yêu cầu *Activate PDP context* gửi đến SGSN, sau đó yêu cầu này lại được gửi tiếp đến GGSN trong bản tin yêu cầu *Create PDP Context*. GGSN sử dụng thông tin này để xác thực MS. Sau khi MS được xác thực, GGSN quyết định nên gửi thông tin cấu hình máy trạm nào đến MS

(bao gồm địa chỉ IP cho MS, địa chỉ IP của server DNS sơ cấp hoặc thứ cấp hay địa chỉ IP của server tên của NetBIOS sơ hoặc thứ cấp) bằng cách sử dụng một PCO IE trong trả lời *Create PDP context*.

Chế độ truy nhập dựa trên kiểu IP PDP cho phép hai lớp cùng mức kết nối theo tunnel đến mạng liên kết với APN như trong trường hợp IP đơn giản. Nó bổ sung thêm khả năng thực hiện xác thực người sử dụng đối với truy nhập mạng dựa trên *secret shared* giữa thực thể quản lý mạng ngoài và người sử dụng đầu cuối, vì thế cho phép mức an ninh chặt chẽ hơn chế độ IP đơn giản. Điểm yếu duy nhất trong mô hình này là hacker có ý đồ xấu có thể tìm ra cặp *challenge/response* được gửi trong PCO IE và sau đó sử dụng lại nó để truy nhập mạng. Thực chất, chế độ truy nhập mạng này không cho phép GGSN (hay hệ thống AAA) tạo ra challenge đối với MS, vì thế không bị các tấn công kiểu phát lại xảy ra, và đây không phải là một việc đơn giản cho hacker khi mạng được thiết kế tốt.

Trong [RFC2486], khái niệm NAI (Network Access Identifier) được đưa ra để định nghĩa tên người sử dụng với khuôn dạng "user@domain". IP với chế độ truy nhập PCO cho phép sử dụng GGSN trong một mạng khách, cung cấp khả năng chuyển mạng mức AAA (như iPass và GRIC là các ISP cung cấp truy nhập Internet toàn cầu dựa trên thỏa thuận chuyển mạng với ISP nước khác). Ngoài ra bằng cách thay đổi phần tử miền, nhiều nền tảng dịch vụ IP thông minh có thể được cấu hình trả về:

- Tên của dịch vụ cho thuộc tính ID bộ lọc hay các thuộc tính RADIUS khác,
- Các chính sách truy nhập mạng, nhận được từ một LDAP hay kho lưu số liệu cấu hình về các chính sách dịch vụ tương đương.

Các chính sách dịch vụ khác nhau cho phép GGSN định lại tuyến các gói đến các mạng khác nhau tùy thuộc vào phần tử miền của tên người sử dụng, rồi cho phép thuê bao chọn mạng đặc thù và dịch vụ mà mạng cung cấp dựa trên giá trị này.

Bằng cách bổ sung thêm thuộc tính "3GPP-GGSN-MCC-MNC" RADIUS Vendor-Specific ([3GPP TS29.061]) cho các bản tin RADIUS, khi một GGSN trong mạng khách sử dụng AAA server nhà, ta có thể áp dụng các chính sách phụ thuộc mạng khách. Hệ thống con AAA cũng có thể khởi động các ứng dụng trong

mạng nhà để gửi đến MS nội dung push đặc tả mạng khách, như tin tức hay cảnh báo trong mạng khách. AAA server trong mạng nhà có thể lệnh cho các push server trong mạng nhà khởi tạo các phiên push với MS bằng cách sử dụng địa chỉ có trong *Accouting Request START* (bắt đầu yêu cầu kế toán) nhận được từ GGSN. Một cách khác, nếu GGSN nằm trong mạng nhà, một chức năng tương đương sẽ được cung cấp bằng cách sử dụng thuộc tính "3GPP-SGSN-IP address" RADIUS 3GPP Vendor-Specific để xác định xem hiện người sử dụng đang tại mạng nhà hay chuyển mạng. Bằng cách tra cứu DNS ngược cũng có thể nhận được thông tin bổ sung và nhận dạng nhà cung cấp hiện thời hay xác định thông tin vị trí địa lý.

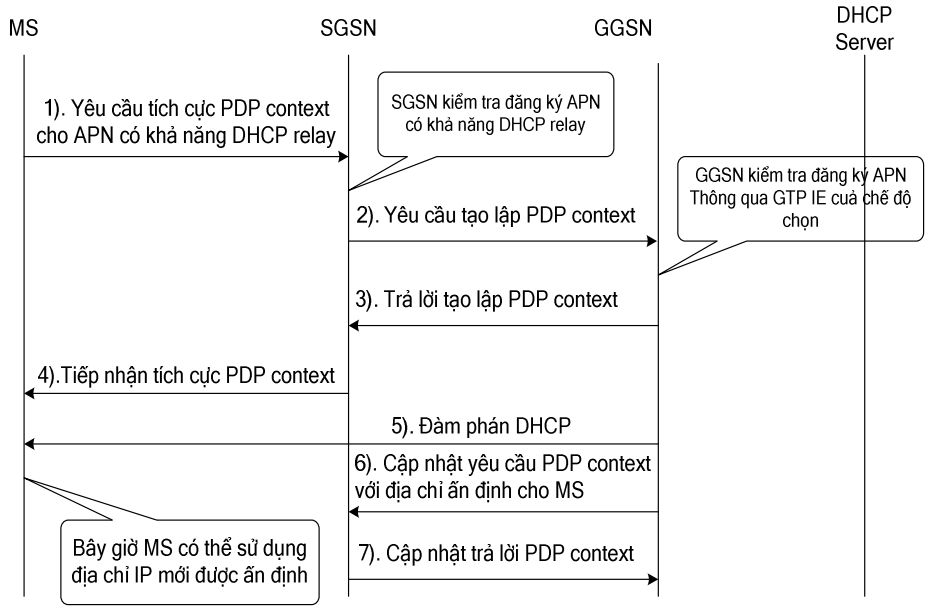
Chuyển tiếp DHCP và MIPv4

3GPP R99 đã tăng cường các đặc tả GPRS, cho phép lập cấu hình APN hỗ trợ dịch vụ chuyển tiếp DHCP (DHCP Relay) hay chức năng FA (Foreign Agent) của MIP. Hình sau mô tả kịch bản phương pháp truy nhập DHCP Relay điển hình.

Khi một yêu cầu Create PDP context được phát đến GGSN để lập cấu hình APN nhằm hỗ trợ DHCP hay MIP FA, một trả lời *Create PDP context* được gửi ngược lại SGSN ngay lập tức mà không có bất cứ xác thực người sử dụng nào khác với ở chế độ truy nhập IP đơn giản. Trả lời này định nghĩa một GTP tunnel và một kênh mang đến một MS mà không có bất cứ địa chỉ IP của MS nào liên kết với nó. Tunnel này có thể được sử dụng để trao đổi các bản tin cấu hình DHCP hay các bản tin quảng cáo và các đăng ký MIP. Sau đó MS sẽ được ấn định một địa chỉ IP bằng cách sử dụng DCHP hay các phương pháp MIP (Mobile IP). Truy nhập mạng từ xa sẽ nhận được bằng cách sử dụng các phương pháp đóng gói gói bởi MIP, hay bằng cách sử dụng lớp liên kết và các công nghệ truyền tunnel được định nghĩa cho IP đơn giản khi DHCP đã được lập cấu hình.

Chế độ truy nhập DHCP Relay được sử dụng khi các phương pháp lập cấu hình máy trạm và khi chế độ truy nhập "giống LAN" được yêu cầu. Chế độ truy nhập giống LAN đặc biệt thích hợp cho các thiết bị vô tuyến đòi hỏi phát hiện nhiều thông tin liên quan đến dịch vụ như HTTP hay địa chỉ SIP proxy IP. Nói chung, xác thực người sử dụng trong phương pháp này cũng gặp phải các nhược điểm giống

như trong chế độ IP đơn giản. Tuy nhiên ở đây xác thực người sử dụng được tăng cường bằng cách sử dụng xác thực DHCP [RFC3118].



Hình 4.2 DHCPv4 trong các hệ thống GPRS

Chế độ truy nhập MIPv4 cũng phù hợp cho chế độ truy nhập giống LAN, vì nó hỗ trợ suôn sẻ chuyển giao giữa GPRS/UMTS và các công nghệ truy nhập khác như WLAN. Các mạng GPRS/UMTS/WLAN kết hợp dựa trên MIP có thể dược triển khai rộng rãi trong tương lai, sau khi đã giải quyết các vấn đề tiêu chuẩn và an ninh và khi xuất hiện các thiết bị người sử dụng có khả năng và cho phép tương hợp.

4.3 Dịch vụ truy cập mạng kiểu PPP PDP

Kiểu PPP PDP được bổ sung cho GPRS bắt đầu từ R98. Đây là một bổ sung rất quan trọng cho các khả năng mà hệ thống GPRS cung cấp vì nó cho phép thích ứng tốt hơn cơ sở đã được thiết lập của hạ tầng truy nhập mạng hữu tuyến chủ yếu dựa trên PPP. Nó cũng giải quyết các yếu điểm của thực thi CHAP dựa trên IP với chế độ truy nhập PCO (các tùy chọn cấu hình giao thức) như đã trình bày ở trên. PPP PDP cho phép sử dụng mật mã PPP và nén PPP, cũng như sử dụng các giao thức lớp mạng khác ngoài IP. PPP cũng định nghĩa EAP (Extensible Authentication Protocol - [RFC2284]) cho phép đàm phán LCP để kết cuối mà không cần xác định giao thức xác thực, giao thức này trong suốt đối với NAS và chỉ được xác định tại

giai đoạn xác thực. Điều này cho phép phát triển các giao thức xác thực mà không cần thay đổi NAS và hạ tầng AAA. Nó cũng cho phép sử dụng các giải thuật xác thực tiên tiến sẽ được phát triển trong tương lai (như các thẻ thông minh,..), không sử dụng lại PAP và CHAP làm phương pháp xác thực.

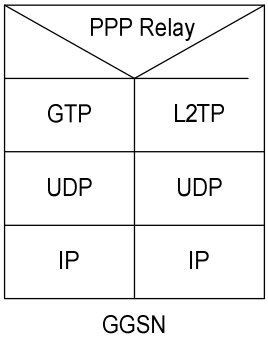
PPP định kỳ kiểm tra tính khả dụng của liên kết đầu cuối-đầu cuối bằng cách sử dụng bản tin *echo request/*response (yêu cầu/đáp ứng hồi âm) của LCP. Điều này có thể dẫn đến một loạt vấn đề liên quan đến cấp phát các đường truyền vô tuyến thậm chí cả khi không cần truyền số liệu hữu ích. Cả GGSN và MT đều có các thông tin tính khả dụng về các kênh mang GPRS/UMTS. Vì thế cả hai thực thể đều tránh chuyển tiếp các yêu cầu LCP echo (hồi âm LCP) và vì thế tự trả lời các yêu cầu echo. Trong trường hợp chuyển tiếp PPP (PPP Relay), cả hai GGSN và MT sẽ hoạt động như các đại diện bản tin LCP echo (GGSN tới các NAS ngoài, MT tới TE). Khi PPP kết cuối tại GGSN, GGSN sẽ không phát các yêu cầu LCP echo và MT phải hoạt động như một LCP proxy. Thiết lập này đảm bảo hiệu năng tối ưu của kiểu PPP PDP dựa trên MVPN và nó không thể hiện bất cứ hạn chế thực tế nào trong việc phát hiện trạng thái liên kết.

Một số các thực hiện MVPN client, như các VPN client dựa trên L2TP và các IPSec VPN client, thường trao đổi các bản tin *keep-alive* với cổng VPN. Trong trường hợp này mạng không điều khiển chúng cũng như không hoạt động như là một proxy để tránh sử dụng không hiệu quả các tài nguyên vô tuyến. Vì thế điều này có thể ảnh hưởng tiêu cực đến sử dụng các tài nguyên vô tuyến và người sử dụng phải trả cước nhiều hơn một cách không mong muốn. Ngoài ra, kiểu PPP PDP dựa trên giải pháp LCP proxy sẽ cho phép kênh mang đầu cuối-đầu cuối được thiết lập chừng nào kênh mang vô tuyến còn được thiết lập, trong khi một liên kết VPN client-VPN cổng có thể bị xóa thậm chí cả khi kênh mang vô tuyến không có (chẳng hạn vì các bản tin *keep-alive* VPN tunnel bị mất trên vô tuyến). Vì các khiếm khuyết này và các một số khiếm khuyết khác, nên các giải pháp đầu cuối-đầu cuối dựa trên VPN client thường có thể không tối ưu trong môi trường TTDĐ, cả nhìn từ phía nhà khai thác lẫn thuê bao. Vì thế giải pháp MVPN bắt buộc có khả năng thành công cao hơn trong môi trường TTDĐ.

Lợi ích bổ sung của kiểu PPP PDP dựa trên MVPN là ở trường hợp chuyển tiếp PPP, nhà cung cấp dịch vụ có thể cho phép nhà quản lý mạng số liệu riêng thực hiện quản lý địa chỉ và AAA, nhờ vậy giảm thiểu ảnh hưởng lên quản lý mạng vô tuyến và sự phức tạp. Mặt khác các nhà khai thác, có thể cung cấp phương tiện cho dịch vụ này và cũng hợp nhất trên một nền tảng chung kết cuối các L2TP tunnel từ cả CSD và truy nhập dựa trên PS và thậm chí cả truy nhập quay số, băng rộng và WLAN.

Chuyển tiếp PPP

Trong kiểu truy nhập PPP PDP có thể lập cấu hình một APN để chuyển tiếp các khung PPP đến một thiết bị NAS bên ngòai. Công nghệ thực tế được sử dụng trong trường hợp này là L2TP. L2TP có thể được chuyển tiếp trên Frame Relay, ATM và UDP/IP. APN tại GGSN phải được lập cấu hình bằng địa chỉ L2 (Frame Relay hay ATM) hay địa chỉ IP của LNS cùng với tên của tunnel L2TP và mật khẩu. Thông tin liên kết với APN để xác định khung PPP của mạng từ xa này sẽ được chuyển tiếp, vì thế chỉ cần GGSN thiết lập tunnel và các cuộc gọi L2TP trong tunnel. Đây là một quá trình thiết lập đơn giản và có thể đảm bảo đủ mức an ninh đầu cuối-đầu cuối khi các L2TP tunnel được đảm bảo an ninh bằng chế độ giao vận IPSec và mật mã PPP được đàm phán. Ngoài ra trong kịch bản này GGSN có thể hoạt động như một LCP echo Proxy. Hình 4.3 cho thấy ngăn xếp giao thức liên quan đến cấu hình PPP Relay sử dụng L2TP giao vận trên UDP/IP.



Hình 4.3 PPP Relay sử dụng L2TP

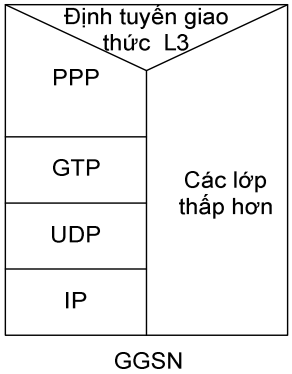
GGSN thiết lập trong suốt các cuộc gọi đến LNS được lập cấu hình cho PPP Relay APN, và khuyến cáo gộp APN vào trong tập nội dung thông tin *PDP context*

lưu trong HLR. Theo cách này, IE của chế độ chọn trong yêu cầu *Create PDP context* được thiết lập giá trị "0" hay APN, hay còn gọi "MS hay mạng đã cung cấp APN, đã được đăng ký, đã được kiểm tra", và các thuê bao không xác thực được mà cố gắng thiết lập L2TP tunnel sẽ bị từ chối ngay khi thực hiện thiết lập L2TP. Tính năng này hỗ trợ bảo vệ chống lại các tấn công DoS (Từ chối phục vụ). Ngoài ra cặp giá trị thuộc tính số chủ gọi L2TP AVP (Attribute-Value Pair) sẽ được thiết lập tới MSISDN của MS. Khi đó LNS có thể được lập cấu hình từ chối các cuộc gọi vào từ các số chủ gọi không thuộc tập danh sách các số cho phép quy định trước. Nhà quản lý LNS có thể sử dụng tùy chọn này để phát hiện MSISDN của người sử dụng tìm cách truy nhập LNS trái phép khi cần thiết để đảm bảo an ninh. Ngoài ra việc gửi AVP cần thiết để LNS chuyển tiếp thông tin MSISDN đến hệ thống con AAA hay đến các cổng WAP thông qua giao diện dựa trên RADIUS (ở đây thuộc tính RADIUS được sử dụng là Calling Station ID: Nhận dạng trạm chủ gọi).

PPP kết cuối tại GGSN

Phương pháp truy nhập PPP kết cuối tại GGSN bổ sung thêm các tính năng xác thực và lập cấu hình máy trạm dựa trên PPP để được một biến thể truy nhập mạng rất linh hoạt cho một loạt các dịch vụ IP tiên tiến. Chẳng hạn khi người sử dụng đã được xác thực, AAA server gửi trở lại người sử dụng tên của dịch vụ sẽ được cung cấp (đã được trình bày trong phần trước, "IP với PCO") hay có thể gửi đến một LNS thông tin cần thiết cho các khung PPP của tunnel. GGSN cũng hỗ trợ nén PPP (thường là LZC và MPPC) để nâng cao hiệu suất sử dụng giao diện vô tuyến.

Trên cùng một nền tảng GGSN được sử dụng để kết cuối các GTP tunnel kiểu PPP PDP thường có thể kết cuối/khởi tạo các tunnel L2TP, vì thế có thể liên kết nhiều công nghệ truy nhập cả hữu tuyến lẫn vô tuyến. Hình 4.4 minh họa các ngăn xếp giao thức cụ thể được hỗ trợ bởi PPP kết cuối GGSN.



Hình 4.4 PPP kết cuối tại GGSN

Khi so sánh giữa các chế độ truy nhập PPP kết cuối tại GGSN và IP PCO sẽ cho ta hiểu được các điểm yếu và mạnh của từng phương pháp. Chế độ PPP kết cuối tại GGSN thân thiện hơn đối với hoạt động của giao thức GTP, vì trong trường hợp này có thể thiết lập GTP tunnel ngay lập tức mà không cần GGSN đợi hoàn thành các quá trình AAA người sử dụng và cấu hình, và có thể thiết lập L2TP tunnel khi các thuộc tính tunnel được gửi trả lời trong bản tin RADIUS Acccess Accept.

Trong một số thực thi GGSN, có thể cấu hình GGSN để thiết lập ngay tức thì cuộc gọi L2TP khi bản tin Create PDP context kiểu IP PDP là bản tin cho APN chế độ truy nhập "IP với PCO" đặc thù. Tuy nhiên thiết lập này sẽ tạo nên một sử dụng L2TP không tiêu chuẩn và làm cho phiên đầu cuối-đầu cuối dễ bị tổn thương do các tấn công kiểu replay-based tác động lên chế độ IP PCO. Việc thiết lập L2TP và quá trình AAA đối người sử dụng đòi hỏi nhiều thời gian dẫn đến khó khăn cho các bộ xử lý giao thức GTP tại SGSN. Về nguyên tắc, nhà khai thác có thể điều chỉnh các bộ định thời GTP và các phát lại các yêu cầu tạo lập PDP context để đảm bảo trễ liên kết với "IP với PCO" trong quá trình thiết lập các tunnel. Nhưng nói chung đây không phải là biện pháp an toàn và cũng không đủ đảm bảo cam kết SLA (thỏa thuận mức dịch vụ) khi người sử dụng chuyển sang các mạng không sử dụng cùng phương pháp điều chỉnh tương tự cho các tham số GTP.

Như vậy, giải pháp này giải quyết được việc thiếu các đầu cuối GPRS có khả năng hỗ trợ PPP, trong khi vẫn đảm bảo tính linh hoạt của dịch vụ bằng phương pháp khác. Cuối cùng, kiểu PPP PDP cho phép sử dụng và đàm phán các giao thức

nén PPP (như STAC LZC và MPPC) mà IP không thể cho phép. Điều này làm cho vấn đề chi phí bổ sung bởi PPP (2 byte trên gói) không còn đáng kể nữa.

Tóm lại, IP với PCO bị kiểu PPP PDP kết cuối tại GGSN vượt trội, nhưng nó sẽ tồn tại một thời gian nữa ít nhất là cho đến khi hỗ trợ kiểu PPP PDP trong các đầu cuối sẽ phổ biến.

4.4 Các thỏa thuận mức dịch vụ (Service Level Agreements)

Các SLA được định nghĩa bởi các nhà cung cấp dịch vụ UMTS MVPN cho khách hàng, nó bao gồm cả các sắp đặt kinh doanh, điều khoản pháp lý và tài chính, không liên quan đến công nghệ. Thông thường, các SLA chứa các số liệu về sự khả dụng, mất gói trên một loại dịch vụ, các chính sách thay thế các khối bị hỏng trong mạng của khác hàng nếu nhà khai thác cũng cung cấp cả các thiết bị đặt tại khách hàng, sửa chữa hỗ trợ bộ phận trợ giúp cho các nhà quản lý, đào tạo kỹ thuật cho các người quản lý, thông tin đánh địa chỉ IP và phạm vi các biến này mà khách hàng có thể điều khiển từ xa.

Các cam kết khả dụng và hỗ trợ được thỏa thuận trong SLA có thể được biểu thị ở thuật ngữ MTBF (Mean Time Between Failure), MTTR (Mean Time to Repair) và khả năng nhận được sự hỗ trợ kỹ thuật hay sự sẵn sàng của các linh kiện dự phòng để thay thế cho các cấu kiện bị hỏng. Chẳng hạn, có thể có các cước phí khác nhau được áp dụng tùy thuộc vào việc đảm bản hỗ trợ thường xuyên hay hạn chế.

Các mức đảm bảo QoS cũng là một bộ phận của SLA, cùng với một thỏa thuận điều kiện lưu lượng theo mô hình DiffServ bao gồm cả: một lý lịch lưu lượng mà khách hàng phải tuân thủ và các quy tắc kiểm sóat và lưu ý mà nhà cung cấp dịch vụ thi hành tại biên với mạng khách hàng cho lưu lượng tuân thủ và không tuân thủ lý lịch lưu lượng. SLA cũng đặc tả cách thức mà IPSec thiết lập các tính năng an ninh và bảo mật, như:

- Các giải thuật mật mã và xác thực hearder bản tin nào sẽ được sử dụng.
- Lập cấu hình nhân công hay hạ tầng PKI được sử dụng để phân phối các khóa xác thực.
- Chế độ giao vận hay tunnel được sử dụng.

- Các chính sách IPSec cụ thể.
- Các địa chỉ IP của các cổng an ninh.

Các tiêu chuẩn quản lý mật khẩu cho các L2TP tunnel cũng có trong SLA. Trong phần liên quan đến các thông số-an ninh này của SLA, cần trình bày quá trình xử lý các lý lịch của thuê bao và số liệu. Ngoài ra quan hệ tin tưởng giữa khách hàng và nhà cung cấp thường phụ thuộc vào các điều khỏan rất đặc thù và các đảm bảo sẽ được trình bày trong phần này.

Các phương pháp thiết lập tài khoản và đăng ký dịch vụ cho các thuê bao liên kết với mạng khách hàng phải là một bộ phận của thoả thuận. Nhà cung cấp dịch vụ có thể cung cấp một trang Web đăng ký dịch vụ cho mục đích này. Kiểu thông tin xác thực thuê bao mà khách hàng có thể yêu cầu về sửa chữa, hỗ trợ hay quyền lợi đối với dịch vụ chăm sóc khách hàng cũng phải có và cách xử lý số liệu đòi hỏi riêng tư và bảo mật cũng cần được đề cập.

Các đặc tả khác của SLA bao gồm:

- Phương pháp truy nhập AAA server (qua đại diện hay truy nhập trực tiếp hay mạng môi giới) cũng như thông tin đánh địa chỉ cho các server chứa thông tin cấu hình máy trạm và các phương pháp truy nhập mạng được phép (IP vớp PCO, PPP Relay, PPP kết cuối), cùng với tính khả dụng, an ninh và các thuộc tính bản tin AAA cần thiết để cung cấp dịch vụ.
- Số liệu tính cước và các phương pháp trả tiền, tài liệu số liệu về sự sử dụng và các vấn đề khác về tính cước và tài chính.
- Tính khả dụng của dịch vụ MVPN khi chuyển mạng và phí chuyển mạng.

Ở đây ta không có ý định cung cấp một danh sách đầy đủ về một SLA cho MVPN phải gồm cái gì mà muốn nhấn mạnh tầm quan trọng của nó. Ngoài những vấn đề về luật và kinh doanh, còn đưa ra các kỳ vọng của khách hàng và định nghĩa dịch vụ mà khách hàng cuối cùng nhận được. Như vậy điều quan trọng là cả nhà cung cấp dịch vụ lẫn khách hàng nhận thấy đây là một công cụ hữu ích để tương tác với nhau: định nghĩa dịch vụ và thực hiện.

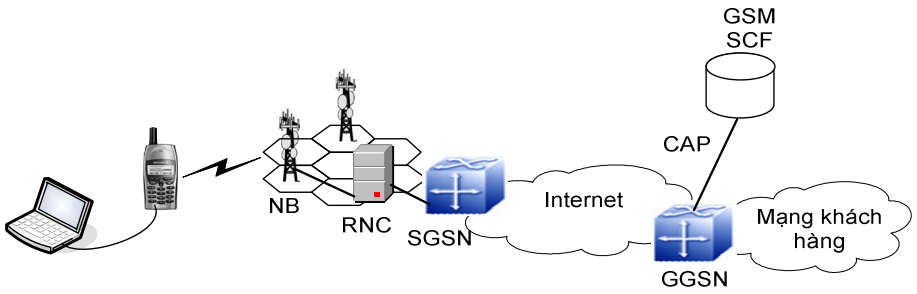
Yêu cầu mạng khách hàng là một tập rất hợp lớn, mức độ khách hàng hóa SLA sẽ phụ thuộc rất lớn vào kích cỡ MVPN khách hàng. Nó cũng phụ thuộc vào việc

liệu nhà cung cấp có muốn chuẩn hoá dịch vụ hay nhà cung cấp này muốn sử dụng tính linh hoạt của mạng mình để đáp ứng các nhu cầu khác nhau khách hàng.

4.5 Tính cước

Nếu dự tính các dịch vụ MVPN sẽ là một trong nguồn doanh thu chính cho các nhà cung cấp dịch vụ trở thành hiện thực, việc thu thập số liệu kế toán và thông tin tính cước trở thành một vấn đề quan trọng nhất để cung cấp các dịch vụ MVPN. Các nhà khai thác có thể định nghĩa kế hoạch tính cước theo thời gian, theo ngưỡng khối lượng lưu lượng, theo vị trí, hay theo các thông số khác như thông tin về mức ứng dụng được rút ra từ kiểm tra gói cụ thể.

Tính cước GPRS dựa trên CDR (Charging Data Record: Bản ghi số liệu tính cước) được thu thập để kế toán sự sử dụng truy nhập vô tuyến. Tuy nhiên, truyền kế toán RADIUS cũng được sử dụng để kế toán thời gian phiên và có thể giao tiếp với hạ tầng kế toán do mạng đối tác vận hành. Chẳng hạn RADIUS được sử dụng khi mạng khách hàng yêu cầu thu thập số liệu kế toán để phân tích xu thế và lập hồ sơ mức độ sử dụng và có thể sử dụng để tính cước cho chính truy nhập mạng một cách độc lập với tính cước được thực hiện bởi nhà cung cấp dịch vụ vô tuyến. Các tiêu chuẩn cũng định nghĩa việc hỗ trợ các dịch vụ trả trước trong GPRS. Tiêu chuẩn này là CAMEL giai đoạn 3 ({3GPP TS23.078], hình 4.5). CAMEL giai đoan 3 định nghĩa tương tác giữa SGSN với GSM SCF để cung cấp dịch vụ trả trước. Giao thức được sử dụng cho tương tác này được gọi là CAMEL Application Part hay CAP được định nghĩa trong [3GPP TS29.078].



Hình 4.5 Kiến trúc hệ thống trả trước theo CAMEL giai đoạn 3

4.6 Chuyển mạng (Roaming)

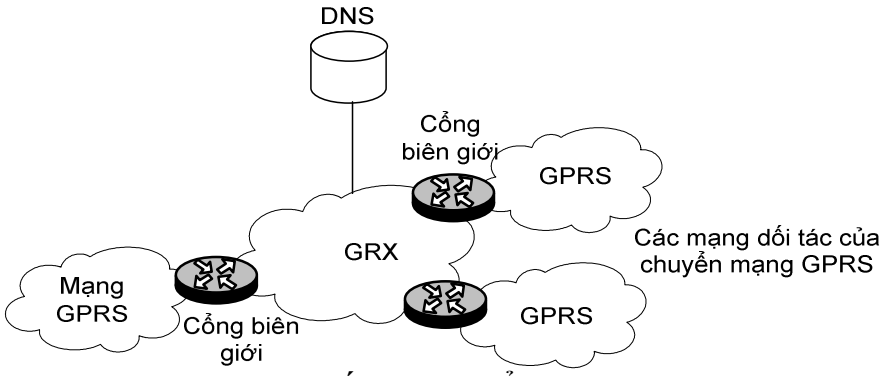
Một điểm mạnh của các hệ thống GSM/GPRS và UMTS là khả năng chuyển mạng (chuyển vùng) xuôn sẻ giữa các nước và các mạng nhà khai thác khác nhau.

Hỗ trợ chuyển mạng là nguyên nhân vì sao hiệp hội GSM được thành lập đầu tiên. Nhiều nhà khai thác đã thỏa thuận cung cấp dịch vụ cho các thuê bao di chuyển vào mạng của mình từ mạng HPMLN (Home PLMN) khác theo tập các quy tắc được định nghĩa rõ ràng được đưa ra trong GSM MoU (biên bản ghi nhớ GSM). Biên bản này đã khuyến khích nhiều hoạt động trong hiệp hội như Nhóm chuyên gia chuyển mạng quốc tế IREG (International Roaming Expert Group) để hỗ trợ chi tiết hóa kỹ thuật khi cung cấp chuyển mạng cho các thuê bao di chuyển đến các mạng hoặc các nước khác cho các dịch vụ khác nhau.

Một trong các nguyên tắc chỉ đạo của GSM MoU là VPLMN (visited PLMN – PLMN, mạng khách) không thể cung cấp nhiều dịch vụ hơn các dịch vụ mà thuê bao đã đăng ký ở HPLMN. Các mạng tham dự thỏa thuận chuyển mạng cần đặc tả các dịch vụ mà người chuyển mạng được quyền nhận khi ở chế độ làm khách và cũng phải thỏa thuận các quy tắc điều khiển cách thức có thể từ chối các dịch vụ này. Nhà khai thác mạng nhà có thể luôn luôn định nghĩa các loại người sử dụng được phép phục vụ chuyển mạng bởi VPLMN bằng cách định nghĩa thông tin cấm tất cả hay một bộ phận các dịch vụ khả dụng trong mạng VPLMN. Thông tin này được lưu trong HLR và được tải xuống nút phục vụ của mạng khách tại thời điểm nhập mạng của người sử dụng hoặc nó được chuyển đến nút phục vụ khi một người sử dụng thực hiện thủ tục cập nhật vị trí/chuyển giao. Khi MS hay thiết bị người sử dụng tìm cách nhập mạng mà nó muốn chuyển đến nhưng không được quyền chuyển mạng, mạng này có thể thông báo điều này và MS sẽ không cố gắng nhập mạng này nữa.

Vì tầm quan trọng của chuyển mạng, phần còn lại của chương sẽ tập trung lên khả năng cho phép chuyển mạng đối với các dịch vụ số liệu. Ngoài ra các tiêu chuẩn cho CAMEL vẫn còn có một số điểm chưa rõ ràng, chủ yếu do các vấn đề tương hợp, làm cho thuê bao trả trước chuyển mạng khó khăn.

Chuyển mạng số liệu GPRS/UMTS chịu sự điều khiển của cả các tiêu chuẩn và các tài liệu của conxoocxium công nghiệp như [PRD IR34] từ GSM Association IREG. Các tiêu chuẩn GPRS cho phép người sử dụng chuyển vào mạng khách và sử dụng GGSN mạng nhà hay sử dụng GGSN mạng khách. Giao diện giữa GGSN mạng nhà và SGSN mạng khách được gọi là Gp. GTP tunnel (khi GGSN mạng nhà được sử dụng) xuyên qua mạng được cung cấp bởi một nhà cung cấp mạng quá giang, gọi là mạng (GPRS Roaming Exchange). Theo IREG, GRX là một mạng số liệu riêng được xây dựng trên sơ đồ đánh địa chỉ công cộng.



Hình 4.6 Kiến trúc chuyển mạng GPRS.

Truy nhập đến GRX có thể xảy ra tại các điểm của tổng đài trung tâm giống như truy nhập đến IXC (Internet Exchange) hay các điểm truy nhập tổng đài Internet nơi mà nhiều nhà khai thác có thể trao đổi lưu lượng chuyển mạng và thiết lập liên kết đồng cấp BGP4 trên một hạ tầng L2 do nhà cung cấp GRX cung cấp. Các tuyến BGP (Border Gateway Protocol) được quảng cáo trên GRX không được phân bố bên ngoài GRX và cũng không có tuyến Internet được phân bố trên GRX. Vì thế không có kết nối tương hỗ lớp mạng giữa Internet và GRX. Các thành viên IREG cho rằng không thể điều phối sử dụng không gian địa chỉ riêng giữa các nhà khai thác, và vì vậy đây là chọn lựa tốt nhất. Tuy nhiên, hoạt động của một mạng GPRS đòi hỏi khá nhiều các địa chỉ công cộng và các cơ quan đăng ký địa chỉ Internet không cấp nhiều địa chỉ IP trong thời gian gần đây, vì thế đây là rào cản trong hoạt động của mạng.

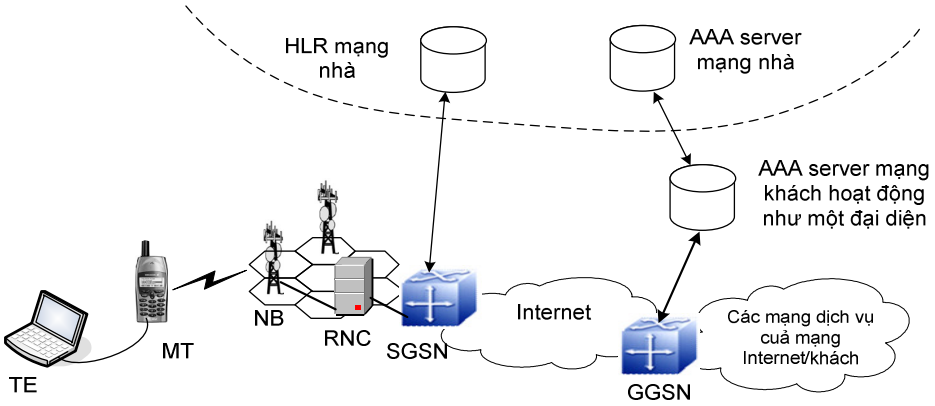
Thông thường một GRX cũng cung cấp dịch vụ DNS cho GPRS, vì thế mạng GPRS có thể phân giải tên điểm truy nhập thành địa chỉ IP trong các mạng ở xa.

Dịch vụ MVPN trên GPRS được cung cấp dựa vào GGSN mạng nhà: dành một APN cho mạng khách hàng và APN này được phân giải thành một địa chỉ hay một danh sách các địa chỉ trực thuộc GGSN trong mạng nhà. Phương pháp này đòi hỏi các GTP tunnel giữa các SGSN và các GGSN phải được bảo vệ bởi chế độ giao vận IPSec, vì thế không cần quan hệ tin cậy giữa nhà khai thác mạng khách và mạng nhà. Không cần phải mở rộng trên toàn bộ các nhà cung cấp mạng mà GTP tunnel đi qua. Tuy nhiên cũng có thể sử dụng một GGSN trong mạng khách bằng cách định nghĩa một APN phổ dụng có thể biên dịch được tại SGSN của mạng khách vào một APN và chuyển đổi APN này vào một hay nhiều địa chỉ IP trực thuộc GGSN trong mạng khách. Điều này đòi hỏi một APN kiểu PPP PDP hay một APN hỗ trợ kiểu IP PDP với chế độ truy nhập PCO và khả năng GGSN ấn định động yêu cầu đến từ người sử dụng tới một mạng VPN phù hợp và thiết lập kết nối nếu không có kết nối nào được thiết lập tĩnh. Ấn định người sử dụng đến một VPN thường dựa trên thông tin về lý lịch người sử dụng nhận được từ hệ thống con AAA (chẳng hạn thông qua Filter ID RADIUS hay các thuộc tính của "thông tin RADIUS L2TP tunnel". Các giải pháp khác có thể đòi hỏi khách hàng hóa nút GGSN nhiều hơn (chẳng hạn các bảng tra cứu).

Khi người sử dụng chuyển mạng sử dụng GGSN, cần có thông tin kế toán tại GGSN để ghi lại số liệu được sử dụng trong mạng nhà một cách độc lập với mạng khách. Ngoài ra, GGSN nhà, như đã nói ở trên, có thể sử dụng kế toán RADIUS để đảm bảo các nhu cầu của mạng khách hàng. Xác thực người sử dụng ở GGSN nhà được thực hiện giống hệt như kịch bản xác thực không chuyển mạng. Đối với các trường hợp sử dụng số liệu đăng ký thuê bao để xác thực người sử dụng, cần phải đảm bảo tính toàn vẹn báo hiệu từ SGSN khách đến GGSN nhà (IE chế độ chọn không bị thay đổi), bởi mạng khách có quan hệ tin tưởng với mạng nhà. Vì là một bộ phận của thỏa thuận chuyển mạng, cần đàm phán và định nghĩa cách thức đảm bảo bảo tính toàn vẹn báo hiệu GTP. Các kiểm soát IPSec đối với các VPN có thể được định nghĩa là một bộ phận của thỏa thuận chuyển mạng.

Xác thực người sử dụng trong GGSN mạng khách thường được điều khiển bởi thỏa thuận chuyển mạng AAA, trong đó GGSN khách có thể hoạt động như AAA

client đối với một hạ tầng AAA dựa trên RADIUS proxy và có thể có cả RADIUS môi giới (hình 4.7). Tuy nhiên cách tổ chức này không phổ biến trong GPRS, trong khi các mạng CDMA2000 chủ yếu dựa trên cách này.



Hình 4.7 Chuyển mạng GPRS với GGSN trong mạng khách

4.7 Kịch bản triển khai MVPN

Trong phần này ta sẽ phân tích một hãng lớn tại Châu Âu, có tiềm lực tài chính, tạm gọi là hãng EU. Hãng EU cung cấp các dịch vụ dựa trên CSD nhiều năm như dịch vụ truy nhập Internet và WAP. Họ cũng đã triển khai GPRS và đang lập kế hoạch hỗ trợ nhiều dịch vụ số liệu tiên tiến hơn và tiến đến 3G.

Sự phát triển mạng chuyển đến một mạng số liệu và thoại dựa trên IP thống nhất. Giao vận sẽ dựa trên MPLS. Vô tuyến quy hoạch trên cơ sở tái sử dụng mạng ATM bằng cách kết nối với MPLS và lớp ATM tại các nút biên của ATM để sử dụng lại tối đa cơ sở lắp đặt hiện có. Trao đổi lưu lượng với hãng dựa trên L2TP tunnel được đảm bảo an ninh bởi chế độ giao vận IPSec hay trên cơ sở các chế độ tunnel. Điều này đảm bảo hãng EU linh hoạt tối đa khi chọn lựa quan hệ đối tác cung cấp POP cho các khách hàng. Thực chất, các tunnel an ninh tách riêng kiến trúc cung cấp VPN ra khỏi công nghệ truy nhập lớp liên kết và ra khỏi sự tin tưởng tương hỗ giữa nhà khai thác truy nhập vô tuyến và nhà khai thác hãng EU.

Nếu khách hàng truy nhập theo phương tiện hãng khác từ xa đến một nhà cung cấp truy nhập toàn bộ nào đó, thì hãng EU có thể đảm bảo nhu cầu từ phía vô tuyến thông qua kết cuối PPP tại GGSN hay bằng cách sử dụng phương pháp truy nhập IP

vớp PCO. Hãng EU khuyên khách hàng rằng chế độ truy nhập IP PCO có thể bị tấn công bằng cách phát lại và rằng truy nhập dựa trên PPP là tốt nhất cho an ninh. Trong trường hợp mạng khách hàng sử dụng truy nhập từ xa qua L2TP, hãng EU cung cấp chức năng LAC bằng cách cho phép GGSN khởi đầu các L2TP tunnel và quản lý tất cả các đàm phán và cấu hình PPP với sử dụng số liệu truyền đến GGSN qua GTP. Hãng EU không tin đây là giải pháp đích, nhưng họ vẫn đưa ra lựa chọn này cho khách hàng không có các đầu cuối hỗ trợ PPP PDP (giai đoạn đầu của GPRS và UMTS, kiểu PPP PDP chưa phổ biến do hạ tầng chưa phát triển). Hãng EU không tiếp nhận đề xuất từ một số nhà cung cấp thiết bị bố trí hỗ trợ toàn bộ MVPN dựa trên các VPN client ở các đầu cuối, vì đây là phương pháp ít lợi nhuận nhất và không cho phép điều khiển cung cấp dịch vụ giống như các phương pháp dựa trên mạng. Chẳng hạn, nhà cung cấp có thể điều khiển PPP LCP echo qua đại diện tại GGSN hay cấm nó tại GGSN khi PPP kết cuối tại GGSN. Các bản tin *Keep Alive* do các client VPN tạo ra không thể điều khiển được, vì hạ tầng sẽ cảm nhận nó như lưu lượng thông thường của người sử dụng. Ngoài ra, các giải pháp VPN dựa trên mạng không tạo ra định kỳ các bản tin *Keep Alive* trên giao diện vô tuyến. Điều này cho phép các chu kỳ không tích cực dài để không phải cấp phát các kênh mang vô tuyến cố định cho người sử dụng vô tuyến. Vì thế hãng EU chỉ quy hoạch theo các giải pháp dựa trên mạng.

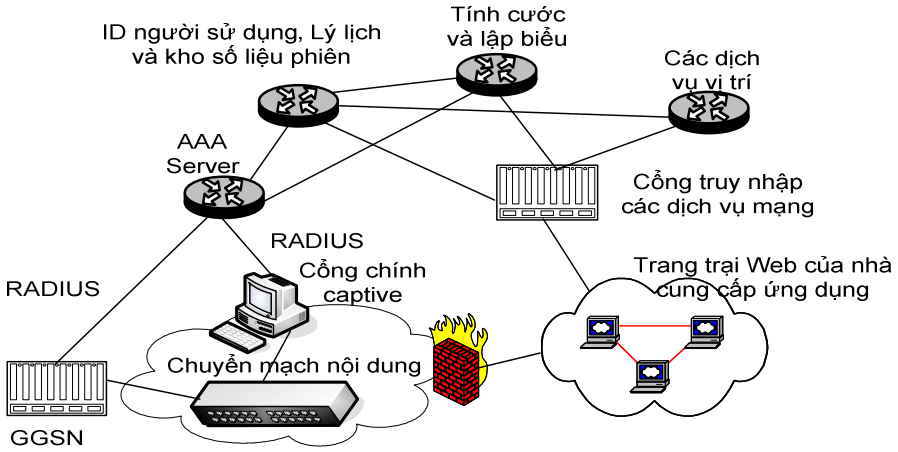
Hãng EU nhận thấy rằng tùy chọn quản lý các cổng IPSec VPN thuộc hãng khác là đắt tiền, mà không có lợi rõ ràng. Ngoài ra nó đòi hỏi các VPN GW/VPN client phải được chuẩn hoá cho mạng, vì các vấn đề tương hợp chung giữa các VPN client và các GW từ các nhà sản xuất khác nhau.

Hãng EU cũng bảo vệ đầu tư tiền bạc trong các dịch vụ số liệu và cơ sở khách hàng. Thông thường điều này thể hiện bởi người sử dụng dịch vụ WAP dựa trên CSD. Trong thực tế truy nhập từ xa đơn giản không đòi hỏi các hãng thiết lập bất cứ một thoả thuận nào với hãng, vì số quay truy nhập giống như số quay được sử dụng để truy nhập hữu tuyến. Tốc độ thấp và sử dụng dịch vụ hạn chế hầu như dẫn đến không khách hàng nào sử dụng dịch vụ truy nhập dựa trên L2TP thực hiện bằng

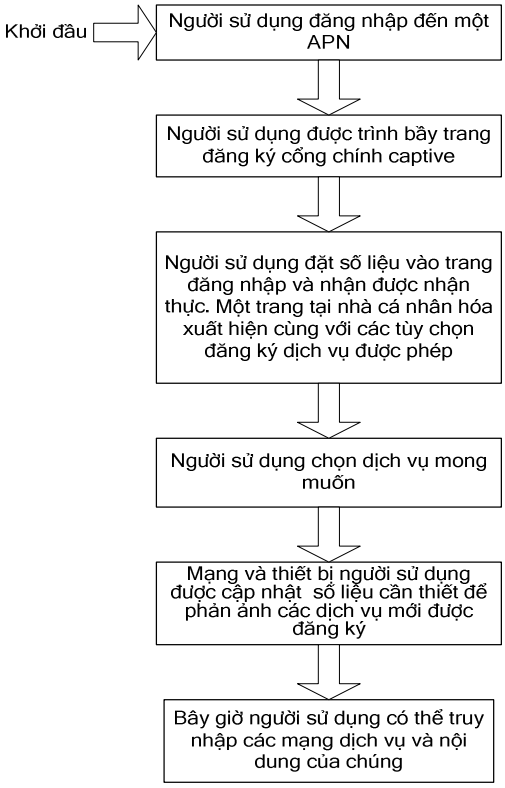
cách sử dụng IWF như LAC. Điều lo ngại thực tế là làm sao hạ tầng WAP trở lên chung nhất giữa các miền CS và PS. Điều này khá dễ do cách giống nhau để truy nhập các dịch vụ WAP từ GPRS và CSD bằng cách tái sử dụng WAP GW và các thủ tục tương tác WAP GW thông qua truy nhập L2TP đến LNS bằng cách tương tác với WAP GW.

Từ góc độ quản lý mạng và cung cấp dịch vụ, tích hợp các ứng dụng với lập cấu hình các phần tử mạng được thực hiện theo lưu đồ quá trình cung cấp (hình 4.10) và có thể có các kịch bản phức tạp hơn. Điều này cho phép người sử dụng bắt đầu phiên bằng một APN duy nhất để truy nhập mạng dịch vụ và sau đó nối đến mạng hãng hay một mạng trò chơi trong đó một cộng đồng người có thể chia sẻ thông tin và trao đổi các phương tiện trên một mạng có mức QoS đặc thù và dự báo được.

Tại từng giai đoạn, giá truy nhập mạng sẽ thay đổi nhờ vậy thích ứng động phí truy nhập mạng đối với ứng dụng được sử dụng, và đem lại ưu việt cho khách hàng mạng EU và bản thân nhà khai thác mạng này. Các khách hàng phải trả tiền ở giá cả hợp lý cho từng hoạt động mà họ thực hiện, trong khi nhà khai thác giữ được các khách hàng và thu hút các khách hàng mới bằng giá cước hợp lý đồng thời cung cấp một môi trường ứng dụng có thể dự báo trước và nhận được lợi nhuận phù hợp cho từng dịch vụ truy nhập mạng cung cấp.



Hình 4.9 Kiến trúc quản lý nhận dạng người sử dụng



Hình 4.10 Lưu đồ cung cấp dịch vụ

Chương 5 Thị trường và khả năng triển khai MVPN

5.1 Thị trường MVPN

Các nhà kinh doanh đã làm việc hiệu quả với VPN hữu tuyến hiện nay đang chờ các nhà khai thác vô tuyến mở rộng các dịch vụ này vào môi trường vô tuyến. Trong vài năm tới đây, khi các thế hệ mới nhất của các hệ thống TTDĐ và các công nghệ vô tuyến mới phát triển, cơ hội thị trường to lớn chờ đợi các nhà khai thác có khả năng đáp ứng nhu cầu cho các dịch vụ đòi hỏi truy nhập mạng số liệu riêng.

Hơn nữa, các công ty và cơ quan lớn muốn tận dụng các dịch vụ MVPN của các nhà khai thác vô tuyến để trở thành một bộ phận của cơ sở hạ tầng IT của họ. Do vậy MVPN là dịch vụ rất có tương lai.

Các động lực để phát triển MVPN:

1. Tăng năng suất nhờ áp dụng công nghệ IT và tăng trưởng Internet.
2. Nhu cầu di động rộng khắp.
3. Phát triển thiết bị di động mới.
4. Tiến bộ của các hệ thống TTDĐ (mạng số liệu gói trong 2G và 3G).
5. Lối sống và vị trí công tác di động.
6. Tăng trưởng VPN hữu tuyến.

Thị trường MVPN (như mọi thị trường khác), bao gồm các loại hành hóa (dịch vụ) mà người mua sẽ nhận được, người mua (khác hàng truy nhập mạng số liệu riêng) và người bán (các nhà khai thác vô tuyến và các nhà cung cấp dịch vụ) tham gia các giao dịch liên quan đến một sản phẩm hay loại sản phẩm (truy nhập mạng số liệu riêng ở môi trường di động) và cuối cùng là hợp đồng hay cam kết giữa người bán và người mua.

MVPN có một danh sách các dịch vụ đa dạng có thể bao quát khá rộng các nhu cầu của khách hàng. Tùy theo SLA được thỏa thuận giữa khách hàng và nhà cung cấp dịch vụ, khách hàng có thể được hưởng các mức an ninh khác nhau. Các dịch vụ mà MVPN có thể cung cấp cho khách hàng là:

Các dịch vụ dựa trên các mô hình truyền tunnel như:

- Đầu cuối đầu cuối, hay tự ý
- Dựa trên mạng hay bắt buộc
- Kênh hay các tunnel trung gian

Trên GPRS/UMTS các dịch vụ này là:

- Kiểu IP PDP.
- Simple IP (IP đơn giản).
- IP với các tùy chọn cấu hình giao thức.
- Kiểu PPP PDP (bắt đầu có từ R98).
- Chuyển tiếp PPP.
- PPP kết cuối tại GGSN.

Trên CDMA2000 các dịch vụ này là:

- IP đơn giản
- MIP

Đối với các nhà khai thác đang triển khai các hệ thống thông tin di động thế hệ mới như UMTS và CDMA2000, MVPN không chỉ là một trong các công nghệ cần thiết để truy nhập mạng số liệu riêng của khách hàng mà còn là nền tảng tương tác với các mạng số liệu riêng. Lợi ích triển khai MVPN bao gồm:

- Khả năng kết nối không gián đoạn, độc lập vị trí đến mạng số liệu riêng.
- Khả năng di động truy nhập mạng số liệu riêng suôn sẻ.
- Khả năng kết nối đến một ISP hay ASP.
- Các khả năng truy nhập di động từ xa.
- Cho phép thương mại di động an ninh.
- Chi phí cơ hội (do thời gian đáp ứng nhanh).

Các ích lợi triển khai MVPN có ý nghĩa đối với cả khách hàng và nhà cung cấp dịch vụ. MVPN cho phép cán bộ công tác xa kết nối thường xuyên, độc lập phương tiện đến mạng số liệu riêng hay đến các ISP và các ASP. MVPN cho phép khách hàng sử dụng thiết bị của hãng khác để truy nhập từ xa và trong một số trường hợp có thể thay thế hoàn toàn các cơ sở hạ tầng truy nhập từ xa hữu tuyến, nhờ vậy tránh

được các chi phí mua và hỗ trợ thiết bị truy nhập từ xa trong khi vẫn cho phép các mạng số liệu riêng duy trì điều khiển hoàn toàn việc ấn định địa chỉ IP cho người sử dụng, xác thực và an ninh. Các khách hàng sử dụng MVPN tiềm năng là:

- Các nhà kinh doanh nhỏ.
- Các xí nghiệp lớn.
- Các công sở nhà nước, các học viện.
- Các nhà cung cấp ứng dụng (ASP).

5.2 Mô hình MVPN tham khảo đề xuất cho Việt Nam

Việt nam hiện nay có 6 nhà cung cấp, với đủ đại diện của 2 nền công nghệ đang có hiện nay trên thế giới là GSM/GPRS và CDMA2000. Bảng 5.1 cho thấy rõ các đặc điểm cơ bản của các nhà cung cấp này (đến 10/2006).

Nhà cung cấp	Công nghệ sử dụng	Tình trạng mạng	Số lượng thuê bao
VMS-MobiFone	GSM/GPRS; 4/2005 thử nghiệm thành công 3G.	Triển khai năm 1993	5,8 triệu
VinaPhone	GSM/GPRS	Triển khai năm 1996	5,9 triệu
Viettel	GSM/GPRS	Triển khai năm 2004	5,0 triệu
S-Fone	CDMA-3x	Triển khai năm 2003	0,7 triệu
EVN	CDMA-1x	Triển khai năm 2006	Chưa có số liệu
HaNoi Telecom	CDMA-3x	Chưa triển khai	Chưa có số liệu

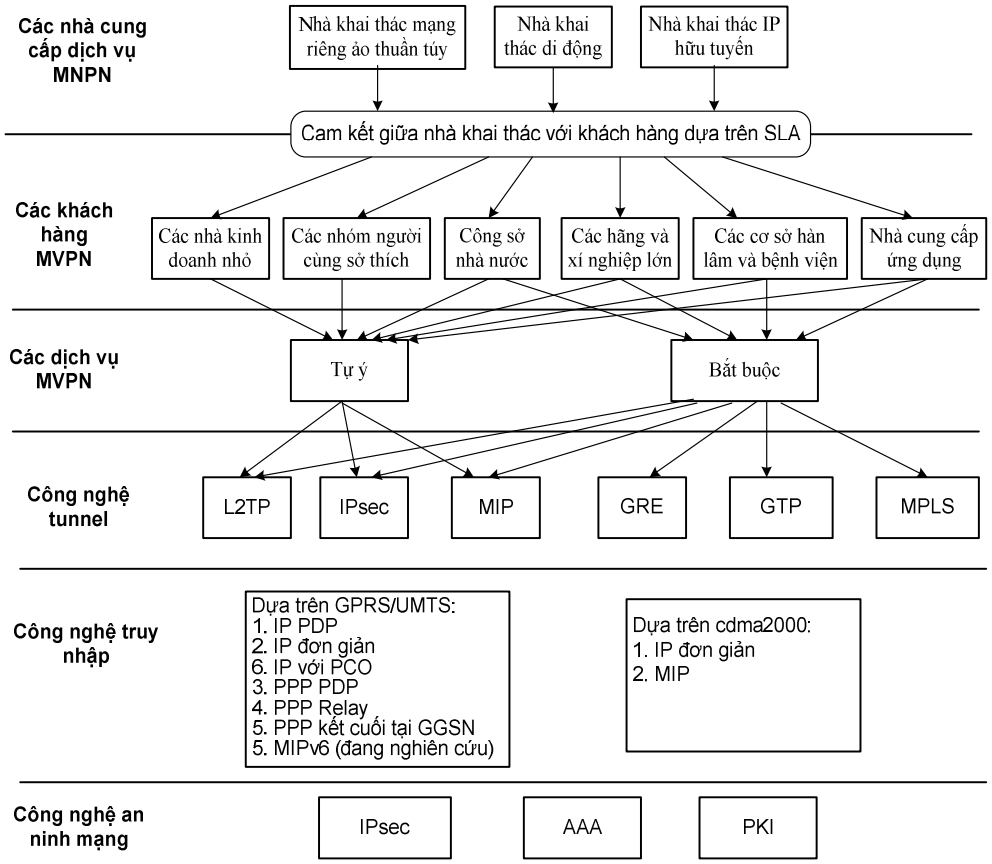
Bảng 5.1 Các nhà cung cấp TTDĐ tại Việt Nam [nguồn trên mạng Internet]

Động lực phát triển MVPN tại Việt Nam:

1. Mục tiêu chính phủ điện tử của nhà nước Việt Nam
2. Số lượng doanh nghiệp thành lập ngày càng lớn. Qui mô và mạng lưới các doanh nghiệp rộng lớn. Dẫn đến mạng lưới VPN hữu tuyến gia tăng mạnh mẽ.
3. Đầu tư CNTT để tăng cường sức cạnh tranh đang là trào lưu và được chú trọng trong các doanh nghiệp. Nhất là trong các nghành ngân hàng, bảo hiểm, viễn thông, ...;

4. Bùng nổ về Internet băng thông rộng (ADSL, SHDSL, ..) và các ứng dụng trên mạng;
5. Làn sóng đầu tư lớn, mới của các công ty đa quốc gia đang diễn ra vào Việt Nam.
6. Số lượng thuê bao di động lớn (17 triệu hiện nay), tốc độ tăng trưởng bình quân từ 25 đến 35 % năm.
7. Các doanh nghiệp viễn thông có đủ tiềm lực và kinh nghiệm đáp ứng.

Từ các phân tích trên, mô hình tham khảo MVPN tổng quát đề xuất ứng dụng vào Việt Nam, hình 5.1:



Hình 5.1 Mô hình tham khảo MVPN tham khảo

Mô hình này chia thành các lớp sau:

- Các nhà cung cấp dịch vụ.
- Các khách hàng.

- Các dịch vụ.
- Công nghệ tunnel.
- Công nghệ truy nhập.
- Công nghệ an ninh mạng.

Lớp các nhà cung cấp dịch vụ MVPN bao gồm:

- *Các nhà khai thác thông tin di động*: là nhóm cung cấp dịch vụ MVPN lớn nhất vì họ có giấy phép phổ tần lẫn hạ tầng vô tuyến.
- *Các nhà khai thác mạng riêng ảo thuần túy*: cung cấp dịch vụ MVPN dựa trên các phương tiện truyền thông của các nhà khai thác thông tin di động và hữu tuyến.
- *Các nhà cung cấp dịch vụ Internet hữu tuyến*: tham gia cung cấp dịch vụ MVPN thông qua các thỏa thuận với các hãng khai thác vô tuyến. Cung cấp dịch vụ MVPN không phải là khả năng tạo lợi nhuận mới mà chỉ đơn thuần mở rộng dòng sản phẩm, nghĩa là tăng thêm các dịch vụ hữu tuyến bằng các tùy chọn MVPN mới. Điều này cho phép các ISP hữu tuyến trở thành nhà cung cấp dịch vụ duy nhất cho các khách hàng truyền thống không phụ thuộc vào phương pháp truy nhập mạng (vô tuyến hay hữu tuyến).

Việt Nam chưa tồn tại phương thức kinh doanh bằng cách cho thuê lại cơ sở hạ tầng vô tuyến, do vậy *Các nhà khai thác thông tin di động* là khả thi nhất.

Lớp các khách hàng:

Việt Nam hiện nay hội đủ các khách hàng trên. Tuy nhiên các khách hàng lớn nhất là các khách hàng có tiềm lực tài chính, có nhu cầu trao đổi thông tin, giao lưu, và nhu cầu di chuyển cao như các doanh nghiệp lớn, các nhà cung cấp ứng dụng, các hộ kinh doanh vừa và nhỏ, các nhóm cùng sở thích.

Lớp dịch vụ

- *MVPN tự ý*
- Rất thích hợp cho các hộ kinh doanh vừa và nhỏ, các nhóm cùng sở thích, và các nhà cung cấp ứng dụng.

- *MVPN bắt buộc*
- Rất thích hợp cho các doanh nghiệp lớn có nhu cầu sử dụng cao như viễn thông, ngân hàng, bảo hiểm,… Các doanh nghiệp này có mạng lưới rộng lớn, nhu cầu đáp ứng sản xuất kinh doanh mọi lúc mọi nơi. Khi sử dụng dịch vụ này, doanh nghiệp phải thiết lập SLA chi tiết với nhà cung cấp dịch vụ và phải tin tưởng nhà cung cấp dịch vụ trong việc xử lý số liệu giá trị với trách nhiệm và bí mật cần thiết. Tuy nhiên luật pháp hiện nay còn có nhiều hạn chế trong vấn đề này, gây ra nhiều lo ngại cho doanh nghiệp sử dụng dịch vụ.

Lớp công nghệ truyền tunnel và công nghệ truy nhập

Các công nghệ tunnel như L2TP, IPSec, GRE, .. đều được hầu hết các thiết bị trên mạng lưới hỗ trợ (cả cứng và mềm). Riêng MPLS chưa phổ biến, ví dụ như các Cisco router có phiên bản IOS từ 12.x mới hỗ trợ.

Lớp công nghệ truy nhập

Các hệ thống GSM/GPRS và CDMA2000-1x đã sẵn sàng hỗ trợ *IP đơn giản*, *MIP* và *PPP kết cuối tại GGSN*. Chỉ cần thực hiện một số bước là cấu hình và khai báo thích hợp để cung cấp dịch vụ.

Lớp công nghệ an ninh mạng

IPSec, AAA, PKI đã trở lên quen thuộc và phổ biến trên thị trường. Trong các mạng viễn thông, nó đang dần trở thành các chuẩn bắt buộc thông qua các dịch vụ mới đưa vào.

Với các phân tích trên, việc triển khai MPVN tại Việt Nam về mặt kỹ thuật là hoàn toàn khả thi, với các dịch vụ sản phẩm phù hợp. Triển khai mạng NGN gần đây là bước thúc đẩy quan trọng trong việc thiết lập mạng IP hỗ multimedia.

Tuy nhiên, Vì nhiều lý do khác nhau, nên các nhà cung cấp dịch vụ hiện chưa mặn mà lắm cho triển khai MVPN như: Do chính sách tầm vĩ mô (nhà nước) chưa thích hợp, cạnh tranh giữa các nhà cung cấp đang ở thời kỳ cao điểm và đang chú trọng đến mở rộng vùng phủ sóng cũng như nâng cấp chất lượng mạng lưới,....

Kết luận

Luận văn đã đạt được các mục tiêu sau:

- Nghiên cứu tổng quan các hệ thống thông tin di động trên thế giới
- Nghiên cứu Cơ sở nền tảng MVPN
- Nghiên cứu các giải pháp VPN trên CDMA2000
- Nghiên cứu các giải pháp VPN trên GMS/GPRS/UMTS
- Thị trường và khả năng triển khai MVPN

Trên cơ sở các nghiên cứu đạt được đề xuất:

- Để phát triển các dịch vụ MVPN cũng như các dịch vụ di động mới, cần nhanh chóng triển khai thử nghiệm và đưa vào khai thác các hệ thống thông tin di động thế hệ ba
- Nhà nước cũng cần đưa ra các quy định pháp lý để bảo vệ khách hàng khi SLA của họ bị vi phạm để họ tin tưởng hơn vào dịch vụ MVPN

MVPN không chỉ mới ở Việt Nam mà còn cả ở trên thế giới, nhưng sự phát triển của nó trong tương lai là tất yếu. Tuy nhiên MVPN còn đang trong giai đoạn nghiên cứu và hoàn thiện, và chưa có triển khai áp dụng thực tế.

Hạn chế của đề tài là chưa đề cập đến các vấn đề liên quan đến MVPN như : QoS, chưa có các bước và lộ trình chuyển đổi cụ thể cho các hệ thống TTDĐ hiện nay như thế nào khi ứng dụng MVPN, ... Vì thế các nhận định cũng như đề xuất chỉ mang tính khởi đầu và cần theo dõi sự phát triển MVPN trong những năm tới.

Tài liệu tham khảo

[1] RFC (Request for Comments):

- [RFC2486] "The Network Access Identifier", 1999.
- [RFC2709] "Security Model with Tunnel-mode IPSec for NAT", 1999.
- [RFC2983] "Differentiated Services and Tunnels", 2000.
- [RFC3118] "Authentication for DHCP Messages", 2001.
- [RFC3141] "CDMA2000 Wireless Data Requirements for AAA," 2001.
- [RFC3220] "IP Mobility Support for IPv4", 2002.
- [RFC2865] "Remote Authentication Dial In User Service (RADIUS)," 2000.
- [RFC2866] "RADIUS Accounting," 2000.

[2] 3GPP (The 3rd Generation Partnership Project) Specifications:

- [3GPP TS 24.008] "Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3," 2002.
- [3GPP TS 32.215] "Telecommunication Management; Charging and Billing; 3G call and event data for the Packet Switched (PS) domain," Release 4 and Release 5, 2002.
- [3GPP TS 29.061] "Packet Domain; Interworking between the Public Land Mobile Network (PLMN). Supporting Packet Based Services and Packet Data Networks (PDN)," 2002.
- [3GPP TS 27.060] "Packet Domain; Mobile Station (MS) Supporting Packet Switched Services," 2001.
- [3GPP TS 23.003] "Numbering, addressing and identification."

[3] Dave Wissely, Philip Eardley and Louise Burness. " IP for 3G. Networking Technologies for Mobile Communication", John Wiley and Sons, 2002.

[4] Alex Shneyderman and Alessio Casati, "Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems, Jhon Wiley & Sons, 2003.

[5] Basavaraj Patil, Yousuf Saifullah, Stefano Faccin and others, "IP in Wireless Networks", Prentice Hall PTR, 2003